BALANCING CODE AND LAW:

Governance and Policy Challenges of Blockchain

FLORENCE G'SELL

Stanford University

TABLE OF CONTENTS

Acknowledgments	1
Executive Summary	2
Chapter 1: Introduction	6
Chapter 2: Blockchain Technology: The Basics	28
Chapter 3: Blockchain Governance	86
Chapter 4: Use Cases	127
Chapter 5: Risks and Challenges	171
Chapter 6: Legal Challenges	232
Chapter 7: Policy Strategies	299
Chapter 8: General Conclusion	381
Appendices	402
Selected Bibliography	444
List of Figures	448

ACKNOWLEDGMENTS

This work would not exist without the dedicated efforts of the members of the Governance of Emerging Technologies program at the Cyber Policy Center. We are greatly indebted to the Project Liberty Institute for their support of the Program on Governance of Emerging Technologies, which made this report possible.

Primavera De Filippi (Director of Research, CNRS; Faculty Associate, Harvard) made a substantial contribution to Chapter 3 on blockchain governance, revising and finalizing significant portions of the chapter on the basis of an earlier draft.

Several researchers and scholars contributed at the inception of the project, producing original draft materials or inputs that informed specific sections of the report: Ashok Ayyar (Stanford), Zeke Gillman (Stanford), Claude Humbel (Lucerne), Wanjiku Karanja (Stanford), Adrian Mak (Stanford), Hailing Ni (Stanford), Juan Du (Sydney), and Reuben Youngblom (Stanford). Some of these contributions are reflected in the final text, while others are included in the Appendices and attributed to their respective authors.

Significant research assistance —including fact-checking, legal verification, updating of sources and selected passages, and Bluebook citation— was provided by Kyrylo Korol (Stanford) and Sushmita Som (Stanford). Additional research assistance, fact-checking, and Bluebook citation support were provided by Adèle Boreau-Potocki (Sciences Po), David Mollenkamp (Stanford), Aniket Rajpurohit (Stanford), and Reynold Lagman Orsua (Stanford).

This report has benefited from careful review and comments from Keith Bear (Cambridge Centre for Alternative Finance), Oguz Genc (University of Tokyo), Bianca Kremer (Wharton Blockchain and Digital Asset Project), Prof. William Lehr (MIT), Alexander Neumueller (Cambridge Centre for Alternative Finance), Scott Moore (Gitcoin), Riana Pfefferkorn (Stanford), Prof. Jeff Strnad (Stanford), Samuel Vance Law (Decentralization Research Center), and Anja von Rosenstiel (Boston University).

Sincere thanks are also due to Prof. Florence Guillaume (Neuchâtel), Morshed Mannan (Edinburgh), Marina Markezic (European Crypto Initiative), and Sarah Nicole (Project Liberty) for their helpful comments.

Invaluable technical support was provided by copy editor Lisa Keen and designer Michi Turner.

EXECUTIVE SUMMARY

Blockchain technology emerged from a long-standing ambition to develop decentralized digital systems capable of operating without trusted intermediaries. Drawing on late-twentieth-century cypherpunk and crypto-anarchist thought and brought into practical form with the launch of Bitcoin in the aftermath of the 2008 financial crisis, blockchain was designed to replace reliance on centralized institutions with trust in decentralized, code-based infrastructures. The ambition was not merely technical, but political: to enable peer-to-peer coordination, resist censorship, and reduce dependence on centralized authorities. Today, blockchain is widely presented as a foundational infrastructure for a new phase of the internet —often referred to as Web3— and promises greater user autonomy, transparency, and resistance to centralized control.

At its core, blockchain is a distributed ledger that records transactions in a tamper-resistant and verifiable manner without relying on a central authority. Its defining features —decentralization, transparency, immutability, and programmability— enable new forms of economic organization and governance. Smart contracts allow for the automated execution of agreements, while tokenization supports new models of ownership and value exchange. These innovations have given rise to a rapidly evolving ecosystem that extends far beyond cryptocurrencies. Blockchain-based registries, data-sharing systems, digital identity solutions, supply-chain tools, social-media platforms, and decentralized dispute-resolution mechanisms illustrate the technology's broader potential. Emerging projects in decentralized artificial intelligence further suggest new possibilities for using blockchain-based systems to coordinate compute resources and enable agentic collaboration. While these applications remain at varying stages of maturity and face technical and governance challenges, they demonstrate that blockchain's relevance extends well beyond crypto-asset markets. Across these domains, blockchain can improve transparency, auditability, and user control when embedded within robust governance arrangements.

Yet the promise of decentralization warrants careful qualification. In practice, blockchain systems do not eliminate trust or power; they redistribute them. Governance remains essential to the operation and evolution of these systems. On-chain governance promises automation and transparency through token-weighted voting and smart-contract execution. On-chain rules coexist with off-chain social consensus: informal norms, social influence, and technical expertise often matter as much as formal voting mechanisms. Foundations and developer communities exercise significant influence despite lacking formal accountability. The episode of the DAO attack remains emblematic: Immutability and "code is law" endure only so long as communities accept their implications. Moreover, decision-making authority is often concentrated among a small number of dominant actors —core developers, validators, large token holders, and infrastructure providers. Whereas blockchain systems frequently exhibit technical decentralization —distributing infrastructure across multiple nodes and enabling permissionless participation— their governance tends to remain centralized.

Meanwhile, the blockchain ecosystem has proven particularly vulnerable to systemic failures. Crypto-asset markets remain highly volatile and susceptible to speculation, manipulation, and systemic shocks. High-profile failures —from Mt. Gox to Terra/Luna and FTX— have exposed structural weaknesses, including excessive leverage, opaque governance, and misuse of customer funds. Security vulnerabilities remain significant, particularly at the application layer in decentralized finance (DeFi), where protocols, oracles, and cross-chain bridges constitute frequent attack surfaces. Blockchain's pseudonymity,

permissionless access, and lack of centralized control can facilitate illicit activity —fraud, money laundering, ransomware, and sanctions evasion— even as the radical transparency of public blockchains enables forensic tracing and law-enforcement investigations. Environmental impacts —especially those associated with proof-of-work mining— continue to fuel policy debate.

Blockchain, code, and law

From a legal perspective, blockchain's decentralized, pseudonymous, and transnational architecture fundamentally challenges existing regulatory frameworks. The emergence of code-based governance —reflected in the notion that "code is law"— has led some scholars to characterize blockchain as a distinct normative order, *lex cryptographica*, in which rules are enforced through self-executing protocols rather than legal institutions. On this account, blockchain systems may operate outside, or at the margins of, established legal regimes —a condition described as "alegality." However, this characterization requires substantial qualification. Although law's reach remains more limited in the context of blockchain than in traditional centralized environments, legal orders continue to reassert themselves —albeit incompletely and unevenly— at the points where blockchain systems intersect with human actors, markets, and institutions.

Courts have confronted fundamental questions about the boundary between technically permissible conduct within a protocol and unlawful manipulation under established legal doctrines. To date, they have not produced stable or consistent answers. The *Mango Markets* case, for example, did not resolve whether interacting with a protocol in unanticipated ways constitutes criminal misconduct. This lack of resolution reflects a persistent inability of existing legal frameworks to draw stable boundaries between permissible strategic behavior and unlawful manipulation. Equally unresolved is the question of whether blockchain developers can be held liable for software they create but do not operate. Another key case, the *Uniswap* decision, rejected liability for third-party misuse of smart contract code, while the English Court of Appeal in *Tulip Trading* left open the possibility that developers exercising significant authority over network maintenance may owe fiduciary-like duties to users. While blockchain technology aspires to eliminate intermediaries, it has, in practice, generated new categories of actors —developers, validators, protocol foundations, token holders, and oracles— whose legal accountability is increasingly addressed by courts. However, a coherent liability framework has yet to solidify.

Beyond these foundational questions of code and liability, courts face persistent uncertainty across several other domains. For instance, the legal status of smart contracts remains ambiguous: No stable doctrinal framework has emerged to determine when self-executing code constitutes a legally binding agreement. The *Tornado Cash* litigation illustrates how far this uncertainty extends. The Fifth Circuit held that immutable smart contracts cannot be treated as "property" under the applicable sanctions framework because they operate autonomously beyond any party's control. This decision lent limited support to the thesis of "alegality" while leaving unresolved the status of mutable contracts. Yet the case simultaneously confirmed that human actors involved in the design and deployment of smart contracts remain fully within the reach of the law.

Decentralized Autonomous Organizations (DAOs) present related challenges. Courts have increasingly treated unincorporated DAOs as general partnerships, potentially exposing the holders of governance tokens in those organizations to joint and several liability. This development reveals that decentralization does not shield participants from legal

accountability and may, paradoxically, expand the pool of liable actors. Cross-border fragmentation further compounds these difficulties. Blockchain networks operate transnationally, while regulatory frameworks remain territorially bounded, and neither private international law adaptations nor international soft-law instruments have fully resolved the resulting conflicts. Taken together, these challenges reveal a structural misalignment between decentralized architectures and legal frameworks historically built around identifiable, territorially anchored, and centrally controllable actors.

Regulatory strategies and their limits

Against this backdrop, policymakers have adopted four principal regulatory strategies, each reflecting distinct institutional philosophies and risk tolerances. The *observational approach* —relying on non-binding guidance and regulatory sandboxes— supports innovation and manages uncertainty, but it also generates sustained legal indeterminacy and has frequently served as a transitional phase, as illustrated by the subsequent shift toward more interventionist frameworks in jurisdictions such as Singapore, Canada, and Australia. *Regulation by enforcement* has been most prominently pursued in the United States, where regulators have shaped regulatory boundaries incrementally through case-by-case securities and commodities proceedings rather than ex ante rulemaking. This approach generates legal uncertainty and forces market participants to infer applicable standards from enforcement outcomes. Under the current U.S. administration, however, policy has shifted toward greater ex ante clarity, with the GENIUS Act for stablecoins marking a consequential legislative reorientation, even as broader statutory reform remains under debate.

Proactive legislative frameworks have produced the most comprehensive regimes, as illustrated by the European Union's Markets in Crypto-Assets Regulation (MiCA), which establishes a harmonized framework for crypto-assets. It also explicitly excludes services provided in a fully decentralized manner without any intermediary —an exclusion that both acknowledges the governance challenges posed by blockchain and underscores the structural limits of intermediary-centered regulation. Other jurisdictions have pursued more targeted adaptations of existing legal frameworks, addressing the legal treatment of digital assets, distributed-ledger securities, and decentralized organizations, though these regimes remain fragmented and difficult to apply across borders.

Some jurisdictions have sought to govern blockchain technologies indirectly by targeting specific use cases rather than blockchain systems as such. The EU Data Act, for example, subjects smart contracts used in data-sharing arrangements to detailed design and governance requirements, demonstrating that regulatory obligations can reach into decentralized systems while also revealing their limits. Requirements such as reversibility and "kill switches" conflict directly with immutability and distributed governance, to such an extent that the European Commission has proposed repealing key provisions of the Act. In the U.S., DAO-specific legislative frameworks —including Wyoming's DUNA, Utah's LLD, and New Hampshire's registry-based model— retain a mandatory human-mediated gateway to legal recognition, falling short of more ambitious proposals that would grant DAOs automatic legal personhood based solely on their technical architecture.

At the other end of the spectrum, some jurisdictions have adopted *prohibition-based regimes*. China's ban on decentralized cryptocurrency activity, alongside the promotion of state-controlled blockchain infrastructure, reflects a fundamentally different regulatory philosophy that prioritizes monetary sovereignty over market development.

Across these approaches, a common structural tension persists: regulatory frameworks premised on identifiable intermediaries and centralized control struggle to accommodate genuinely decentralized, permissionless systems. Regulation consequently gravitates toward accessible chokepoints —exchanges, custodial wallet providers, crypto-asset service providers— leaving autonomous protocols only partially governed. No jurisdiction has successfully resolved this tension. The most decentralized blockchain applications continue to operate in legal uncertainty regardless of the regulatory approach adopted. This does not reflect a lack of regulatory ambition but a structural constraint: a fundamental misalignment between decentralized technological architectures and legal frameworks historically built around identifiable intermediaries.

Conclusion

Blockchain does not represent a fully autonomous or “alegal” domain, nor can it be effectively governed through traditional regulatory paradigms alone. What has emerged instead is a contested zone in which code, legal norms, and social coordination interact in ways that existing frameworks were not designed to handle. The central challenge for policymakers is no longer whether blockchain technologies should be regulated —litigation and legislation have settled that question— but how frameworks can meaningfully govern a technology deliberately engineered to resist the intermediaries and territorial anchors on which regulation depends. Addressing these challenges —defining sound governance for decentralized systems, clarifying the legal status of computer code, and establishing credible accountability mechanisms— will require sustained deliberation among technologists, legal scholars, regulators, and the broader blockchain community. What is clear is that effective governance will emerge neither from the unilateral dominance of code over law nor from the wholesale imposition of legacy regulatory frameworks onto decentralized systems. It will instead require adaptive frameworks that take the technology’s structural resistances seriously —not as problems to be eventually solved, but as permanent features of the governance landscape that any credible response must learn to work within.

CHAPTER 1

Introduction

CHAPTER 1 TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION	**6**
1.1. From Crypto Anarchists to Web3	9
1.1.1. The Emergence of Cryptos	10
1.1.2. The Promise of Web3	14
1.2. Challenges of Blockchain Policy	16
1.3. Possible Policy Approaches	18
1.3.1. Regulating or Not Regulating?	19
1.3.1.A. Self-Regulation	19
1.3.1.B. Government Regulation	20
1.3.2. Functional, Regulatory and Technological Equivalence	22
1.3.2.A. Functional Equivalence	22
1.3.2.B. Regulatory Equivalence	23
1.3.2.C. Technological Equivalence	24
1.3.3. Potential Regulatory Options	25
1.4. Purpose and Structure of the Report	26

CHAPTER 1
Introduction

Nearly forty years ago, well before the internet emerged as a truly global communications infrastructure, "crypto anarchists" imagined a digital realm in which individuals would be free to interact anonymously, beyond the reach of taxation, censorship, or state surveillance. Now, the emancipatory promise of what then was called "cyberspace" remains largely unfulfilled. Rather than producing a decentralized and liberating environment, the internet has enabled the rise of immense centralized platforms that harvest unprecedented quantities of personal data for profit. Operating through opaque algorithmic systems, these massive platforms can now mediate access to information and exert profound influence over the everyday lives of billions of people, often without meaningful transparency or public accountability.

Yet, the idea of combining distributed networks with cryptography continued to evolve. It re-emerged in the aftermath of the 2008 global financial crisis with the launch of the Bitcoin network in 2009 *(See Figure 1)*. Ethereum soon followed *(See section 2.3.2.B)*, along with a growing constellation of blockchain-based systems, including Solana, Polkadot, Avalanche, and BNB Smart Chain (formerly known as Binance Smart Chain). Today, by combining the security and relative pseudonymity afforded by cryptographic techniques with decentralization and peer-to-peer interactions, blockchain technology appears as a potential alternative to some of the highly centralized structures of today's internet. This helps explain blockchain's rapid global diffusion and enduring appeal, despite its technical complexity and the considerable computational and energy resources it often requires.

A blockchain is a distributed ledger system[1] that enables the creation of permanent, tamper-resistant records of transactions without reliance on a central authority, such as a government agency or bank. In blockchain networks,[2] transactions are recorded in blocks that are linked cryptographically and replicated across a network of nodes. Participants collectively validate, record, and maintain transaction data in accordance with predefined protocol rules.[3] Nodes maintain a replicated, continuously synchronized copy of the ledger, using consensus mechanisms to ensure agreement on the state of the system and to safeguard the integrity of the information it contains.

1 A distributed ledger is "a type of distributed database that records transactions between entities." This database is shared and synchronized across multiple locations, institutions, people, etc., as opposed to centralized databases. The phrase "distributed ledger technology" refers to a technology that "enables the realization and operation of distributed ledgers." Ali Sunyaev, Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies 269 (2020). *See also* Christina Majaski, Distributed ledgers: Definition, how they're used, and potential, *Investopedia* (Sep. 20, 2024), https://www.investopedia.com/terms/d/distributed-ledgers.asp.

2 *Tchatchou v. India Globalization Cap., Inc.*, No. PWG-18-3396, 2021 WL 307415, at 2 (D. Md. Jan. 29, 2021), https://www.govinfo.gov/content/pkg/USCOURTS-mdd-8_18-cv-03396/pdf/USCOURTS-mdd-8_18-cv-03396-1.pdf ("Blockchain is defined as 'a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network."); *see also* Carla L. Reyes, *The Language Landmines of Blockchain and Cryptocurrency,* in The Cambridge Handbook on Law and Policy for NFTs (Nizan Geslevich Packin ed., 2024), https://www.cambridge.org/core/books/abs/cambridge-handbook-of-law-and-policy-for-nfts/language-landmines-of-blockchain-technology-and-cryptocurrency/BFCD2B92B267624AD3A5F8F930B73F99.

3 The protocol is the fundamental set of rules and standards that govern communication and operations between nodes in a blockchain network, including consensus mechanisms, transaction validation, and data propagation. In other words, a 'protocol' refers to the set of rules—encoded in software—that govern how participants interact, validate transactions, and update the state of the blockchain. *See DeFi Education Fund*, Dictionary, https://www.defieducationfund.org/our-mission/ (last visited Jan. 15, 2026).

A core aim of blockchain technology is to provide an alternative to traditionally trusted institutions —such as banks and other financial intermediaries— by enabling peer-to-peer exchanges without requiring any single intermediary to be trusted.[4] Bitcoin, for instance, was designed explicitly to enable peer-to-peer financial transactions on a global scale without dependence on centralized financial institutions. In 2008, the Bitcoin white paper *(See Figure 1)* proposed "a system of electronic transactions [that does not rely] on trust."[5] The characterization of blockchain as a "trustless" system does not mean that blockchain *eliminates* trust; it *reallocates* trust —from institutions to protocol rules, economic incentives, and collective network governance.

Today, blockchain is widely viewed as a foundational infrastructure for decentralized networks, providing the technical basis for new forms of governance, coordination, and value exchange. Supporters often present it as a means of fostering more open, participatory, and equitable digital environments.[6] At the same time, blockchain underpins the crypto-asset industry, which critics repeatedly admonish for facilitating the movement of substantial funds associated with scams, market manipulation, and other forms of illicit activity.[7]

1.1. FROM CRYPTO ANARCHISTS TO WEB3

Timothy C. May articulated the vision of a "crypto anarchy" in his 1988 *Crypto Anarchist Manifesto*[8] and later elaborated on it in the 1994 *Cyphernomicon*.[9] May argued that strong cryptography and decentralized networks would make certain forms of state control —particularly financial surveillance and taxation— technically difficult, if not impossible, to enforce. His claim was not only normative but predictive: Cryptographic tools, he maintained, would alter the practical capacity of governments to regulate economic and social life. These ideas were expressed through the "Cypherpunks" mailing list.[10] There, programmers and activists developed anonymity tools, digital cash experiments, and decentralized communication systems, seeking to translate political philosophy into functional code. For May and other crypto anarchists, writing code was not merely a technical activity but a political act: Deploying cryptography was a means of circumventing centralized authority and traditional legal constraints.

At the time, crypto anarchist and cypherpunk thinkers built on the earlier work of David Chaum,[11] whose pioneering research in the 1980s demonstrated that cryptographic tools could enable untraceable payments

4 Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (Dec. 2015) (manuscript at 7), https://associazioneblockchain.it/wp-content/uploads/2015/12/SSRN-id2709713.pdf.

5 *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 8, (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf. *See also* Elissar Toufaily & Tatiana Zalan, *In Blockchain We Trust? Demystifying the "Trust" Mechanism in Blockchain Ecosystems*, 206 Tech. Forecasting & Soc. Change 1 (2024) (summarizes existing critique of blockchain and argues that the nature of the technology currently creates trust issues). https://www.sciencedirect.com/science/article/abs/pii/S0040162524003706.

6 E. Johanna Hartelius, *The Great Chain of Being Sure About Things: Blockchain, Truth, and a Trustless Network*, 23 Rev. Commc'n 21 (2023), https://www.tandfonline.com/doi/full/10.1080/15358593.2022.2112270.

7 David Yaffe-Bellany et al., *The Crypto Industry's $28 Billion in 'Dirty Money'* N.Y. Times, (Nov. 17, 2025), https://www.nytimes.com/2025/11/17/technology/crypto-exchanges-dirty-money.html?nl=The+Morning.

8 Timothy C. May, *The Crypto Anarchist Manifesto* (1988), https://perma.cc/7U4C-RMUB. *See also* Eric Hughes, *A Cypherpunk's Manifesto* (Mar. 3, 1993), https://www.activism.net/cypherpunk/manifesto.html.

9 Timothy C. May, *The Cyphernomicon: Cypherpunks FAQ and More* (version 0.666, Sept. 10, 1994), https://cdn.nakamotoinstitute.org/docs/cyphernomicon.txt.

10 For a comprehensive account of the cypherpunk ideology, see Craig Jarvis, *Cypherpunk Ideology: Objectives, Profiles, and Influences (1992-1998)*, Internet Histories, 6:3, 315-342, https://doi.org/10.1080/24701475.2021.1935547.

11 *See, e.g.*, David Chaum, Blind Signatures for Untraceable Payments, *in* Advances in Cryptology: Proceedings of Crypto 82 199, 199 (David Chaum, Ronald L. Rivest & Alan T. Sherman, eds., Springer 1983), https://doi.org/10.1007/978-1-4757-0602-4_18.

and protect privacy. Chaum's primary concern was shielding citizens from excessive government and corporate surveillance by enabling transactions to occur without disclosing the identity of the parties involved.[12] The crypto anarchists extended these technical insights into a broader political philosophy: the conviction that cryptography could be used to limit centralized authority and enable new forms of individual freedom.[13] They provided the conceptual and technical foundation for Bitcoin, which combined Chaum's cryptographic principles with the crypto-anarchist ambition of creating a censorship-resistant, decentralized financial system.

These intellectual and technical movements laid the groundwork for the emergence of blockchain technology. By combining cryptographic tools with distributed network architectures, blockchain introduced a framework for socio-political and economic interactions that circumvented the need for third-party intermediaries.

1.1.1. The Emergence of Cryptos

In October 2008, an anonymous individual or group, using the pseudonym Satoshi Nakamoto, published the white paper *Bitcoin: A Peer-to-Peer Electronic Cash System (See Figure 1)*.[14] The publication took place in the aftermath of the 2008 global financial crisis, which severely undermined public trust in traditional financial institutions.[15] It described a decentralized transaction system that would operate without intermediaries and record all activity in a publicly accessible, immutable, and verifiable distributed ledger. The white paper criticized the "inherent weaknesses" of trusting traditional financial systems,[16] asserting: "We have proposed a system for electronic transactions without relying on trust."[17] In practice, blockchain does not eliminate trust[18] but redistributes it from centralized institutions to a distributed network of participants, whose collective consensus is aimed at ensuring the system's integrity.[19]

Bitcoin thus appeared to give practical form to a long-standing aspiration within cypherpunk thought: the creation of a decentralized system capable of operating without centralized intermediaries and enforcing its rules through cryptographic consensus rather than institutional adjudication. By embedding core governance functions directly into the protocol, it sought to reduce reliance on traditional legal enforcement mechanisms and to allow transactions to occur with minimal dependence on legacy institutions. Beyond reducing reliance on intermediaries, Bitcoin's distributed architecture was designed to enhance the resilience of the system. By distributing verification and record-keeping across a large number of nodes – rather than concentrating them in a single institution – the network reduces single points of failure and becomes more resistant to censorship, technical disruptions, or targeted attacks.

12 For a sample of Chaum's scholarship concerning surveillance, see David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, 28 Commc'ns ACM 1030 (1985); https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf.

13 See generally Kelsie Nabben, *Cryptoeconomics as Governance: An Intellectual History from 'Crypto Anarchy' to 'Cryptoeconomics',* 7 Internet Hists. 254 (2023), https://doi.org/10.1080/24701475.2023.2183643.

14 See generally Nakamoto, *supra* note 5.

15 Bitcoin's genesis block included a reward of 50 bitcoins. It also included a coinbase message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This line quoted the headline of a *London Times* article published on January 3, 2009, reporting the British government's bailout of banks. Many interpret it as a commentary on the motivation behind Bitcoin: to bypass traditional banks and intermediaries, creating a currency controlled by users rather than financial institutions. Benedict George, *The Genesis Block: The First Bitcoin Block*, for CoinDesk (January 3, 2023), https://www.nasdaq.com/articles/the-genesis-block:-the-first-bitcoin-block. *See also* Don Tapscott & Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World, 112 (2018).

16 Nakamoto, *supra* note 5, at 1.

17 *Id.* at 8.

18 Eugenia Politou et al., *Blockchain Mutability: Challenges and Proposed Solutions*, 9 IEEE Transactions on Emerging Topics in Computing 1972, 1973 (2019) https://ieeexplore.ieee.org/document/8883080.

19 Moritz Becker & Balázs Bodó, *Trust in Blockchain-Based Systems*, 10 Internet Pol'y Rev. 1, 5-6 (2021), https://doi.org/10.14763/2021.2.1555.

FIGURE 1.

The Bitcoin white paper

In the Bitcoin white paper, an anonymous individual or group operating under the pseudonym Satoshi Nakamoto introduced the concept of a decentralized, peer-to-peer electronic cash system secured through cryptographic techniques.[20] The proposal aimed to enable the verification and recording of transactions without relying on a trusted intermediary.[21]

Bitcoin is designed to enable the transfer of value (denominated in units called bitcoins) between parties who do not know or trust one another.[22] At its core, Bitcoin relies on a public ledger (the *blockchain*) that records and validates transactions across a globally distributed network of *nodes*. Transactions are digitally signed, timestamped,[23] grouped into blocks and recorded permanently and sequentially in a linear "chain."[24] Blocks are added to the ledger through a *consensus mechanism*[25] based on proof-of-work mining, in which network participants compete to validate transactions and append new blocks to the chain.[26] Once added, transactions become practically irreversible, as altering the transaction history would require controlling a substantial share of the network's computational power.

Through this design, trust is no longer vested in a central authority but, instead, is distributed across the network's participants.[27] Bitcoin thus constitutes a decentralized, peer-to-peer payment system that seeks to reduce reliance on intermediaries and to enable value transfers in an environment characterized by limited mutual trust.

Bitcoin went live in January 2009. The Bitcoin network was designed to maintain a verifiable record of ownership of digital assets known as "bitcoins" and to share this record among multiple participants. Adoption was modest at first, but the network gradually expanded and, in 2010, the network recorded its first real-world transaction: the purchase of two pizzas for 10,000 bitcoin (BTC).[28] Developers soon began experimenting with alternatives to Bitcoin, creating "altcoins,"[29] such as Litecoin,[30]

20 Nakamoto, *supra* note 5, at 1.

21 Melanie Swan, Blockchain: Blueprint for a New Economy 2 (2015); Michael J. Casey & Paul Vigna, *In Blockchain We Trust*, MIT Tech. Rev. (Apr. 9, 2018), https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/; Teck Ming Tan & Saila Saraniemi, *Trust in Blockchain-Enabled Exchanges: Future Directions in Blockchain Marketing*, 51 J. Acad. Mark. Sci. 914, 917-18 (2022), https://doi.org/10.1007/s11747-022-00889-0.

22 The best references for a full account of Bitcoin are the white paper (https://bitcoin.org/bitcoin.pdf) and the public GitHub repository (https://github.com/bitcoin/bitcoin).

23 Hash values are unique digital signatures that verify the authenticity of blockchain transactions. Howard Poston, *Hash Functions in Blockchain*, Infosec Institute (Sept. 29, 2020), https://www.infosecinstitute.com/resources/blockchain-security-overview/hash-functions-in-blockchain/.

24 Nakamoto, *supra* note 5, at 3.

25 There are two main types of consensus protocols: proof of work and proof of stake. Bitcoin utilizes a proof of work consensus protocol. Daniel Krawisz, *The Proof-of-Work Concept*, Satoshi Nakamoto Institute (June 24, 2013), https://nakamotoinstitute.org/mempool/the-proof-of-work-concept. For a detailed discussion of consensus protocols, *see* section 2.3 of this report.

26 Network participants in proof-of-work consensus protocols are incentivized to validate transactions through a process known as "mining," enabling them to earn rewards of cryptocurrencies. Nakamoto, *supra* note 5, at 2-3.

27 Sinclair Davidson, Primavera De Filippi & Jason Potts, *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology* (July 22, 2016) (manuscript at 2, 21), https://dx.doi.org/10.2139/ssrn.2811995.

28 Alan Suderman, *15 Years Ago, a Software Developer Paid for Two Pizzas with 10,000 Bitcoin. Those Pies Would Be Worth $1.1 Billion Today*, Fortune (May 22, 2025), https://fortune.com/article/pizza-bitcoin-day-story-laszlo-hanyecz-papa-johns-pizzas-value/.

29 The Investopedia Team, *Understanding Altcoins: Types, Benefits, and Market Potential*, Investopedia (Aug. 10, 2025), https://www.investopedia.com/terms/a/altcoin.asp.

30 *The Cryptocurrency for Payments*, Litecoin, https://litecoin.org/ (last visited Jan. 15, 2026).

Namecoin,[31] and Peercoin.[32] These alternatives tested variations in consensus mechanisms, supply models, and block times (the average amount of time it takes to create and add a new block to the chain). And they gave rise to new fundraising mechanisms. In July 2013, Mastercoin, later renamed Omni, conducted what is widely regarded as the first Initial Coin Offering (ICO),[33] raising approximately 5,000 bitcoins by selling digital assets directly to investors. This innovation laid the foundation for a fundraising model that would soon dominate the sector.

Ethereum, the second most active blockchain behind Bitcoin,[34] launched its ICO in 2014,[35] which marked a decisive turning point in the industry. It raised over $18 million worth of bitcoin and helped popularize the ICO model ahead of its wider adoption. When the Ethereum network launched in July 2015, it introduced a flexible scripting language that enabled decentralized applications (dApps). These software programs could encode rules and automate interactions on the blockchain. This development expanded blockchain's potential far beyond cryptocurrency, opening up new possibilities for decentralized finance (DeFi), token issuance,[36] and decentralized governance.

Between 2016 and 2017, the Initial Coin Offering phenomenon exploded.[37] Thousands of projects raised billions of dollars by selling digital tokens directly to investors and bypassing traditional venture capital. The frenzy reached its peak in 2017–2018, when projects often raised millions of dollars within minutes, despite offering little more than a white paper as a justification for their technological promise.[38] Regulatory authorities, most prominently the U.S. Securities and Exchange Commission (SEC), determined that many of these tokens constituted unregistered securities[39] *(See below section 7.2.2.A.)*. Combined with a broader market correction, these interventions exposed numerous fraudulent or technically infeasible projects, bringing the ICO boom to an end. The regulatory crackdown on token sales, however, did not halt innovation in blockchain-based financial services. Instead, developers shifted their focus from fundraising mechanisms to building functional protocols for peer-to-peer finance. The DeFi ecosystem continued to expand rapidly, developing protocols for lending, borrowing, and decentralized exchanges.

In parallel, blockchain applications extended into new domains. Non-Fungible Tokens (NFTs) *(See below section 2.4.2.)*, which represent unique digital assets such as artwork, music, or virtual real estate, gained prominence on Ethereum. The NFT boom,[40] which began in late 2020 and peaked in 2021, transformed digital art and collectibles into a multi-billion-dollar market. While characterized by both artistic experimentation

31 *Namecoin*, https://www.namecoin.org/ (last visited Jan. 15, 2026).

32 *The Pioneer of Proof-of-Stake*, Peercoin, https://www.peercoin.net/ (last visited Jan. 15, 2026).

33 Moe Adham, *The Ongoing Evolution of the ICO*, Forbes (Nov. 27, 2018), https://www.forbes.com/councils/forbesfinancecouncil/2018/11/27/the-ongoing-evolution-of-the-ico/.

34 See *What is Ethereum?* Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-ethereum (last visited Jan. 15, 2026).

35 Robert D. Knight, *10 Years on: How Ethereum's ICO Changed the Crypto Landscape*, COIN TELEGRAPH (July 23, 2024), https://cointelegraph.com/news/10-years-ethereum-ico-crypto-landscape.

36 On tokens, see section 2.4.1.B.

37 Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, 60 HARV. INT'L L.J. 269 (2019), https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/3_ICO_60.2.pdf.

38 Magnus Schückes & Tobias Gutmann, *Why Do Startups Pursue Initial Coin Offerings (ICOs)? The Role of Economic Drivers and Social Identity on Funding Choice*, 57 Small Business Economics 1027 (2021), https://doi.org/10.1007/s11187-020-00337-9.

39 Jay Clayton, Chairman, Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings, U.S. Securities and Exchange Comm. (Dec. 11, 2017), https://www.sec.gov/newsroom/speeches-statements/statement-clayton-2017-12-11.

40 Clive Thompson, *The Untold Story of the NFT Boom*, N.Y. Times (May 12, 2021), https://www.nytimes.com/2021/05/12/magazine/nft-art-crypto.html.

and speculative excess, NFTs demonstrated how blockchain could establish verifiable digital ownership. After prices collapsed in 2022,[41] attention shifted toward more utilitarian applications, including event ticketing, intellectual property rights, and gaming assets. More recently, meme coins *(See section 2.4.1.D.)* have proliferated, sometimes with explicitly political overtones. Tokens such as $TRUMP[42] and $LIBRA, associated with the current leaders of the United States and Argentina,[43] illustrated how blockchain-based assets could be employed as tools of political identity and expression.

Meanwhile, spectacular failures, bankruptcies, and frauds have regularly punctuated the industry's growth. Early scandals included the illicit marketplace Silk Road in 2013 *(See Figure 38)*,[44] the collapse of the Mt. Gox exchange in 2014 *(See Figure 45)*,[45] and fraudulent schemes such as OneCoin *(See section 5.2.2.B.1)*[46] and BitConnect *(See Figure 41)*.[47] In 2022, the collapse of the Terra/Luna algorithmic stablecoin *(See Figure 27)* triggered a cascade of failures across the crypto ecosystem, including Celsius Network *(See section 5.1.5.B.)*. This sequence of crises culminated in the 2022 collapse of FTX, widely regarded as one of the largest financial frauds in modern history, which profoundly undermined confidence in the cryptocurrency ecosystem.[48] In reaction, some observers dismissed crypto as more speculative than innovative and as structurally insecure,[49] reducing it to little more than a glorified form of gambling[50] or a mass delusion.[51]

Nevertheless, since then, blockchain and cryptocurrency regained momentum and consolidated a committed base of supporters.[52] In the United States, President Donald Trump openly embraced the sector and pledged to make the country "the crypto capital of the planet and the bitcoin superpower of the world"[53] *(See below section 7.2.4.)*.

---

41 Sidhartha Shukla, *NFT Trading Volumes Collapse 97% From January Peak*, BLOOMBERG (Sept. 28, 2022) https://www.bloomberg.com/news/articles/2022-09-28/nft-volumes-tumble-97-from-2022-highs-as-frenzy-fades-chart.

42 Nic Tse, *What Is the TRUMP meme coin? How to buy TRUMP in the US,* CRYPTO.COM, https://crypto.com/us/crypto/learn/what-is-the-trump-meme-coin (last visited Jan. 15, 2026).); Ignacy Nieweglowski, Aviv Yaish, Fahad Saleh & Fan Zhang, *PoliFi Tokens and the Trump Effect* (Dec. 2025) (unpublished manuscript), ARXIV (2025), https://arxiv.org/abs/2512.06036.

43 In February 2025, Argentina's President Milei promoted a little-known cryptocurrency called $LIBRA on social media. Its price skyrocketed before crashing within hours, wiping out millions of dollars in investments from both domestic and international holders. BUENOS AIRES TIMES *Congress report into '$LIBRA' scam accuses Milei of alleged crypto fraud,* (Nov. 19, 2025), https://www.batimes.com.ar/news/argentina/congress-report-into-libra-scam-accuses-milei-of-alleged-crypto-fraud.phtml.

44 *Ross William Ulbricht's Laptop*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop (last visited Jan. 15, 2026).

45 The Investopedia Team, *Mt Gox Explained: History, 2014 Collapse, and Current Status,* INVESTOPEDIA (Oct. 4, 2025), https://www.investopedia.com/terms/m/mt-gox.asp.

46 Press Release, U.S. ATT'Y'S OFF., S.D.N.Y., *Co-Founder of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced to 20 Years in Prison* (Sept. 12, 2023), https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison.

47 Press Release, U.S. DEP'T OF JUST., OFF. OF PUB. AFFS., *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme* (Feb. 25, 2022), https://www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

48 Forbes Staff, *The Collapse of FTX*, FORBES, https://www.forbes.com/sites/forbesstaff/article/the-fall-of-ftx/ (last visited Jan. 15, 2026). *See also*: Lucas Ropek, *SBF Is Headed to Prison But FTX Will Haunt the Crypto Community For Years*, GIZMODO (Nov. 3, 2023), https://gizmodo.com/ftx-fbi-sam-bankman-fried-cryptocurrency-data-1850990825; Alexander Osipovich, *Sam Bankman-Fried Verdict Reflects Crypto's Broken Dreams*, WALL ST. J. (Nov. 4, 2023), https://www.wsj.com/finance/sam-bankman-fried-verdict-reflects-cryptos-broken-dreams-bd1a6081; Thomas Conlon, Shaen Corbet & Yang Hu, *The Collapse of FTX: The End of Cryptocurrency's Age of Innocence*, DUBLIN CITY UNIV. BUS. SCH. RESEARCH PAPER (Dec. 14, 2022), https://ssrn.com/abstract=4283333.

49 Nicholas Weaver, *The Death of Cryptocurrency: The Case for Regulation,* Digital Future Whitepaper Series, INFORMATION SOC'Y PROJECT, YALE LAW SCHOOL (Dec. 2022), https://law.yale.edu/sites/default/files/area/center/isp/documents/weaver_death_of_cryptocurrency_final.pdf.

50 Fabio Panetta, Member of the Executive Board of the ECB, Speech at the 22nd BIS Annual Conference: *Paradise Lost? How Crypto Failed to Deliver on Its Promises and What to Do About It* (June 23, 2023), https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html.

51 *See generally* ZEKE FAUX, NUMBER GO UP: INSIDE CRYPTO'S WILD RISE AND STAGGERING FALL, CROWN CURRENCY, (2023).

52 Daren Matsuoka, et al., *State of Crypto 2025: The year crypto went mainstream*, (Oct. 22, 2025), A16ZCRYPTO, https://a16zcrypto.com/posts/article/state-of-crypto-report-2025/

53 Exec. Order No. 14178, Strengthening American Leadership in Digital Financial Technology, 90 Fed. Reg. 8647 (Jan. 31, 2025) (promoting digital asset innovation and establishing the President's Working Group on Digital Asset Markets); Exec. Order No. 14233, Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile, 90 Fed. Reg. 11789 (Mar. 11, 2025); Joint Stipulation to Dismiss and Releases, *SEC v. Coinbase, Inc.*, No. 23-cv-4738 (S.D.N.Y. Feb. 27, 2025), ECF No. 176; Joint Stipulation to Dismiss, *SEC v. Payward, Inc.* (Kraken), No. 23-cv-06003 (N.D. Cal. Mar. 27, 2025); Joint Stipulation to Dismiss, *SEC v. Binance Holdings Ltd.,* No. 23-cv-01599 (D.D.C. May 29, 2025) (reflecting the SEC's changed enforcement posture); Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act, Pub. L. No. 119-27, 139 Stat. 419 (2025) (signed into law July 18, 2025).

1.1.2. The Promise of Web3

Blockchain represents far more than digital currencies. It advances a transformative vision of the internet, strengthening user autonomy and challenging the prevailing centralized digital order. It is frequently cast as an instrument of social resistance, purposefully designed to elude state authority and limit the influence of centralized digital platforms and financial intermediaries.[54] Indeed, the initial impetus for decentralization was the desire to circumvent potentially corrupt financial and political institutions. Over time, however, the blockchain movement has increasingly positioned decentralization as a counterweight to the concentration of power in Big Tech, distributing control across a broader network of participants.

Over the past decade and a half, a small number of technology companies have monopolized online infrastructure, particularly in social media. Platforms such as Facebook, Instagram, YouTube, and X (formerly Twitter) have built enormous businesses by monetizing user-generated content, while capturing a disproportionate share of the economic value generated by user activity.[55] These corporations have established near-total control over digital ecosystems, managing critical services such as digital identity and online transactions. Their business model relies on extensive data collection. By harvesting and analyzing user information, they create detailed profiles primarily to enable targeted advertising, effectively turning user interactions into a commodity that can be sold to advertisers.[56]

Blockchain technology, by contrast, offers the prospect of a more democratic digital future through a decentralized alternative,[57] which constitutes the fundamental promise of "Web3."[58] Gavin Wood introduced the term Web3 (initially Web 3.0) in 2014, shortly after he co-founded Ethereum.[59] To its proponents, Web3 represents the next stage of the internet and, potentially, a new mode of social and economic organization. At its most basic level, it denotes a decentralized online ecosystem where services and applications are not controlled by a single corporate actor. Instead, ownership and governance are distributed among users themselves, who acquire stakes by contributing to the development, operation, or maintenance of these services.

In this narrative, Web 1.0, which emerged in the 1990s, was the era of open, decentralized protocols, when users primarily navigated among static, read-only websites with minimal user interaction.[60] Web 2.0, emerging in the 2000s, developed in an era of "re-centralization," in which a significant share of communication, commerce, and information flowed through closed platforms operated by a small number of dominant corporations —Google, Facebook, Amazon. Web 2.0 introduced interactive platforms and user-generated content, exemplifying what Tim O'Reilly described as an "architecture of

54 Armin Krishnan, *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations*, 13 J. Strat. Sec. 41 (2020) https://www.jstor.org/stable/26907412.

55 *See* Tim Wu, The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity 1 (2025). Tim Wu describes these platforms as "instruments of wealth extraction," arguing that they have transformed the Internet from its original promise of democratization into a system that seizes money, data, and attention from users while concentrating wealth among platform owners.

56 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight For A Human Future At The New Frontier of Power 8 (2019); Tim Wu, The Attention Merchants: The Epic Struggle To Get Inside Our Heads 3 (2016).

57 Vitalik Buterin, *Make Ethereum Cypherpunk Again* (Dec. 28, 2023), https://vitalik.eth.limo/general/2023/12/28/cypherpunk.html.

58 Thomas Stackpole, *What is Web3?* HARV. BUS. REV. (May 10, 2022), https://hbr.org/2022/05/what-is-web3.

59 Gavin Wood played a central role in the creation of Ethereum. He now heads the Web3 Foundation, which funds and supports decentralized technology initiatives, and leads Parity Technologies, a company dedicated to developing blockchain infrastructure for Web3 applications; Gilad Edelman, *The father of Web3 wants you to trust less*, Wired (Nov. 20, 2021), https://www.wired.com/story/web3-gavin-wood-interview/.

60 Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, 1–17 (Yale Univ. Press 2006).

participation"[61] in which users not only consume but actively create and share content.

By contrast, Web3 is presented as a way to break free from the oligopolistic architecture of Web 2.0, where centralized technology corporations control access to critical digital infrastructure, user data, and online interactions.[62] Web3 is envisioned as a decentralized web, aiming to return ownership and control to users and to give individuals greater authority over their digital identities, data, and transactions.[63] Its core features include decentralization, transparency, user ownership, tokenization, and interoperability.[64] While decentralization aims to reduce the domination of large technology companies over data and digital assets, transparency —achieved through open-source protocols and verifiable transactions— fosters trust and accountability. Tokenization —the process of representing assets, rights, or claims in digital form on a blockchain *(See section 4.2)*— introduces new economic models by enabling users to be directly rewarded for their contributions through cryptocurrencies, non-fungible tokens (NFTs), or other digital assets. Interoperability facilitates seamless interaction between different platforms and applications.

The promise of Web3 is well presented in venture capitalist Chris Dixon's recent book entitled *Read Write Own*.[65] The book advances the view that blockchain networks could inaugurate a new stage in the evolution of the internet. Dixon characterizes the early internet as a "read" era in which users primarily accessed information through open protocols, followed by a "read–write" era dominated by centralized corporate platforms. Dixon argues that blockchain-based networks could enable a "read–write–own" phase in which users not only create and consume content but also hold ownership rights over digital assets and participate in protocol governance through token-based mechanisms. According to this perspective, tokenization may enable new forms of digital ownership and economic coordination within online networks.

While blockchain is not the only means of creating such a decentralized, user-controlled internet that reduces reliance on centralized gatekeepers, the term "Web3" is generally understood to refer to an internet built on blockchain technologies. Blockchains provide the technical infrastructure that enables decentralized networks to function without a central authority, thereby supporting Web3's model of distributed ownership and governance. Blockchain systems also provide programmability through smart contracts *(See section 2.5.1)*, which allow developers to encode rules that automatically execute transactions or interactions when predefined conditions are met. Many blockchain systems also rely on governance tokens, which grant the token holders the ability to vote on protocol upgrades or parameter changes within decentralized networks, sometimes through decentralized governance mechanisms implemented in decentralized autonomous organizations *(DAOs, See section 2.5.2.)*.

Decentralization is central to this vision. Decentralized blockchain-based networks diminish reliance on

61 Tim O'Reilly, *The Architecture of Participation*, O'Reilly (2004) https://www.oreilly.com/pub/a/tim/articles/architecture_of_participation.html; *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'Reilly (Sept. 30, 2005), https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html; see *also* Trebor Scholz, *Market Ideology and the Myths of Web 2.0*, 13 First Monday (2008) https://firstmonday.org/ojs/index.php/fm/article/download/2138/1945; Ryan Singel, *Are You Ready for Web 2.0?* Wired (Oct. 6, 2005) https://www.wired.com/2005/10/are-you-ready-for-web-2-0/.

62 "Web1 is a readable-only network, whereas Web2 is a readable and writable network, and Web3 is a readable and writable network that empowers users with data ownership," Renke Huang et al., *An overview of Web3.0 Technology: Infrastructure, Applications, and Popularity*, ArXiv, 3 (2023), https://arxiv.org/abs/2305.00427.

63 Yiwei Lai et al., *Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership,* MDPI, Blockchains 1(2) 111-131 (2023), https://doi.org/10.3390/blockchains1020008; see also David Krause, *The Rise of Web3: Opportunities and Challenges* (July 15, 2024), SSRN, https://ssrn.com/abstract=4895353.

64 See Amazon Web Services, *What is Web3?* https://aws.amazon.com/what-is/web3 (last visited Jan. 15, 2026).

65 Chris Dixon, Read Write Own: Building the Next Era of the Internet (Random House, 2024).

traditional intermediaries, where any transaction — whether of data, information, or value— depends on trusting a centralized operator.[66] By contrast, blockchain systems give participants greater autonomy, effectively displacing conventional gatekeepers across financial, social, and digital interactions. In decentralized systems, smaller stakeholders can participate in governance and economic activity, and decision-making authority is more broadly distributed rather than concentrated in a single entity.[67] This stands in sharp contrast to centralized platforms, where key decisions —such as changes to policies, data-collection practices, or fee structures— are determined by a small group of executives or major shareholders, leaving ordinary users with little or no meaningful influence. Proponents argue that decentralized ecosystems may foster more open-ended and resilient forms of innovation, insofar as multiple independent actors are able to experiment, iterate, and build without restrictive oversight.[68]

A further aspect of this shift concerns privacy and control over personal data. Instead of relinquishing information to corporations that collect and monetize it without meaningful consent, blockchain systems seek to allow individuals to retain control over their data, with access mediated through private encryption keys and user-defined permissions.[69]

Overall, the most enthusiastic advocates of blockchain technology foresee the emergence of a "decentralized society," organized around on-chain identities, tokenized assets, and interconnected digital communities.[70] This vision, however, should be assessed in light of the potential for blockchain ecosystems to generate new concentrations of power and new forms of intermediation and control *(See chapter 3)*.

1.2. CHALLENGES OF BLOCKCHAIN POLICY

As with any major technological innovation, blockchain presents a mix of opportunities and risks. Its potential applications are now well established, while its vulnerabilities —frequently highlighted by the volatility of crypto-assets and the numerous scandals that have marked the crypto industry— have been extensively scrutinized. It is, therefore, unsurprising that policymakers increasingly confront the question of what regulatory stance to adopt and, more fundamentally, whether, when, and how to implement regulation.

Unlike other emerging technologies, such as artificial intelligence, blockchain's distinctive technical architecture makes questions of governance and regulation particularly difficult to address. The decentralization of blockchain networks, the automated execution of transactions, and the cryptographic techniques that enable participants to act with varying degrees of pseudonymity together create significant challenges for legal and policy frameworks. Any attempt to

66 *What Is Web3?* McKinsey & Company (Oct. 10, 2023), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3.

67 Hanna Halaburda, *The hidden danger of re-centralization in blockchain platforms,* Brookings (April 10, 2025), https://www.brookings.edu/articles/the-hidden-danger-of-re-centralization-in-blockchain-platforms/#:~:text=Blockchain%20technology%20was%20envisioned%20as,seen%20in%20traditional%20digital%20monopolies; *see also* Hanna Halaburda, *Blockchain Toolbox for Digital Platforms*, in Cambridge Handbook on Digital Platforms (Jan 19, 2025), https://ssrn.com/abstract=4999550; Ruben Leal Buenfil & Alexander Hernández Romanowski, *Implications of Decentralized Finance for Competition, Antitrust Policy and Economic Growth,* Baker Inst. for Pub. Pol'y (Dec. 1, 2022), https://www.bakerinstitute.org/research/implications-decentralized-finance-competition-antitrust-policy-and-economic-growth.

68 T. Charles Clancy & Sriram Viswanath, *Decentralized Innovation: Approach to Building Multilateral Collaborations in Science and Technology*, 2-4, MITRE Corp. (Sept. 2023), https://www.mitre.org/news-insights/publication/decentralized-innovation-approach-building-multilateral-collaborations.

69 Decentralization makes the network exceptionally resistant to data breaches or unauthorized access, as compromising the system would require controlling the majority of the nodes on the network. *See* Yoan Hermstrüwer, *Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems* 38-39 (Stanford-Vienna Transatl. Tech. L. F., Working Paper No. 49, 2020), https://law.stanford.edu/publications/no-49-the-limits-of-blockchain-democracy-a-transatlantic-perspective-on-blockchain-voting-systems/.

70 *See generally* Puja Ohlhaver, E. Glen Weyl & Vitalik Buterin, *Decentralized Society: Finding Web3's Soul* (May 10, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763.

develop policy approaches for blockchain thus requires confronting foundational questions about how traditional legal systems should understand —and engage with— decentralization and computer code.

Twenty-six years ago, Lawrence Lessig famously argued that "code is law" in cyberspace, insofar as computer code performs regulatory functions comparable to those of formal legal rules *(See section 6.1.1)*.[71] In most contemporary online platforms, however, code remains subject to the control of platform operators, who are themselves embedded within, and constrained by, the legal systems of the jurisdictions in which they are established. Blockchain-based systems present a different configuration. Here, the delegation of authority from human operators to computer code has prompted many commentators to characterize blockchain as a "trustless" technology —one that minimizes reliance on intermediaries and other trusted third parties.[72] The underlying claim is that blockchain replaces trust in a centralized operator with trust in a distributed peer-to-peer network. Accordingly, as long as users retain confidence in the technology —namely, in the network's capacity to function as intended— they need not depend on any external authority.

The widely discussed case of The DAO clearly illustrates the difficulties and challenges inherent in this model. In April 2016, its founders launched The DAO as a blockchain-based decentralized organization *(See section 2.5.2.B. and section 6.2.1.)* without any formal legal personality. Its technical infrastructure consisted exclusively of automated software programs ("smart contracts," *See section 2.5.1.)*. The DAO's primary purpose was to raise cryptocurrencies in order to finance blockchain-based projects and distribute potential profits to token holders.[73] Its operational rules were embedded directly in the software, which executed and enforced them automatically. This novel experiment attracted more than $150 million in ether (ETH) from over 11,000 investors.[74] Within weeks, however, a hacker exploited a vulnerability in the code and extracted approximately one-third of The DAO's assets (about $60 million).[75]

Rather than pursue judicial remedies, the Ethereum community collectively decided to adopt a blockchain update that restored the ledger to its state prior to the attack. The implementation of this decision (a "hard fork," *See Figure 11)* created a new blockchain, effectively reversing the hack-related transactions. Although this operation succeeded in restoring investor funds, it was controversial, as it undermined the fundamental principle of blockchain immutability and resistance to change:[76] Once recorded on the blockchain, transactions should be irreversible. Yet adhering strictly to immutability would have left investors with no effective remedy. The incident

71 *See* Lawrence Lessig, *The Laws of Cyberspace* (Taiwan Net conference, 1998), https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf; Lawrence Lessig, *Code: and Other Laws of Cyberspace* 3 (1999) https://lessig.org/images/resources/1999-Code.pdf; Lawrence Lessig, *Lawrence Lessig on the Increasing Regulation of Cyberspace*, Harv. Mag. (Jan. 1, 2000), https://www.harvardmagazine.com/2000/01/code-is-law-html; Lawrence Lessig, Code: and Other Laws of Cyberspace Version 2.0, (Basic Books 2006) (Ch. 7 "What Things Regulate").

72 Nakamoto, *supra* note 5; *but see* Gili Vidan & Vili Lehdonvirta, *Mine the gap: Bitcoin and the maintenance of trustlessness*, 21 New Media & Soc'y 42 (2019), https://ssrn.com/abstract=3225236, arguing that a "promissory gap" exists between the promise of trustlessness and Bitcoin's practical operations; *also see* Primavera De Filippi et al., *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, 62 Tech. in Soc'y 101284 3-7 (2020), https://www.sciencedirect.com/science/article/pii/S0160791X20303067.

73 As the founders put it, their goal was to "blaze a new path in business for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of unstoppable code", *See* Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 34-81207, 117 SEC Docket 745 (July 25, 2017) [hereinafter SEC Investigative Report: The DAO], at 5 https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

74 *See Ethereum DAO Hack*, Bitstamp Learn (July 17, 2023), https://www.bitstamp.net/learn/crypto-101/ethereum-dao-hack/; Robert Morrison, Natasha C. H. L. Mazey & Stephen C. Wingreen, *The DAO Controversy: The Case for a New Species of Corporate Governance*, 2 Frontiers Blockchain 1, 6 (2020), https://doi.org/10.3389/fbloc.2020.00025.

75 SEC Investigative Report: The DAO, see *supra* note 73, at 9.

76 Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. Times (June 18, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html.

demonstrated that the security and governance of blockchain systems cannot be reduced to code alone.[77]

Ultimately, the continuity of the Ethereum network rested on collective decision making outside the software's predetermined rules.[78] Yet The DAO incident also surfaced a series of fundamental legal questions *(See section 6.2.1)*. Could the attacker —who exploited a flaw in the code— truly be said to have acted unlawfully if his conduct remained within the technical parameters of the system? Could investors plausibly seek compensation from the code's authors and, if so, how would that work, given that developers often remain anonymous or dispersed across jurisdictions? Even assuming their identities were known, which courts would have jurisdiction and which substantive laws would apply to a borderless, decentralized network? By bringing these questions into sharp relief, The DAO case became one of the earliest and clearest illustrations of the profound challenges that blockchain governance poses for legal systems attempting to apprehend it. It also underscored that the maxim "code is law" holds only to the extent that it is supported —and, when necessary, overridden— by social consensus. At the same time, the hard fork that followed was exceptional rather than representative, as later major exploits have generally not led to similar protocol-level reversals.

Of course, these questions are far from the only challenges faced by policymakers seeking to understand and regulate blockchain technology. Detractors frequently criticize the crypto ecosystem for enabling dramatic losses stemming from extreme asset volatility, pervasive scams, high-profile corporate failures, and illicit activities facilitated by the pseudonymity afforded by cryptography *(See section 2.6.1.)*. They increasingly contest the democratizing aspirations of decentralized networks in light of governance practices that erode democratic principles by concentrating influence in the hands of a small elite.[79] This process of "re-centralization,"[80] whereby decentralized networks become increasingly shaped and dominated by the interests of a limited group, creates a new class of powerful actors who closely resemble the very intermediaries blockchain was designed to bypass *(See section 3.3)*. Moreover, like traditional digital platforms, many blockchain ecosystems also exhibit strong network effects: The value of a protocol tends to increase as more users, developers, and applications build on it, which can create forms of technological lock-in and reinforce the dominance of early or widely adopted networks.

Ultimately, the challenge for policymakers lies in ensuring that blockchain systems operate in accordance with principles of transparency, fairness, and accountability, while at the same time protecting users from the most acute risks —foremost among them being the risk of losing the funds they invest in crypto-assets.

1.3. POSSIBLE POLICY APPROACHES

Blockchain's technical characteristics require policymakers to anchor their strategies in carefully designed methodological frameworks. This need arises not only from the features of the technology itself, but also from the fact that blockchain infrastructures are decentralized, operate across jurisdictions, and partially escape traditional territorial and institutional control.

77 While "the idea of a perfectly neutral, self-patrolling system is appealing, high-profile mishaps have cast doubt on the idea that code is a sufficient form of regulation on its own —or that it is immune to human mistakes and manipulation." Ephrat Livni, *For Rules in Technology, the Challenge is to Balance Code and Law*, N.Y. Times (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/business/dealbook/cryptocurrency-code-law-technology.html.

78 *Id*.

79 Clara Jammot, *The Tech Elites' Takeover of Crypto Is a Growing Threat to European Democracy*, Tech Policy Press (July 3, 2025), https://www.techpolicy.press/the-tech-elites-takeover-of-crypto-is-a-growing-threat-to-european-democracy/.

80 Halaburda, *supra* note 67.

Regulatory choices must also take into account the diversity of blockchain architectures. Several distinct approaches may therefore be envisaged.

1.3.1. Regulating or Not Regulating?

For policymakers, choosing an appropriate strategy for addressing an emerging technology becomes particularly difficult when its risks and future evolution remain uncertain. One option is a *laissez-faire* approach, in which governments allow innovation to unfold with minimal interference, assuming that market forces will naturally support economic growth and help correct early inefficiencies. At the opposite end of the spectrum, policymakers may adopt a more interventionist stance, requiring private actors to comply with predefined rules or standards designed to mitigate existing or foreseeable risks.

1.3.1.A. Self-Regulation

For policymakers, a laissez-faire approach consists in relying on markets and private actors to steer the development of an innovation. While such freedom may indeed accelerate innovation, it does not necessarily give rise to self-regulation —understood as a process in which firms within a sector collectively agree to follow shared rules, standards, or principles.[81] In theory, self-regulation enables those with the greatest technical expertise and practical experience to design realistic and effective governance standards. Yet, relying on self-regulation presupposes that stakeholders in the blockchain industry are well-placed to anticipate and assess risks and have sufficient incentives to address them. These assumptions do not consistently hold in practice.

At present, there is little evidence of industry-wide coordination within the blockchain ecosystem to develop best-practice standards for risk governance or to establish shared codes of conduct. Several organizations have nevertheless emerged to participate in policy debates surrounding the regulation of crypto-assets. Some function primarily as industry lobbying groups representing the interests of market participants, such as the Blockchain Association,[82] and the Crypto Council for Innovation (CCI);[83] the European Crypto Initiative (EUCI);[84] and INATBA[85] in the European Union; and Global Digital Finance (GDF)[86] and CryptoUK[87] in the United Kingdom. Other organizations engage more specifically in policy advocacy or strategic litigation relating to digital assets. For example, Coin Center[88] has been active in litigation concerning the U.S. sanctions imposed on the Tornado Cash protocol *(See section 6.5.3.)*,[89] while the DeFi Education Fund[90] participated as amicus curiae in litigation affecting decentralized finance.[91] While these organizations play an important role in shaping

81 Florence G'sell, *Regulating Under Uncertainty: Governance Options for Generative AI* 16 (Stanford Cyber Policy Ctr., 2024), https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai.

82 Blockchain Ass'n, *Policy*, https://theblockchainassociation.org/policy/ (last visited Jan. 15, 2026).

83 Crypto Council for Innovation, *Policy*, https://cryptoforinnovation.org/policy (last visited Jan. 15, 2026).

84 *See generally* European Crypto Initiative, Policy Documents, https://eu.ci/advocacy/ (last visited Jan. 15, 2026).

85 Int'l Ass'n for Trusted Blockchain Applications, https://inatba.org/policy/inatba-has-issued-a-public-position-on-the-international-organization-of-securities-commissions-ioscos-policy-recommendations-for-crypto-and-digital-asset-markets/ (last visited Jan. 15, 2026).

86 Global Digital Finance, *Standards*, https://www.gdf.io/code-standards/ (last visited Jan. 15, 2026).

87 CryptoUK, *Publications*, https://cryptouk.io/publications/ (last visited Jan. 15, 2026).

88 Coin Center, *About*, https://www.coincenter.org/about/ (last visited Jan. 15, 2026).

89 Shalini Nagarajan, *Coin Center Sues Over Treasury's Tornado Cash Sanctions*, Blockworks (Oct. 13, 2022), https://blockworks.com/news/coin-center-sues-over-treasurys-tornado-cash-sanctions.

90 DeFi Education Fund, https://www.defieducationfund.org/ (last visited Jan. 15, 2026).

91 DeFi Education Fund, Litigation Contributions, https://www.defieducationfund.org/docs/legal/litigation-contributions/ (last visited Jan. 15, 2026).

regulatory debates, they do not typically produce binding governance standards or enforceable codes of conduct that could amount to genuine industry self-regulation.

More significantly, leading international standard-setting bodies have launched extensive standard-development initiatives related to blockchain and distributed ledger technologies.[92] They include the International Organization for Standardization,[93] the International Telecommunication Union's Telecommunication Standardization Sector,[94] the Institute of Electrical and Electronics Engineers,[95] and the World Wide Web Consortium.[96] They have established dedicated committees and working groups and already have published several blockchain-related international standards. While these efforts contribute to the global standardization of blockchain technologies, they focus primarily on technical specifications and interoperability requirements, rather than on governance or risk-management standards of the kind associated with self-regulation.

Yet decentralized forms of voluntary standard setting exist on blockchain systems. The Ethereum network, for example, develops and updates technical standards through an open process known as Ethereum Improvement Proposals (EIPs). Through this process, developers and community members propose, debate, and refine protocol changes *(See section 3.1.3.)*. Several widely adopted token standards —such as ERC-20 for fungible tokens *(See section 2.4.1.B.)* and ERC-721 for non-fungible tokens *(See section 2.4.2.A.)*— have emerged from this process. Although participation is voluntary, these standards have become de facto technical norms that facilitate interoperability across applications and services built on the Ethereum ecosystem. However, these mechanisms primarily lead to the adoption of technical standards designed to ensure interoperability and protocol functionality. They do not constitute self-regulation in the strict sense, as they do not establish enforceable governance rules or collective commitments regarding risk management, market conduct, or user protection.

Moreover, on blockchain systems, powerful stakeholders — cryptocurrency exchanges, custodial wallet providers, and major merchants— decide whether to support or reject protocol upgrades, which significantly influence how the systems evolve *(See section 3.1.3.)*. This influence is not a form of self-regulation aimed at responsible innovation; rather, it reflects business priorities. These actors typically privilege performance, user demand, and profitability over risk mitigation or broader public-interest considerations, raising concerns about the concentration of influence in entities that lack formal accountability mechanisms.

1.3.1.B. Government Regulation

Another option for policymakers is to rely on regulation in its traditional form —that is, the adoption of statutes or other binding legal frameworks.[97] This path is far from straightforward, particularly when lawmakers lack the technical expertise needed to understand complex

92 Xiaoyun Jia, et al., *International Standardization of Blockchain and Distributed Ledger Technology: Overlaps, Gaps and Challenge* 137(2) Computer Modeling in Eng'g & Scis. 1491-1523 (2023), https://www.techscience.com/CMES/v137n2/53354/pdf; see *also* The Global Standards Mapping Initiative (GSMI), which was a project by the World Economic Forum and the Global Blockchain Business Council to provide a comprehensive overview of blockchain technical standards: World Econ. Forum & Glob. Blockchain Bus. Council, *Global Standards Mapping Initiative: An Overview of Blockchain Technical Standards* (2020), https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf.

93 Int'l Org. for Standardization, *ISO/TC 307 - Blockchain and Distributed Ledger Technologies*, https://www.iso.org/committee/6266604.html (last visited Jan. 15, 2026).

94 Int'l Telecomm. Union, *Focus Group on Application of Distributed Ledger Technology*, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx (last visited Jan. 15, 2026).

95 Inst. of Elec. & Elecs. Eng'rs, *Standards*, https://blockchain.ieee.org/standards (last visited Jan. 15, 2026).

96 World Wide Web Consortium, *Blockchain Community Group*, https://www.w3.org/community/blockchain/ (last visited Jan. 15, 2026).

97 Florence G'sell, *Regulating Under Uncertainty: Governance Options for Generative AI* 20 (Stanford Cyber Policy Ctr., 2024), https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai.

domains such as blockchain. They must, therefore, seek external experts to obtain the information required for drafting well-adapted regulations. In doing so, however, excessive reliance on industry actors risks exposing regulators to biased or incomplete input, potentially leading to legal frameworks that reflect private interests more than the public good. At the same time, contributions from industry and from highly specialized technical experts are indispensable in a rapidly evolving technological environment, where the aim is to design rules that are informed, proportionate, and capable of being updated as the technology changes. Expertise is equally crucial for enforcement: Without specialists capable of monitoring technological developments in real time, effective oversight becomes extremely difficult.

Only close collaboration between regulators and the industry can address these challenges so as to secure balanced and accurate expertise. Yet, in the blockchain ecosystem, this cooperation is hard to implement because it is often unclear who the appropriate interlocutors are. Some prominent actors —such as major foundations (e.g., the Ethereum Foundation), large centralized exchanges (e.g., Coinbase or Binance), custodians and infrastructure providers (e.g., Ledger), or the developers of leading dApps and DeFi protocols (e.g., MakerDAO, Uniswap Labs)— can certainly serve as useful counterparts in discussions aimed at developing appropriate rules and standards. However, these major players represent only a fraction of the ecosystem. The broader blockchain landscape is composed of a multitude of independent and often anonymous participants, which makes it difficult to identify all relevant actors and reflects the highly decentralized nature of participation.

Despite these difficulties, policymakers may still decide to regulate. This choice may arise from the need to create new, carefully tailored legal categories that provide legal certainty and ensure that transactions produce their intended effects. For example, the legal status of "smart contracts" *(See section 6.5.)* or Decentralized Autonomous Organizations *(See section 6.4.)* must be clarified. More generally, regulation tends to be more effective than self-regulation in ensuring safety and mitigating harm. When well designed, regulatory frameworks can offer meaningful oversight and help steer the development of new technologies.

However, choosing to regulate also requires determining *how* to regulate. The legislator's first task is to identify the objectives the law should pursue. Should it articulate core principles through a principles-based approach? Or should the drafters take a more pragmatic stance, focusing primarily on risk mitigation through a risk-based approach? These approaches are not mutually exclusive, but each raises distinct considerations. Further questions soon arise: On whom should the law impose obligations? This question is particularly difficult in the blockchain context, where networks lack centralized servers and many key participants are anonymous and have no territorial anchor.

In fact, an established method for governing online activity is concentrating regulatory efforts on strategic gateways and chokepoints.[98] This approach emerged in the early decades of internet governance, when policymakers realized that direct regulation of end users was largely impractical on highly distributed networks, particularly in the absence of clear jurisdictional anchors *(See section 6.1.)*.[99] Consequently, regulators directed their attention to a limited set of intermediaries — internet service providers, hosting providers, payment

98 Natasha Tusikov, Chokepoints: Global Private Regulation on the Internet, Ch. 6, "Changing the Enforcement Paradigm." (Univ. of Cal. Press 2017).

99 David R. Johnson & David Post, *Law and Borders - The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370–76 (1996), https://yalelawtech.org/wp-content/uploads/2011/08/riseofcyberlaw.pdf.

processors—[100] and other actors who operate at critical junctures where identities are verified, data must pass, or financial transactions are executed. Because these intermediaries maintain a physical or economic presence within national jurisdictions, they serve as effective points of legal leverage.[101] Their services and infrastructure function as gateways through which online activity must pass, enabling regulators to impose obligations on these intermediaries and, in turn, influence the behavior of a much broader population of users.

In the blockchain context, governments can likewise intervene at points of centralization, most notably through service providers and centralized exchanges. For example, centralized cryptocurrency exchanges and custodial wallet providers that bridge the blockchain ecosystem with the traditional financial system play a crucial role. These actors typically must comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations. However, because blockchain transactions are pseudonymous and the underlying networks do not rely on identifiable, centrally administered servers, the effectiveness of this chokepoint strategy remains inherently limited.

1.3.2. Functional, Regulatory and Technological Equivalence

Blockchain scholarship has proposed several insightful concepts to support proactive and nuanced approaches for integrating blockchain into existing legal frameworks. These approaches stress the need to analyze both the underlying functions performed by the technology and the regulatory objectives pursued by existing legal rules. For example, Primavera De Filippi and co-authors argue that legal systems can adapt to blockchain by applying the principles of "functional equivalence" and "regulatory equivalence."[102]

1.3.2.A. Functional Equivalence

The principle of functional equivalence entails evaluating technologies based on the functions they perform rather than their technical form. Under this approach, different technologies that serve the same function should receive the same or comparable regulatory treatment, regardless of their specific implementation. This principle allows existing legal rules to apply to digital innovations without requiring entirely new regulatory regimes.[103]

A prominent example of functional equivalence is the case of digital signatures. Although digital signatures do not replicate the physical form of handwritten ones, they can serve an equivalent function if they ensure the verification of identity and intent. Accordingly, many jurisdictions recognize that an electronic document can be legally equivalent to a paper-based document for the purposes of contract formation. Some countries rely on interpretation (judicial or doctrinal) to apply functional equivalence,[104] but many have explicitly incorporated it into legislation,

100 "ISPs (Internet Service Providers), search engines, browsers, the physical network, and financial intermediaries." *See* Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 69-74 (2006), https://scholarship.law.columbia.edu/books/175/.

101 *Id*. at 68. *See also Id.* at 81-82 (pointing out that the United States and France are more powerful controllers of intermediaries than Fiji and Ghana, for example, because they have more intermediaries within their borders to go after).

102 "Functional equivalence relies on analysing the function of a particular artefact (e.g., paper document) with a view to determining how those functions could be fulfilled through another type of artefact (e.g., electronic document) within a particular legal context (e.g., contract law)." Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 Pol'y & Soc'y 358, 359, 364-66 (2022), https://ssrn.com/abstract=4001696.

103 *Id.* at 359, 368.

104 In the United States, courts have interpreted pre-existing statute of frauds provisions to encompass electronic signatures without explicit legislative amendment. *See Cloud Corp. v. Hasbro, Inc.*, 314 F.3d 289 (7th Cir. 2002) (holding that a typed name on an email satisfied the "writing" and "signature" requirements under the Uniform Commercial Code Statute of Frauds based on whether the electronic form served the same authentication purpose as traditional signatures). In the United Kingdom, courts have similarly recognized that typed names function as signatures when intended to authenticate the communication. See *Golden Ocean Group Ltd v Salgaocar Mining Industries Pvt Ltd* [2012] EWCA Civ 265 (holding that a sequence of negotiating emails constituted a valid written guarantee under Section 4 of the Statute of Frauds because the typed name authenticated the communication and the emails collectively served the statute's evidentiary purpose).

often derived from the UNCITRAL Model Law on Electronic Commerce (1996).[105] This Model Law articulates the principle of functional equivalence by providing that "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."[106] Similarly, in the blockchain environment "shares that are recorded on a blockchain-based system could be regarded as valid titles to a share, transferable via a blockchain-based registry."[107]

1.3.2.B. Regulatory Equivalence

Regulatory equivalence refers to the recognition that distinct regulatory systems may achieve comparable outcomes or levels of protection, even when their substantive rules or institutional arrangements differ.[108] Sometimes, various legal frameworks achieve comparable regulatory outcomes or an equivalent level of protection across different jurisdictions. For instance, "in certain cases, the EU may recognise that a third country's legal, regulatory and/or supervisory regime is equivalent to a corresponding EU framework."[109] Rather than requiring the application of identical legal rules, it allows for alternative regulatory frameworks that can attain the same policy objectives. For example, under Article 45 of the General Data Protection Regulation (GDPR),[110] the European Commission may determine that a third country ensures a level of data protection that is *essentially equivalent* to that of the European Union, even if the underlying legal provisions differ.

Regulatory equivalence stands in contrast to *functional equivalence*. While functional equivalence asks whether a new technology can be governed under existing legal requirements —so long as it fulfills the same legal or operational functions as its traditional counterpart— regulatory equivalence focuses on whether various legal frameworks adequately safeguard desired policy objectives. In this sense, regulatory equivalence requires assessing whether existing rules are sufficient or whether new regulatory measures are needed to maintain those underlying policy goals.

A logic of regulatory equivalence may therefore lead to the adoption of new regulatory regimes to adapt established legal principles to the distinctive features of emerging technologies, with the goal of ensuring an equivalent level of protection. Although more complex, this approach may prove indispensable to ensuring that fundamental principles —such as privacy, accountability, and transparency— can be effectively safeguarded in rapidly evolving technological environments.

1.3.2.C. Technological Equivalence

A line of scholarship has adapted the concept of "regulatory equivalence" to the technological domain. Rather than concentrating on the comparability of regulatory regimes, Primavera De Filippi and co-authors examine whether technological systems can provide

105 U.N. Comm'n on Int'l Trade Law, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, paras. 48-56, U.N. Sales No. E.99.V.4 (1999), https://digitallibrary.un.org/record/286739/files/19-04970_ebook.pdf; *see also* UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, annex, art. 7, U.N. Doc. A/RES/51/162 (Dec. 16, 1996) https://docs.un.org/en/a/res/51/162.

106 *Id.* at art. 5.

107 Constance Choi et al., Coal. of Automated Legal Applications, Model Law for Decentralized Autonomous Organizations (DAOs) (2021) [hereinafter COALA DAO Model Law], Preamble, at 7 (2021), https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf.

108 Regulatory equivalence is also articulated within discussions of mutual recognition in international regulatory cooperation and financial regulation. *See* Pierre-Hugues Verdier, *Mutual Recognition in International Finance*, 52 Harv. Int'l L.J. 55, 63 (2011), https://ssrn.com/abstract=1757259. For a discussion on regulatory equivalence in the context of blockchain systems, see Primavera De Filippi & Morshed Mannan, *Regulatory Equivalence in Blockchain Systems: The Role of Public Values and Legitimacy*, in Public Governance and Emerging Technologies 152-153 (Jurgen Goossens et al. eds., 2025), https://doi.org/10.1007/978-3-031-84748-6_8.

109 Norton Rose Fulbright, *Examining Regulatory Equivalence* (Jan. 12, 2017), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/regulatory-equivalence-paper.pdf?la=en&revision=0f14b026-231a-4fe0-9c59-5aec60d27ac7.

110 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 45, 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

equivalent safeguards and guarantees to advance existing policy objectives.[111] For instance, the introduction of the DAO Model Law published by the Coalition of Automated Legal Applications (COALA) *(See section 7.3.1.A.)*[112] states that "regulatory equivalence [...] allows for the establishment of equivalence between the function of a legal rule and the function of a technology."[113] This entails assessing whether technology can achieve the purposes pursued by regulation —such as transparency or accountability— even when it does not replicate the formal legal processes that traditionally ensure those outcomes.[114] For instance, the COALA DAO Model Law suggests "to achieve traditional objectives of corporate law by relying on technological means where possible."[115]

In this approach, the focus shifts from jurisdictional comparability to the ability of technical systems to achieve the regulatory objectives traditionally pursued through legal rules.[116] The inquiry examines whether the technical features of a system can fulfill the same regulatory purpose that law ordinarily secures through institutional or procedural mechanisms.[117] Where this condition is satisfied, the technological system may be considered capable of achieving the goals of the existing regulation through its technical characteristics alone. It follows that, under this logic, no immediate regulatory reform would be required, even though the system's technical characteristics prevent the straightforward application of existing legal categories. For example, the drafters of the COALA DAO Model Law argue that the deployment of a smart contract on a blockchain containing relevant data about a DAO can, in certain circumstances, meet the policy objectives of registration requirements for corporate entities, which are driven by objectives of publicity and reliability. Hence, even if unregistered DAOs do not comply with formal registration requirements, the technological features may nonetheless be argued to satisfy the underlying policy objectives of those requirements.[118]

This technological reinterpretation of "regulatory equivalence" tends to blur the analytical boundary between functional equivalence and regulatory equivalence. In practice, blockchain-based mechanisms may sometimes be characterized as functionally equivalent to legally prescribed mechanisms and, on that basis, treated as compliant with existing legal requirements. It is more difficult to understand how technological features can be claimed to achieve comparable regulatory objectives but not be considered functionally equivalent, either operationally or legally.[119]

To preserve conceptual clarity, this report maintains the distinction but adopts different terminology. "Functional equivalence" refers to situations in which a technology performs the same legally relevant function as an existing legally recognized instrument. By contrast, the report uses the term "technological equivalence" to designate

111 Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 Pol'y & Soc'y 358, 368-69 (2022), https://ssrn.com/abstract=4001696.

112 COALA DAO Model Law, *supra* note 107, at 7-8.

113 *Id.,* at 8.

114 "Regulatory equivalence goes one step further, by analysing the purpose of a particular legal or regulatory provision (e.g., auditing for the purpose of verifying credit-worthiness) to determine under which conditions the same purpose could be achieved, in a wholly different manner, through alternative technological means (e.g., using fully collateralized smart contracts to eliminate counterparty-risk)." De Filippi et al., *The Alegality of Blockchain Technology, supra* note 111, at 368.

115 COALA DAO Model Law, *supra* note 107, at 8.

116 For a discussion of the idea that technological artifacts can fulfil the regulatory functions or policy objectives ordinarily secured by law, see De Filippi & Mannan, *Regulatory Equivalence in Blockchain Systems, supra* note 108, at 159-160.

117 For a discussion on how algorithmic systems operate as "architectural" or "design-based" regulation—embedding policy objectives directly into technological infrastructure rather than relying on traditional legal commands and institutional enforcement. *See* Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 Regul. & Governance 505, 509 (2018) https://doi.org/10.1111/rego.12158.

118 COALA DAO Model Law, *supra* note 107, at 7-8.

119 *Id.* at 7-9; De Filippi & Mannan, *Regulatory Equivalence in Blockchain Systems, supra* note 108, at 154-160.

claims that a technology's design and operation can achieve the underlying policy objectives of a legal framework, even where existing legal categories cannot be straightforwardly applied.

1.3.3. Potential Regulatory Options

Within the framework outlined above, policymakers may choose among three main approaches:

First, they may **apply existing legal frameworks to new technological contexts** by extending established laws to cover novel phenomena, such as blockchain (functional equivalence). For instance, a smart contract may be treated as the functional equivalent of a traditional written contract. This approach relies on identifying parallels between traditional legal categories and technological systems, applying existing principles and rules rather than enacting new legislation.

Second, they may pursue regulatory equivalence, which involves assessing or designing frameworks that **adapt established legal principles to the specific features of emerging technologies**. The goal is to ensure an *equivalent level of protection* to that offered under existing regimes, even where the regulatory techniques differ. This approach may require drafting new legal instruments when existing ones cannot adequately address the distinctive characteristics of a given technology. It is particularly important for safeguarding fundamental principles —such as privacy, accountability, and transparency— in rapidly evolving digital environments.

Third, they may **assess whether technological features themselves can achieve the policy objectives** that law traditionally secures through institutional or procedural mechanisms, which could be expressed as "technological equivalence." For example, corporate law may require registration to promote transparency and accountability; a blockchain could satisfy the same purpose by making all transactions publicly verifiable.

These three approaches, while illuminating, do not account for situations in which the emergence of a fundamentally new technology requires policymakers to rethink policy goals and principles from the ground up.[120] Every regulatory choice reflects deeper considerations: How strongly does a government value the potential of blockchain technology? How seriously does it regard the associated risks? And does a government perceive the technology primarily as a threat to be contained or an innovation to be supported? When dealing with a novel technology, policymakers must anticipate and mitigate significant risks while adopting regulatory frameworks that do not unduly hinder innovation. This task is especially challenging because emerging technologies often give rise to new categories of risk for which effective mitigation strategies are not yet clear. In such cases, selecting an appropriate regulatory strategy — and designing a tailored legal framework— may fall outside the three equivalence models. Existing policy objectives may simply be ill-suited to the challenges posed by the technology, making it necessary to formulate new principles and redefine the goals that regulation should pursue.

1.4. PURPOSE AND STRUCTURE OF THE REPORT

Within this framework, the purpose of this report is to provide an overview of blockchain technology and to identify the principal challenges it raises for policymakers. Given the breadth and rapid evolution of the technology and its ecosystem, a truly comprehensive account of all its dimensions would not be feasible, and this report does not attempt to be exhaustive. Nor does it offer an exhaustive treatment of crypto-assets and their

120 Alesia Zhuk, *Beyond the blockchain hype: addressing legal and regulatory challenges,* SN Soc. Sci. 5, 11 (2025), https://doi.org/10.1007/s43545-024-01044-y.

surrounding ecosystems, though these developments are discussed insofar as they inform broader policy and governance challenges. Likewise, it does not seek to provide a comprehensive historical account of the incidents, failures, and scandals that have shaped the sector over the past decade but instead draws selectively on such examples where they help illustrate those broader issues.

Instead, this report seeks to clarify the questions that policymakers confront when engaging with a technology whose technical underpinnings are complex and whose future trajectory remains uncertain. It focuses in particular on what is arguably the most difficult challenge for regulators: the decentralized structure of most blockchain networks –a structure which complicates both governance and regulation. By examining this issue, the report aims to contribute to an emerging debate on decentralization and its implications. To that end, it analyzes the difficulties involved in designing regulatory frameworks for decentralized systems and the existing modes of decentralized governance and the challenges they present.

The significance of decentralization extends well beyond blockchain and is likely to shape the evolution of a wide range of networked technologies. Artificial intelligence provides an illustrative example. Although the development and deployment of state-of-the-art AI systems remain heavily concentrated within major private companies, an increasingly dynamic open-source ecosystem is enabling models to be trained, fine-tuned, and operated across more distributed infrastructures. Emerging approaches suggest that certain forms of AI may progressively shift toward decentralized architectures *(See section 4.9)*. These developments raise governance questions that parallel, and may eventually surpass, those encountered in blockchain ecosystems, particularly as responsibility, control, and oversight become harder to assign in distributed environments.

Likewise, the issues of automation illustrated by smart contracts are not unique to blockchain. Rather, they foreshadow broader debates about agentic AI and autonomous computational agents, which similarly involve systems that can initiate, execute, and coordinate actions without continuous human intervention. The challenges posed by such autonomous systems — ensuring accountability, embedding ex-ante constraints, and maintaining compliance in real time— echo the regulatory dilemmas already visible in blockchain-based smart contracts *(See section 6.5)*.

Against this backdrop, the aim of this report is to contribute to the ongoing, long-term reflection on how policymakers might approach decentralized and increasingly autonomous networked systems: How can such systems be governed in accordance with democratic principles and the rule of law? And how can legal frameworks meaningfully apprehend a technology that has, in many respects, been deliberately engineered to resist traditional forms of regulation? The report's central claim is that blockchain occupies neither a space of "alegality" nor one of effective regulation, but a condition of persistent, partial, and unstable legality that reflects structural features of the technology and its governance architecture. Its ambition is not to resolve this condition, but to map it with sufficient precision that future regulatory responses can rest on solid analytical foundations.

This report is current and reflects the legal and technological landscape as of January 15, 2026. It is structured as follows:

Chapter 2 provides a conceptual and technical primer on how blockchains work: It explains the technology's core properties (decentralization, transparency, immutability, cryptography, and programmability), the roles and functions of key participants, and the mechanisms that

collectively enable blockchain networks to operate, govern themselves, and support diverse applications.

Chapter 3 analyzes how blockchain systems are actually governed: It examines the mechanisms through which protocol changes, upgrades, and collective decisions are made —including on-chain voting systems and off-chain coordination. It highlights the concentration of real decision-making power among core developers, validators, foundations, and large token holders, and the vulnerabilities to which these governance structures remain exposed.

Chapter 4 surveys the major applications of blockchain beyond cryptocurrencies, showing how it enables new forms of cross-border payments, fundraising, financial services (tokenization and DeFi), recordkeeping, data sharing, identity, social networks, dispute resolution, supply chains, emerging decentralized AI systems, and experimental forms of digital political organization such as network states.

Chapter 5 analyzes some of the risks associated with crypto-assets and blockchain systems, from extreme price volatility, fragile stablecoin designs, NFT speculation, market manipulation, and repeated institutional failures to illicit uses, security vulnerabilities, environmental impacts, and profound privacy challenges.

Chapter 6 examines how blockchain technologies collide with existing legal frameworks. Drawing on widely discussed cases —including *The DAO*, *Mango Markets*, *Platypus*, *Peraire-Bueno*, and *Tornado Cash*— it highlights the unresolved tensions between "code is law" and the authority of traditional legal systems. And it shows how decentralization does not really remove blockchain from the reach of law despite generating complex legal uncertainties.

Chapter 7 surveys the regulatory strategies some states have adopted to address blockchain. It compares observational, enforcement-based, proactive, and restrictive approaches through detailed case studies ranging from the United States —where a shift from regulation by enforcement toward legislative frameworks such as the GENIUS Act marks a significant policy reorientation— to the European Union's comprehensive MiCA regime, Switzerland's technology-neutral adaptation of existing law, South Korea's interventionist model, and China's prohibition-based approach.

Chapter 8 synthesizes the report's overall findings. It highlights four interrelated dynamics: decentralization as a relative rather than achieved ideal; the rise of code-governed systems; the limits of blockchain's supposed 'alegality'; and the structural regulatory gaps that persist across jurisdictions. It then identifies a range of policy options —including hybrid regulatory frameworks that integrate legal rules with code-based mechanisms, voluntary governance standards, targeted liability clarifications for developers and token holders, and soft-law instruments for international coordination —to guide the development of more accountable and coherent frameworks for blockchain governance.

CHAPTER 2

Blockchain Technology: The Basics

CHAPTER 2 TABLE OF CONTENTS

CHAPTER 2. BLOCKCHAIN TECHNOLOGY: THE BASICS **28**
2.1. Blockchain Fundamentals 30
2.1.1. Main Concepts 30
2.1.2. Key Features 32
2.1.2.A. Decentralization 32
1. Definition Attempts 32
2. Decentralization and Distribution 34
2.1.2.B. Transparency 35
2.1.2.C. Immutability 35
2.1.2.D. Cryptography 36
2.1.2.E. Programmability and Composability 36
2.1.3. Participants and Actors 36
2.1.4. Public, Permissioned, Private Blockchains 37
2.2. Cryptographic Foundations 39
2.2.1. Hashing 39
2.2.2. Public Key Cryptography 40
2.2.3. Blocks 41
1. Block Header 41
2. Block Hash 42
3. Chain of Blocks 42
2.2.4. Transactions 43
2.3. Consensus Mechanisms 44
2.3.1. Proof of Work 44
2.3.1.A. The Proof-of-Work Mechanism 45
2.3.1.B. Economic Incentives to Mining 46
2.3.1.C. Reliability of PoW 47
2.3.2. Proof of Stake 47
2.3.2.A. The Proof-of-Stake Mechanism 47
2.3.2.B. Ethereum Proof of Stake 48
2.3.3. Other Consensus Mechanisms 49
2.3.4. Forking 50
2.3.4.A. Accidental Forks 51
2.3.4.B. Intentional Forks 52
2.4. Blockchain Assets 54
2.4.1. Fungible Coins and Tokens 54
2.4.1.A. Native Assets or Coins 54
2.4.1.B. Tokens 55
2.4.1.C. Stablecoins 57
2.4.1.D. Meme Coins 58
2.4.2. Non-Fungible Tokens (NFTs) 59
2.4.2.A. Key Features of NFTs 60
2.4.2.B. The NFT Use Cases 61
2.5. Smart Contracts and DAOs 62
2.5.1. Smart Contracts 63
2.5.1.A. The Emergence of Smart Contracts 63
2.5.1.B. Key Features of Smart Contracts 64
1. Automation 64
2. Immutability 64
3. Gas 65
4. Oracles 65
2.5.1.C. Main Applications 66
2.5.2. Decentralized Autonomous Organizations 67
2.5.2.A. What Is a DAO? 68
2.5.2.B. The Organization of a DAO 69
2.6. Privacy Enhancing Techniques 70
2.6.1. Pseudonymity 70
2.6.2. Techniques for Transaction Anonymization: Mixers and Tumblers 72
2.6.3. Zero-knowledge Proofs 74
2.6.4. Privacy Coins 76
1. Monero 76
2. Zcash 77
2.7. Properties and Limitations 77
2.7.1. Notable Properties 78
2.7.2. The Blockchain Trilemma 79
KEY TAKEAWAYS 82

CHAPTER 2
Blockchain Technology: The Basics

At its core, blockchain technology addresses a simple but fundamental problem: how to maintain a reliable record of transactions among participants who do not fully trust one another. Traditional recordkeeping systems typically rely on a centralized ledger —for example, a single spreadsheet that records who owns what and in what quantities. While administratively straightforward, such arrangements create structural vulnerabilities: The entity controlling the ledger becomes a single point of failure, a potential bottleneck, and a possible source of error, manipulation, or abuse.

Blockchain systems propose an alternative architecture. Rather than entrusting recordkeeping to a central authority, they distribute the ledger across a network of participants, each maintaining a synchronized copy. This chapter provides an overview of the technical features of blockchain systems and introduces the core principles that underpin these distributed architectures.

2.1. BLOCKCHAIN FUNDAMENTALS

Blockchains enable the creation and maintenance of a shared ledger without relying on a central authority. When a user initiates a transaction on a blockchain, it is broadcast to the network. Each node independently verifies the proposed transaction and updates its local copy of the ledger in accordance with predefined rules. If the transaction satisfies these rules, participants to the network accept it through the system's consensus mechanism and incorporate it into the shared transaction history. Under normal operating conditions, honest participants converge on the same record of transactions. No single actor can unilaterally alter the shared ledger without controlling a sufficiently large share of the system's validating power. As the network grows, the coordination and economic costs required to do so generally increase (although this depends on the distribution of validating power and the degree of coordination among participants).

2.1.1. Main Concepts

A digital ledger. Blockchains are essentially digital ledgers. They maintain a tamper-resistant digital record in a manner that can be shared and validated by its users. In some cases, the state of the blockchain resembles that of a financial ledger, with lists of transactions and account balances. In other cases, it may represent the status of a computer program, a data storage structure, or other use cases. At a foundational level, the core operation performed on a blockchain is a *state transition* —that is, an update to the system's state, such as modifying account balances or the stored state of a blockchain-based application. In Bitcoin, altering the state means changing the owner-of-record when some bitcoins are sold by their previous owner-of-record.

Blocks. The term "blockchain" derives from the fact that the system groups transactions into discrete batches known as "blocks," which it then links together in sequence to form a chain. This block-based architecture provides a chronological structure for recording

transactions and contributes to the integrity and practical immutability of the ledger. Each block contains a set of validated transactions, along with metadata. Once the network accepts the block according to the consensus rules, nodes add it to the end of the canonical chain. This sequential ordering of blocks creates a continuous record of changes to the blockchain's state over time. Crucially, each block includes a cryptographic "hash" (a digital fingerprint) of the previous block's header. This hash-based linkage ensures that any attempt to modify a past block would alter its hash and thereby break the continuity of the chain, making tampering readily detectable. Architecturally, the requirement that all transactions be included in blocks, combined with the requirement that the canonical chain include all accepted blocks, implies that the blockchain records every validated change to the ledger's state in an append-only manner.

Nodes. A blockchain network consists of multiple "nodes," which are "connection points that receive, store, verify, and transmit data."[121] A blockchain node can be "any device —such as a computer, server or even a specialized appliance— that runs the blockchain's protocol software and connects to its network."[122] These nodes are distributed across different geographic locations worldwide. Nodes typically host their own copy of the blockchain and validate new blocks to be added. This architecture, involving nodes across a widely distributed network, requires high levels of synchronization, as opposed to the classic client-server relationship that dominates centralized network architecture. Getting independent nodes to agree on a shared state of reality is a challenging problem to solve, especially when dealing with digital money.

Consensus mechanism. To enable participants to converge on a shared view of the ledger's state, blockchain networks rely on a *consensus mechanism* *(See below Section 2.3)*. A consensus mechanism consists of a set of protocol rules encoded into the network that govern how nodes validate transactions, propose and select blocks, and determine which version of the ledger is considered canonical. These rules allow otherwise independent participants to coordinate the maintenance, synchronization, and updating of the ledger without relying on a central authority. Under this framework, participants first check proposed transactions for validity according to predefined protocol rules, such as the verification of digital signatures and compliance with transaction formats. Then they group valid transactions into blocks that are accepted through the consensus process, enabling network-wide convergence on a single transaction history. In proof-of-work systems *(See below Section 2.3.1)*, consensus is achieved by requiring participants who propose new blocks to perform computationally intensive, hash-based calculations. To add a block to the chain, a participant must find a value that satisfies a predefined condition, a task that is computationally expensive to perform,[123] but straightforward for other nodes to verify. In sufficiently large networks, this mechanism makes it economically prohibitive and statistically unlikely for malicious actors to record invalid transactions or rewrite recent transaction history. Because each block is cryptographically linked to its predecessor, any attempt by a malicious actor to modify a previously accepted block would require recomputing that block and all subsequent blocks while

121 Corey Barchat, *What are blockchain nodes and how do they work?*, MOONPAY (Oct. 7, 2025), https://www.moonpay.com/learn/blockchain/what-are-blockchain-nodes.

122 In decentralized systems, nodes "take over the role that central servers once held." They "validate transactions, store data, and communicate with one another to ensure that every copy of the public ledger remains synchronized and tamper-resistant." Kamel Haouchine, *Blockchain Nodes Explained*, CONTABO BLOG (Mar. 17, 2025), https://contabo.com/blog/blockchain-nodes-explained/.

123 In a proof-of-work (PoW) system, miners face a probabilistic cryptographic challenge. They repeatedly vary the nonce (and, in Bitcoin, the extra nonce in the coinbase transaction) and compute the hash of the block header to check whether the output falls below the network's current difficulty target. There is no single "correct" answer; instead, there exists a vast space of potential valid hashes. Any output that satisfies the target condition is acceptable. Consequently, the challenge lies not in solving a deterministic problem but in discovering a valid solution through a brute-force, trial-and-error process. Success depends on probability and computational effort rather than logical reasoning.

simultaneously outpacing the cumulative computational effort of honest participants. Such an attack would demand substantial computational and energy resources and would be highly unlikely to succeed, with expected costs exceeding any plausible economic benefit.

Layers *(see Figure 22)***.** Blockchain systems are often structured in layers The base layer (Layer 1) provides core functions, such as transaction execution, validation, and recording on the network. Additional layers (Layer 2) are built on top of this base to improve scalability and functionality, often by processing transactions off-chain and relying on Layer 1 for final settlement and security.

2.1.2. Key Features

2.1.2.A. Decentralization

Although "decentralization" is frequently described as "the core premise of blockchain technologies,"[124] there is neither an official definition of the concept nor a universal consensus regarding its meaning. While Nakamoto's white paper articulated design principles intended to eliminate central control, it did not employ the term "decentralization."[125] The conceptual indeterminacy of decentralization can be understood as reflecting the axiomatic truth that, however defined, decentralization exists along a continuum between complete centralization and full decentralization.[126]

1. Definition Attempts

Technology experts and researchers have attempted to define and assess "decentralization." These efforts are relatively recent and remain particularly challenging, as scholarly research has yet to converge on a coherent semantic framework.[127]

When introducing the term "Decentralized Autonomous Organization" (DAO) in 2014,[128] Vitalik Buterin, a founder of Ethereum, offered an "applied definition of decentralization."[129] In his view, decentralized structures can reduce the risk of attacks or collusion and can continue to function even when some of their components fail. A few years later, while acknowledging the difficulty of defining "decentralization," Buterin suggested that it should be analyzed across several dimensions: (1) an architectural dimension, referring to the number of computers that compose the system; (2) a political dimension, referring to how many individuals or organizations ultimately control those computers; and (3) a logical dimension, referring to whether the system's interface and data structures resemble a single unified object or a more diffuse, swarm-like network.[130] More recently, Buterin has described decentralization as a normative value, intended to "minimize the dependence of an application on any one single actor. In particular, an application should continue working even if its core developers disappear forever."[131]

124 Miles Jennings, *Decentralization Is Why We Fight for Crypto*, a16zcrypto (Dec. 17, 2024), https://a16zcrypto.com/posts/article/decentralization-fight-for-crypto/.

125 *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 1, 8, (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf (stressing that a peer-to-peer system does not require a trusted third-party).

126 Luke Conway, *Measuring Decentralization: Is Your Crypto Decentralized?*, Blockworks (Mar. 16, 2022), https://blockworks.co/news/measuring-decentralization-is-your-crypto-decentralized; Miles Jennings, et al., *Factors of Decentralization of Web3 Protocols: Tools for Planning Greater Decentralization*, a16zcrypto (May 31, 2023), https://a16zcrypto.com/posts/article/decentralization-factors-web3-protocols-tables/.

127 Huseyin Oguz Genc & Eray Acikgoz, *Constructing an Evaluation Framework for Full Decentralization: A Case Study on DeFi's Stable Currency Issuance Services–CDP Protocols*, 8 Stan. J. Blockchain L. & Pol'y 177, 180 (2025), https://stanford-jblp.pubpub.org/pub/cdp-protocols. *See also*: *See, e.g.*, Ziqiao Ao et al., *Is Decentralized Finance Actually Decentralized? A Social Network Analysis of the Aave Protocol on the Ethereum Blockchain*, arXiv (June 16, 2022), https://arxiv.org/abs/2206.08401

128 Vitalik Buterin, *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*, Ethereum Found. Blog (May 16, 2014), https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

129 Henrik Axelsen et al., *When is a DAO Decentralized?*, 31 Complex Sys. Informatics and Modeling Q. 51, 56 (July 31, 2022), https://doi.org/10.7250/csimq.2022-31.04 (presenting decentralization as a verifiable state in which (1) the design of a DAO is collusion-resistant and grounded in long-term equilibrium, and (2) its governance processes are transparent and unrestricted in access).

130 Vitalik Buterin, *The Meaning of Decentralization*, Medium (Feb. 6, 2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

131 Vitalik Buterin, *Make Ethereum Cypherpunk Again*, Vitalik Buterin Website (Dec. 28, 2023), https://vitalik.eth.limo/general/2023/12/28/cypherpunk.html.

Although there is no official or universally accepted definition of decentralization, it is often defined in blockchain scholarship as the distribution of power, control, and decision making across a network of participants,[132] rather than their concentration in a single entity or authority.[133] For instance, some protocols, such as Bitcoin, operate with thousands of independent nodes and are, therefore, regarded as highly decentralized. Experts often emphasize that decentralization also entails the possibility for users to engage in direct peer-to-peer transactions,[134] thereby granting individuals control over their assets without reliance on intermediaries, such as banks. For instance, Bitcoin users retain full control of their private keys and, consequently, their cryptocurrency.[135] This stands in contrast to traditional bank accounts, which are managed by financial institutions that oversee transactions and hold customers' funds. Of course, definitions of decentralization may evolve over time as technology advances and governance mechanisms become more sophisticated.

Decentralization implies that no individual or institution is formally responsible, whether technically or legally, for establishing the authoritative version of the ledger. For instance, in proof-of-work (PoW) systems, decentralization is assessed by measuring the concentration of mining power, often expressed as the percentage of total hash rate controlled by individual mining pools. In proof-of-stake (PoS) systems, it depends on the number of validators or stake pools, the distribution of staked tokens, and how much of the token supply participates in consensus.[136] These indicators, however, function as proxies rather than exhaustive measures of decentralization, as they may not capture other relevant factors, such as client diversity, governance influence, or geographic dispersion.

Experts have developed frameworks and indices to measure decentralization. Most assessments focus on distributed governance, power distribution, resilience, and token concentration.[137] Among other indexes, the *Nakamoto Coefficient* expresses the minimum number of actors that would need to collude to compromise the system's security or governance.[138] Other means for assessing decentralization involve operational indicators, including the geographic distribution of validators; the diversity of node-hosting infrastructures; and, the heterogeneity of basic software components (such as client implementations).[139]

Overall, decentralization appears less as a fixed condition than as a spectrum or continuum, which helps to explain the

132 For instance, "the dispersion or distribution of functions and powers", Axelsen et al., *supra* note 129, at 55.

133 Decentralization is "the distribution of control and decision-making, eliminating the need for a central authority— ensuring more choice, transparency, security, and resilience for users." Miles Jennings, *supra* note 124.

134 *See* Nakamoto, *supra* note 125, at 1-2 (explaining that one of the challenges with blockchain technology is precisely that it allows direct peer-to-peer interactions without ways to verify the identity of another user).

135 *Non-Custodial Wallets vs. Custodial Wallets: Know the Difference*, BitPay (July 24, 2025), https://www.bitpay.com/blog/non-custodial-wallets-vs-custodial-wallets.

136 Luke Conway, *Measuring Decentralization: Is Your Crypto Decentralized?*, Blockworks (Mar. 16, 2022), https://blockworks.co/news/measuring-decentralization-is-your-crypto-decentralized; Aoyon Ashraf, *Is Miner Concentration Once Again Jeopardizing Bitcoin? Not Exactly*, NASDAQ (Mar. 26, 2022), https://www.nasdaq.com/articles/is-miner-concentration-once-again-jeopardizing-bitcoin-not-exactly (originally published on CoinDesk).

137 For the *Distributed Governance Index*, *see* Tom W. Bell, *Distributed Self-Government in Protocol Communities: An Introduction and Index of Examples*, 25 Indep. Rev. 293, 296-98 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4058722; For the *XYZ Decentralization Index*, *see* Javier Sanchez Valiente, *The XYZ Decentralization Index: A Framework for Assessing Decentralization in Crypto Protocols*, dYdX Foundation (Dec. 18, 2024), https://www.dydx.foundation/blog/the-xyz-decentralization-index-a-framework-for-assessing-decentralization-in-crypto-protocols; For the *Decentralization Quotient*, Jaeseung Lee et al., *DQ: Two Approaches to Measure the Degree of Decentralization of Blockchain*, 7 ICT Express 278, 279-80 (2021), https://doi.org/10.1016/j.icte.2021.08.008.

138 See *Nakamoto Coefficients*, Nakaflow, https://nakaflow.io/ (last visited Jan. 15, 2026), for "a measure of the smallest number of independent entities that can act collectively to shut down a blockchain" in the most popular blockchain networks. Moreover, *Gini coefficients* quantify wealth distribution inequality. *See generally* Lidia Ceriani & Paolo Verme, *The Origins of the Gini Index: Extracts from Variabilità e Mutabilità (1912) by Corrado Gini*, 10 J. Econ. Inequality 421 (2012), https://doi.org/10.1007/s10888-011-9188-x.

139 Stephanie Dunbar & Sam Padilla, *Evaluating Validator Decentralization: Geographic and Infrastructure Distribution in Proof-of-Stake Networks 1*, Messari (June 1, 2023), https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks; Joshua Tan et al., *Open Problems in DAOs* 16, arXiv (Oct. 29, 2023), https://arxiv.org/abs/2310.19201.

appeal of the concept of "progressive decentralization."[140] However, scholars and practitioners continue to debate whether decentralization should be valued as an end in itself or as a means to broader objectives, such as "permissionless participation, censorship resistance, transparency, immutability, self custody [over one's assets] . . . and difficulty of change or inflation."[141]

2. Decentralization and Distribution

The concepts of "distributed systems" and "distributed computing" that pre-date blockchain[142] are often mentioned in reference to decentralization. However, "distributed networks" may be distinguished from "decentralized networks." The adjective "distributed" does not necessarily relate to the network's management structure.[143] A *distributed system* refers to the technical architecture: a network of nodes that coordinate to provide a service. Distributed networks consist of nodes that are geographically or otherwise widely dispersed, while still operating under a top-down or hierarchical control structure.[144] Google's data centers are a good example of distributed networks: Google operates a system of globally distributed data centers,[145] with multiple nodes processing and storing data across different locations. However, the company retains full control over these centers. Therefore, a network may be distributed but still have centralized decision-making or control structures.

By contrast, "decentralized" refers to the distribution of authority, control, and decision making. In decentralized networks, such as the Bitcoin network and other public blockchains, no single entity exercises complete control over the system. A decentralized system typically —though not necessarily— relies on a distributed architecture, but the defining feature lies in the absence of a single authority responsible for coordination or governance. The term thus points not only to network topology but also to how authority, consensus, and control are organized.

The distinction between distributed and decentralized systems is closely related to, but conceptually distinct from, the distinction between technical and political decentralization in blockchain governance. Technical decentralization concerns the architecture of the blockchain protocol and network: how data and computation are distributed across nodes. Political decentralization concerns the distribution of decision-making power among stakeholders, such as who determines protocol upgrades or governance rules. A system may be technically decentralized, with numerous nodes and an open consensus mechanism, yet politically centralized, for example when a small group of core developers or client teams effectively controls protocol evolution.

Most blockchain networks or protocols explicitly or implicitly aspire to achieve both technical distribution (data and operations spread across many computers or nodes) and political decentralization (the absence of any single entity or authority exercising dominant influence).

---

140 *See* Jesse Walden, *Progressive Decentralization: A Playbook for Building Crypto Applications*, Andreessen Horowitz (Jan. 9, 2020), https://a16z.com/progressive-decentralization-a-playbook-for-building-crypto-applications/. *See also* Jad Esber & Scott Duke Kominers, *Progressive Decentralization: A High-Level Framework*, a16z Crypto (Dec. 1, 2023), https://a16zcrypto.com/posts/article/progressive-decentralization-a-high-level-framework/.

141 DeCenter, Princeton Univ., *Decentralizing Power Through Blockchains: Key Research Questions Across Disciplines* 8 (2024), https://decenter.princeton.edu/wp-content/uploads/2024/07/DeCenter-Paper-2024-Q3-Spread.pdf.

142 *See* Dominic Lindsay, *The Evolution of Distributed Computing Systems: From Fundamental to New Frontiers*, 103 Computing 1859, 1863-71 (Jan. 30, 2021), https://doi.org/10.1007/s00607-020-00900-y.

143 *See* Riaan Bezuidenhout, Wynand Nel & Jacques M. Maritz, *Defining Decentralisation in Permissionless Blockchain Systems*, 29 Afr. J. Info. & Commc'n (2022), https://ajic.wits.ac.za/article/view/14247/18656; see *also* Cryptopedia Staff, *What Does Decentralized Mean?*, Gemini (June 30, 2022), https://www.gemini.com/cryptopedia/what-does-decentralized-mean-in-crypto-decentralized-meaning.

144 *See generally* Jean-Philippe Vergne, *Decentralized vs. Distributed Organization: Blockchain, Machine Learning, and the Future of the Digital Platform*, 1 Org. Theory 1 (2020), https://ssrn.com/abstract=3694706. *See also* Cryptopedia Staff, *Centralized, Decentralized, & Distributed Networks*, Gemini (July 12, 2021), https://www.gemini.com/cryptopedia/blockchain-network-decentralized-distributed-centralized (section "What Is a Distributed Network?").

145 Sachin Gupta, *Expanding Our Infrastructure with Cloud Regions Around the World*, Google Cloud (Dec. 1, 2021), https://cloud.google.com/blog/products/infrastructure/google-cloud-platform-region-updates. *See also Discover Where the Internet Lives*, Google, https://datacenters.google/locations/ (last visited Jan. 15, 2026).

However, these characteristics can exist independently. In the case of social media, distributed social media refers to platforms built on infrastructures spread across many nodes —often user devices— that may, in some implementations, operate without servers at all, as each device functions simultaneously as client and server. By contrast, decentralized social media refers to social networking systems, such as *Mastodon* or *Bluesky,* which function, to varying degrees, without a central authority[146] and may or may not rely on blockchain technology *(See section 4.6.1)*.

2.1.2.B. Transparency

Transparency on blockchain networks refers to the accessibility and verifiability of transaction data and network operations. Blockchain protocols typically publish their source code, allowing anyone to review and audit the system. Unlike traditional financial systems, which restrict access to transaction records, most public blockchain networks record transactional details on a publicly accessible ledger, while preserving user pseudonymity through cryptographic mechanisms. Consensus protocols govern the process by which transactions are verified and added to the blockchain, making it visible to all network participants. The blockchain ledger maintains a complete history of transactions, enabling participants to trace assets back to their origin and verify ownership and authenticity.

Transparency may reduce certain forms of information asymmetry between participants, which are traditionally at the core of principal–agent problems in centralized systems *(see section 2.5.2.A)*. The degree of transparency, however, varies across protocols, particularly in the case of permissioned blockchains, privacy-focused networks, or layer-two solutions.

2.1.2.C. Immutability

Immutability is a cornerstone feature of blockchain technology and ensures that, once data are recorded on a chain, no one can alter, delete, or tamper with them without detection.[147] Unlike traditional databases, which may overwrite historical data, blockchain maintains a complete historical record, preserving both original and new entries.[148] This feature contributes to the ledger's resistance to manipulation by any central authority or external entity and reinforces broader properties such as security and censorship resistance.

Blockchain protocols rely on incentive structures grounded in game theory, whereby validators are rewarded for adhering to consensus rules and for confirming the validity of transactions. Collective agreement among validators on transaction validity reinforces immutability by safeguarding against unauthorized modifications and preserving the integrity of the ledger.

Although immutability secures information, it can pose challenges when errors or fraudulent transactions occur, as such records cannot be easily corrected or removed. Blockchain systems are, therefore, not absolutely immutable; under exceptional circumstances, it is possible —though extremely difficult— to retroactively alter transactions, as illustrated by The DAO fork *(See below Figure 11)*.[149]

---

146 *See* Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised Social Media*, 12 Internet Pol'y Rev. 2, 4-5 (2023), https://policyreview.info/pdf/policyreview-2023-1-1681.pdf (also calling these networks "federated"); Mayank Jain et al., *Revamping Social Networking Using Blockchain: Conceptual Case-Study of Lens Protocol*, Proc. of the Int'l Conf. on Innovative Computing & Commc'n (2023), https://ssrn.com/abstract=4367051.

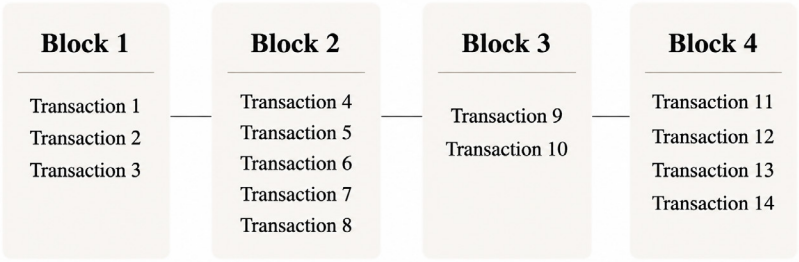
147 *See* Mateusz Godyn et al., *Analysis of Solutions for a Blockchain Compliance with GDPR*, Sci Rep 12, 15021 (2022), https://pmc.ncbi.nlm.nih.gov/articles/PMC9440070/, at 1; Tavish Aggarwal, *Data Immutability in Blockchain Network*, Ejable (Nov. 16, 2023), https://www.ejable.com/tech-corner/blockchain/data-immutability-in-blockchain-network (section "Cryptographic Hash Functions and Checksums").

148 Gousia Habib et al., *Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing*, 14 Future Internet 1, 7 (2022), https://www.mdpi.com/1999-5903/14/11/341.

149 Politou et al. described blockchain technology as tamper-evident rather than immutable, emphasizing that a blockchain retains a complete historical record of transactions up to the point of the fork and maintains this record on all resulting chains. *See* Eugenia Politou et al., *Blockchain Mutability: Challenges and Proposed Solutions*, 9 IEEE Transactions on Emerging Topics in Computing 1972, 1973 (2019) at 2, https://ieeexplore.ieee.org/document/8883080.

FIGURE 2.
Diagram of a blockchain

This diagram depicts an extremely simplified blockchain, in which groups of transactions are organized into blocks, and blocks are linked chronologically.



2.1.2.D. Cryptography

Cryptography is fundamental to blockchain technology. Public-key cryptography *(See below section 2.2.2.)* establishes ownership and secures transactions: Private keys generate digital signatures that prove control over assets, while public keys, often represented as addresses, allow others to verify signatures and transfer assets securely.

Blockchains also employ cryptographic hash functions *(See section 2.2.1.)* to generate fixed-length outputs from data, known as "hashes." Each block contains the hash of its predecessor block, thereby preserving chronological order and linking blocks together. Any alteration to a block would change its hash and invalidate all subsequent blocks, making tampering immediately detectable. In this way, data integrity is maintained through the protocol itself, without reliance on a trusted intermediary or central authority.

2.1.2.E. Programmability and Composability

Programmability and composability constitute additional defining features of blockchain systems. Programmability refers to the ability to encode complex logic directly into the blockchain through smart contracts, enabling automated and conditional execution of transactions. Composability refers to the capacity of different applications and protocols to interact and build upon one another within a shared infrastructure. While these features foster innovation and functional integration, they also create interdependencies across systems, which may amplify operational and systemic risks.

2.1.3. Participants and Actors

Broadly speaking, blockchain systems involve four main groups of participants: core developers, miners and validators, service providers (such as wallet providers — particularly custodial wallets— exchanges, overseers, and custodians of tokens), and users. Additional categories, such as token issuers and market makers on decentralized exchanges, may also be relevant. These participants structure the functioning of blockchain ecosystems and represent potential focal points for regulatory responsibility.

- **Core developers.** Core developers design and maintain the underlying code that runs on blockchains. They may work within a single company or collaborate in open-source communities using platforms such as GitHub. Non-core developers, by contrast, design front-end applications or middleware that facilitate interaction with blockchain protocols.
- **Miners or validators**. Miners and validators assemble transactions into blocks and, in many systems, execute smart contracts as part of that process. As block producers, they determine whether transactions are included and in what order. The term "miner" refers to participants in proof-of-work

("PoW") systems, while "validator" is used in proof-of-stake ("PoS") and other consensus mechanisms *(See details in 2.3.)*. In practice, miners and validators often operate pseudonymously and remain largely invisible to end users. They are identifiable only through blockchain addresses, although large pools, staking services, or professional operators may be publicly identifiable. In permissionless networks, mining or validation roles are open to any actor who meets the technical requirements.

- **Service providers**. Services include exchanges, custodial wallet providers, custodians, and investment funds, many of which have become dominant participants in the ecosystem. By facilitating access to blockchain services, exchanges and similar providers often function as gatekeepers, effectively reintroducing elements of intermediation and centralized control into otherwise decentralized networks.[150] Users who entrust assets to centralized intermediaries relinquish direct control and may be subject to restrictions on account access, withdrawals, or trading. The widely reported collapse of cryptocurrency exchange FTX *(See section 5.1.5.C.)*, which left customers unable to recover their funds, illustrates the risks associated with such reliance.[151]
- **Users**. Users include not only end-users interacting with the system, but also developers, contributors, and other participants who build, maintain, or rely on blockchain-based applications. Blockchain users are pseudonymous by default and can typically be identified only through on-chain identifiers, such as wallet addresses. Anyone can participate in a public blockchain network, although doing so often requires a degree of technical expertise that many users lack. Participation in permissioned blockchain networks, by contrast, is restricted to authorized actors.

2.1.4. Public, Permissioned, Private Blockchains

There are three types of blockchains: public, permissioned, and private.

Public blockchains are publicly accessible through use of open-source software.[152] Anyone can join and participate in a public network and view its transactions.[153] Participation in public blockchains does not require prior approval or authentication of one's identity.[154] Users are identified via account identifiers (for example, by wallet IDs) and not by their "real life identities."[155] At the same time, public blockchains are transparent, and every transaction and wallet address is published.[156]

Those who desire a more controlled system may opt for a *private* or *permissioned* blockchain, which are often operated in closed or restricted environments. Although the terms are frequently conflated and sometimes used interchangeably, there are important architectural and governance differences between permissioned and private models.

150 *See generally* Faisal Haque Bappy, EunJeong Cheon & Tariqul Islam, *Centralized Trust in Decentralized Systems: Unveiling Hidden Contradictions in Blockchain and Cryptocurrency*, arXiv (May 10, 2025), https://arxiv.org/pdf/2505.06661.

151 Tracy Wang, *FTX Exchange Halts All Crypto Withdrawals*, CoinDesk (Nov. 8, 2022), https://www.coindesk.com/business/2022/11/08/ftx-exchange-halts-all-crypto-withdrawals (last visited Jan. 15, 2026).

152 Politou, *supra* note 149.

153 Roy Lai & David Lee Kuo Chuen, *Blockchain – From Public to Private*, *in* 2 Handbook of Blockchain, Digital Finance, and Inclusion 145, 153 (David L. K. Lee & Robert Deng eds., 2018), https://doi.org/10.1016/B978-0-12-812282-2.00007-3.

154 *Id.* at 147.

155 *See* Unal Tatar, Yasir Gokce & Brian Nussbaum, *Law Versus Technology: Blockchain, GDPR, and Tough Tradeoffs*, 38 Comput. L. & Sec. Rev. 1, 3 (2020), https://doi.org/10.1016/j.clsr.2020.105454.

156 Jaekyu Lee et al., *Blockchain-Based One-Off Address System to Guarantee Transparency and Privacy for a Sustainable Donation Environment*, 10 Sustainability, no. 12, art. 4422, at 153 (2018), https://www.mdpi.com/2071-1050/10/12/4422.

FIGURE 3. Attributes of blockchains

	Private	Permissioned (Consortium)	Public-permissionless
Governance	Centralized	Shared among consortium members	Decentralized
Accessibility to users	Closed	Closed to external parties, open to consortium members	Open
Participation rights	Defined and restricted by operator	Restricted to consortium members based on roles	Open participation, subject to protocol-level consensus rules
Identification requirements	All users are identified	Member organizations are identified	Pseudonymous
User base	Very limited	Limited to consortium members	Broad

A ***permissioned blockchain*** refers specifically to a ledger in which meaningful participation (executing transactions, validation, or even submitting changes) is restricted to a set of authorized entities —in effect, "[running] a blockchain among a set of known, identified participants."[157] These entities are occasionally (but not always) referred to as consortiums. This model offers extremely granular control over operations and governance, and it is useful in environments in which the hope is for "secure . . . interactions among a group of entities that have a common goal but which do not fully trust each other."[158] On permissioned blockchains, validators[159] typically must undergo identity verification or formal onboarding procedures comparable to those used in regulated environments, though not necessarily to full Know-Your-Customer ("KYC") processes as applied by financial institutions.[160] Different network participants may enjoy varying levels of access to data and functionality based on their roles and permissions within the network.[161] Hyperledger Fabric and R3 Corda are among the most widely adopted permissioned blockchain platforms, with uptake concentrated primarily among enterprise users and with substantial deployment at scale.[162]

In contrast, **private blockchains** are designed to limit both participation and control, often to a single organization or a tightly controlled group.[163] In a private network, the network operator owns the data, which is typically "not . . . available to anyone outside of the

157 Elli Androulaki et al., *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*, 2018 Proc. of the Thirteenth EuroSys Conf. 1, 1 (Apr. 23, 2018), https://doi.org/10.48550/arXiv.1801.10228.

158 *Id.*

159 Conventionally, the term "miner" is usually applied in proof-of-work chains (network participants who try to extract a valuable resource to facilitate a transaction), whereas "validator" is most often applied to other consensus mechanisms, such as proof of stake (network participants who compete for the right to validate a transaction. That said, "validator" is probably the more common and general term.

160 *See Permissioned Blockchain*, Oracle, https://www.oracle.com/developer/permissioned-blockchain/ (last visited Jan. 15, 2026); *Blockchain Networks: Private, Public, & Permissioned*, CoinGeek, https://coingeek.com/blockchain101/private-vs-public-vs-permissioned-blockchain-a-comparative-guide (last visited Jan. 15, 2026).

161 *See id.* CoinGeek, *Blockchain Networks: Private, Public, & Permissioned*.

162 Toshendra Kumar Sharma, *Types of Blockchains Explained- Public vs. Private vs. Consortium*, Blockchain Council (June 6, 2024), https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/.

163 The implication here is that all private blockchains are permissioned (that is, they require permission or verification to join), but not all permissioned blockchains are private. However, unlike in permissioned blockchains, private blockchain network data is usually non-public. CoinGeek, *Blockchain Networks: Private, Public, & Permissioned*, *supra* note 160.

network."[164] The network operator typically exercises extensive control over the system, including the ability to "override, edit, or delete entries on the network."[165]

Both permissioned and private blockchains restrict participation in consensus and validation processes. However, while private blockchains also restrict access to the underlying data and concentrate control in a central operator, permissioned blockchains may either allow public read access or restrict data visibility, depending on their design choices and use cases.

Some commentators do not regard private and permissioned blockchains as "true" blockchains and classify them instead as a "subclass of Distributed Ledger Technologies,"[166] along with, but distinct from, public blockchains.[167] Each model involves different design tradeoffs. For example, it has been argued that, when designing a private blockchain, "making trustlessness the overarching design principle is neither necessary nor useful."[168] Permissioned blockchains may nonetheless be vulnerable to forms of collusion or majority control analogous to 51% attacks, although the relevant threat models, incentives, and governance responses differ from those applicable to public blockchains *(See below section 5.3.)*. In a classic 51% attack, a party that gains control of more than half of a network's total validation power can potentially manipulate transaction ordering or consensus outcomes.[169]

2.2. CRYPTOGRAPHIC FOUNDATIONS

Blockchain transactions are permanently recorded on a ledger in chronological sequence. Each block contains a unique cryptographic hash that links it to the previous block and secures its place in the chain.[170] Except for the genesis block, each block embeds the hash of the preceding block in its header, creating a tamper-evident structure. The explanations provided here primarily use the Bitcoin blockchain as an illustrative example.

2.2.1. Hashing

Hashing is perhaps the most important cryptographic principle underpinning blockchains *(See Appendix 1)*. A *cryptographic hash function*[171] (or simply "hash function") refers to a mathematical operation that accepts an input of any length and deterministically returns a random-looking output of fixed-length.[172] While it is computationally straightforward to generate this output from a given input, it is exceedingly difficult to reverse the process —that is, to determine the original input from the output alone.

The input can be letters, numbers, or special characters; it can be well-formed words and sentences, absolute gibberish, or even binary code. Upon accepting this input,

164 CoinGeek, *Blockchain Networks: Private, Public, & Permissioned*, *supra* note 160.

165 *Id.*

166 A distributed ledger is "a type of distributed database that records transactions between entities." Distributed ledgers record transactions on distributed databases as opposed to centralized databases. The phrase "distributed ledger technology" simply refers to a technology that "enables the realization and operation of distributed ledgers." Ali Sunyaev, Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies 269 (2020).

167 *See* Oleksii Konashevych, *Why 'Permissioned' and 'Private' are not Blockchains* 2-10 (Nov. 29, 2019), http://dx.doi.org/10.2139/ssrn.3496468.

168 Elias Strehle, *Public Versus Private Blockchains* 2 (Blockchain Rsch. Lab, Working Paper No. 14, 2020), https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf.

169 Politou, *supra* note 149. These attacks pose a serious threat to blockchain network security and integrity; a party that controls over 50% of the computational power can reverse transactions, prevent confirmations of new transactions through denial of service attacks, or modify the blockchain by invalidating or altering blocks. *See* Frank Hofmann et al., *The Immutability Concept of Blockchains and Benefits of Early Standardization*, 2017 ITU Kaleidoscope Tech. Symp. 1, 2 (2017), https://www.itu.int/en/ITU-T/academia/kaleidoscope/2017/Documents/poster/P.5.pdf.

170 *See* Tatar, Gokce & Nussbaum, *supra* note 155, at 2-5.

171 Technically, there is a distinction between "hash functions" and "cryptographic hash functions." In a blockchain context, where only cryptographic hash functions are typically in play, it is common to drop the "cryptographic" label for convenience and readability.

172 It is a "mathematical transformation that takes a message of arbitrary length and computes a fixed length value" such that it is easy to compute the *output* but extremely hard—if given only the output—to find the *input*. Kirti Aggarwal & Harsh K. Verma, *Hash_RC6 — Variable Length Hash Algorithm Using RC6*, 2015 Int'l Conf. on Advances in Comput. Eng'g & Applications 450, 450 (2015), https://doi.org/10.1109/ICACEA.2015.7164747.

the hash function, based on an algorithm that is specially designed to obscure the input, calculates an output that looks completely random. Below is an example of how an input (here, a phrase that says "Good Morning") using a hash function called SHA-256 produces an obscure output:

FIGURE 4. Example of hash algorithm functionality

Input	Output
Good morning	752c3fa953643312e67d82f2cf93bc9db-e5465d27f8f0ae0e4c94551666a906b

The above illustrates how a hash algorithm functions: A brief preimage (the input) is put through the SHA-256 hashing algorithm to produce a random string of numbers and letters (the output).

A good hash function ensures that the input is a secret unless it is intentionally revealed, while simultaneously ensuring that nobody can generate a specific hash without knowing the exact —down to the character— input. Hash functions are designed to make it difficult (to the point of being functionally impossible) to look at a hash *output* and determine the input or, indeed, anything at all about the input.[173]

2.2.2. Public Key Cryptography

Blockchain users employ pseudonymous cryptographic identifiers that may persist across transactions and are not tied to the real-world entity behind them. In most blockchain systems, this identifier is not the public key itself but an address derived from a public key using *public key cryptography* (PKC). PKC is a cryptographic system that generates a mathematically linked pair of keys: a public key and a private key *(See Appendix 2)*. The public key is mathematically linked to the private key such that deriving the private key from the public key is computationally infeasible, and each private key corresponds to a unique public key. The public key is intended to be shared widely, while the private key must remain secret.

Within blockchain-based systems, addresses derived from public keys serve a role analogous to that of an identification number, account number, or pseudonymous username. Participants interact with the holder's address, for instance, by sending transactions or, in some systems, encrypted messages addressed to that identifier. The private key enables the holder to cryptographically demonstrate that a given action (such as authorizing a transaction) is legitimate and originated from the rightful controller of the associated public key by producing a valid digital signature. Importantly, control over a private key confers effective control over the associated assets, but does not necessarily correspond to legal ownership in a formal sense.

The loss or compromise of private keys can lead to irreversible consequences. Instances of individuals misplacing or losing access to their private keys have, at times, resulted in the permanent loss of substantial digital asset holdings.[174] As one example, British IT professional James Howells discarded a hard drive containing 8,000 bitcoins in 2013.[175] At the time, the value of the bitcoins was roughly $800,000–$1,000,000. By the mid-2020s,

173 *See generally* Burton Rosenberg, *Perfect Secrecy and Adversarial Indistinguishability*, Univ. of Miami (Jan. 27, 2018), https://www.cs.miami.edu/home/burt/learning/csc609.182/perfect-secrecy-notes.pdf, for more information on perfect secrecy and the mathematical formulations for obtaining adversarial indistinguishability. Perfect secrecy is when the coded message does not reveal any information about the input. Adversarial indistinguishability is a similar concept: It is a lesser version of secrecy in which someone intercepting the coded message cannot distinguish between encryptions of two chosen messages with probability better than random guessing.

174 Jeffrey Voas & Nir Kshetri, *Lost and Never Found*, 54 Computer 12, 12 (2021), https://doi.org/10.1109/MC.2021.3055712.

175 Ali Watkins, *In Yearslong Search for Lost Bitcoin, a Final Proposal: Let Me Buy the Landfill*, N.Y. Times (Feb. 13, 2025), https://www.nytimes.com/2025/02/13/world/europe/bitcoin-wales-james-howells-landfill.html. Some sources report Mr. Howells had 7,500, not 8,000 bitcoins, *see* D.T. Max, *Half a Billion in Bitcoin, Lost in the Dump*, The New Yorker (Dec. 6, 2021), https://www.newyorker.com/magazine/2021/12/13/half-a-billion-in-bitcoin-lost-in-the-dump.

those bitcoins would have been worth many millions of dollars.[176] Similarly, Stefan Thomas, a San Francisco-based programmer, lost access to 7,002 bitcoins after forgetting the password to his USB bitcoin wallet.[177]

More broadly, cryptographic governance systems illustrate a structural tradeoff: strong security, immutability, and anti-collusion guarantees can make systems fragile to human error, with potentially severe consequences. This vulnerability is not unique to blockchains. In one instance, an organization conducted an election using a cryptographically verifiable online voting system in which the decryption key was split among multiple trustees. One trustee permanently lost their key share, rendering it technically impossible to decrypt or verify the final tally. Despite otherwise proper voting procedures, the election had to be annulled.[178]

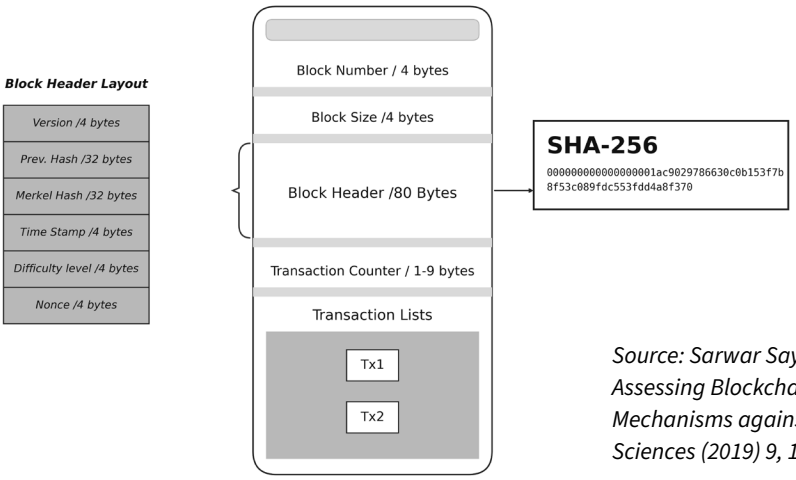
2.2.3. Blocks

The fundamental unit of data storage in a blockchain is called a "block." All Bitcoin blocks follow a specific structure. In practice, this structure is encoded as a software object. A Bitcoin block is composed of two main components: a block header and a list of transactions. A very simplified way to present this structure is to distinguish (i) the block header and (ii) the Transactions *(See below Figure 5)*. The Block Hash is not itself a component of the block but a cryptographic identifier derived from the block header.

1. Block Header

The block header contains metadata that describe the specific block, including the hash of the previous block, a timestamp, a difficulty target, cryptographic data that commits to the transactions included in the block, and the "nonce." Unlike some other distributed systems, Bitcoin does not include an explicit "block number" in the block header. Instead, blocks are identified by their hash, and their position in the blockchain (often referred to as "block height") is inferred from their place in the chain rather than explicitly encoded.

FIGURE 5. Simplified architecture of a Bitcoin block



Source: Sarwar Sayeed & Hector Marco-Gisbert, Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences (2019) 9, 1788, Figure 1. CC BY 4.0.

176 *See Live Bitcoin (BTC-USD) Price Chart*, NASDAQ, https://www.nasdaq.com/market-activity/cryptocurrency/btc (last visited Jan. 15, 2026) (listing the price per bitcoin as of the date and time of writing at $119,347.00).

177 Danielle du Toit, *Stefan Thomas: The Man Behind Bitcoin's Lost Millions*, COINPAPER (Jan. 14, 2025), https://coinpaper.com/6899/stefan-thomas-the-man-behind-bitcoin-s-lost-millions.

178 Dan Goodin, *Cryptography Group Cancels Election Results After Official Loses Secret Key*, ARS TECHNICA (Nov. 21, 2025) https://arstechnica.com/security/2025/11/cryptography-group-cancels-election-results-after-official-loses-secret-key/

Block height is conceptually similar to a page number in a book, as it reflects a block's sequential position within the blockchain. However, miners do not rely on block numbers to attach a newly discovered block. Rather, they reference the hash of the previous block, which uniquely identifies the block they are extending *(See Figure 6 for a visualization of a "chain" of blocks)*. This mechanism imposes a linear and coherent ordering on the blockchain. This ordering is crucial, particularly because the sequence in which transactions are confirmed determines their validity under the consensus rules.

The network determines the canonical ordering of transactions through block inclusion and consensus, not through block numbering. For example, suppose an (imaginary) Bitcoin owner, Alice, attempts to send 0.5 bitcoin to Bob and another 0.5 bitcoin to Charlie while her wallet contains only 0.7 bitcoin. Alice may broadcast both transactions to the network, but only one can ultimately become part of the canonical chain. Once miners include one transaction in a valid block and the network accepts that block through its consensus mechanism, that transaction becomes authoritative. The conflicting transaction is then rejected as a double spend. Block inclusion through consensus —rather than an explicit block number— establishes this canonical ordering of events.

In addition to referencing the previous block, each block header contains the hash of the previous block's header, not the entirety of the preceding block's data. This cryptographic pointer links each block to its predecessor and is the foundational mechanism by which blocks are "chained" together to form a blockchain.

Finally, the block header includes a special numerical field known as the "nonce." A nonce (short for "number used once") is an essential element of the mining process in proof-of-work (PoW) systems, such as Bitcoin *(See below section 2.3.1.)*.[179] It is a variable that miners repeatedly modify in order to generate a valid hash for a new block.

2. Block Hash

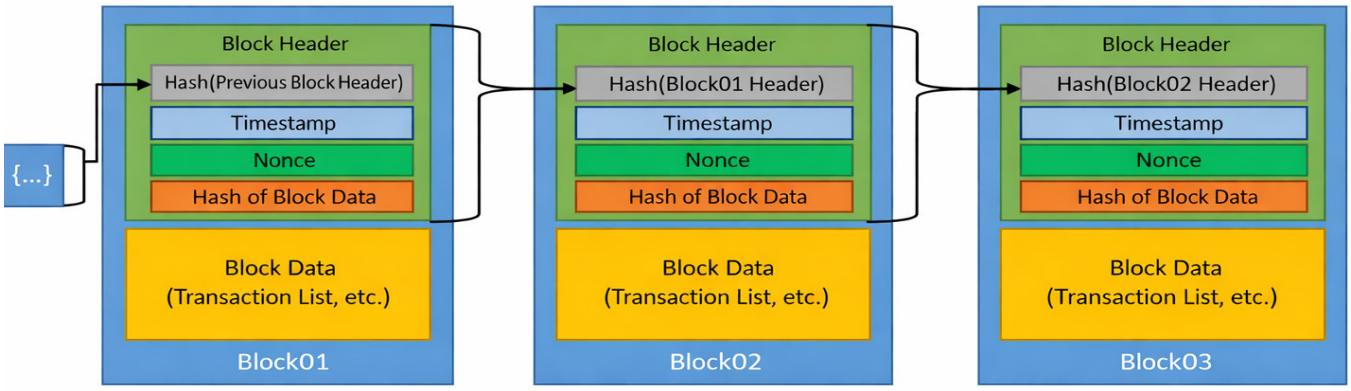
The Block Hash is not a component of the block like the header or the transactions. Rather, it is the cryptographic fingerprint obtained by hashing the block header. In Bitcoin, the block hash is computed exclusively from the block header, which cryptographically commits to the full set of transactions included in the block. If any single bit of data in the block header —or in the transactions to which it commits— is altered, the resulting Block Hash will change. The hash of each block is then included in the header of the next Bitcoin block in the sequence as the new "Hash of the Previous Block."

3. Chain of Blocks

A blockchain, as the name suggests, is a chain of blocks. As each block is finalized, its header is hashed, and this hash is included in the header of the next block *(See Figure 6, below)*:

179 Shivam Sharma, Sajal Jain & B.R. Chandavarkar, *Nonce: Life Cycle, Issues and Challenges in Cryptography*, *in* ICCCE 2020: Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering 183-195 (Amit Kumar & Stefan Mozar eds., 2020), https://doi.org/10.1007/978-981-15-7961-5_18.

FIGURE 6. Chain of blocks



Each block's hash is included on its original block and in the next block's Header, chaining the blocks together. Making even a small change to an early block will change its hash and the hashes of every subsequent block, including the most recent. Adapted from: NIST, Blockchain Technology Overview, NISTIR 8202 (2018), Figure 3. Public domain.

Because cryptographic hashes are extremely sensitive to changes in their input, altering even a single bit of data in Block #2034 will produce a different Block Hash. This, in turn, changes the "Hash of the Previous Block" field in Block #2035, which alters its Block Hash, and so on. This cascading effect propagates forward through the entire chain, regardless of how many blocks have been added since the alteration.

As a result, the hash of the most recent block serves as a compact cryptographic commitment to the entire preceding history of the blockchain.[180] While full verification requires recomputing hashes and validating consensus rules, the presence of a correct "Hash of the Previous Block" field in a newly added block demonstrates that it is building on an unaltered version of the chain. A version of the blockchain with even a single altered bit anywhere in its history would yield a completely different final block hash and would, therefore, be rejected by network participants.

2.2.4. Transactions

Within the context of cryptocurrencies such as Bitcoin, "transactions" can be understood as cryptographically signed instructions that reassign control over digital value from one party to another. As users (e.g., holders of coins) submit proposed transactions to the network, these transactions are collected into blocks. A transaction is considered confirmed once it has been included in a block and becomes increasingly difficult to reverse as additional blocks are added to the blockchain.

On the Bitcoin blockchain, control over a coin is defined by cryptographic spending conditions associated with an address. If a bitcoin is associated with an address such as "3xR…Tw2,"[181] anyone can observe on the blockchain

180 *See* Esthon Medeiros Jr., *Blocks, Chains, and Hashes*, MEDIUM (Nov. 30, 2023), https://medium.com/%40esthon/blocks-chains-and-hashes-b3bc323b978e. *See also* Rosco Kalis & Adam Belloum, *Validating Data Integrity with Blockchain*, PROCESS PROJ. 1, 3 (2019), https://www.process-project.eu/wp-content/uploads/2019/11/Validating-data-integrity-with-blockchain-UvA.pdf.

181 Different blockchains use slightly different protocols for generating keys. As a *very* general rule, Ethereum keys/addresses/etc. will tend to begin with "0x" and contain the letters a-f and the numbers 0-9, while Bitcoin keys/addresses can use a wider variety of letters and numbers. It is common, but by no means required, for Bitcoin addresses to begin with "bc1."

that the value of that bitcoin is locked to that address. But no information about the real-world identity of the controller of that bitcoin is revealed. The network does not determine who owns the bitcoin in a personal sense; rather, it verifies whether a proposed transaction satisfies the cryptographic conditions required to spend it. Only the party controlling the corresponding private key can generate the valid digital signature necessary to meet those conditions. The private key itself is never disclosed, and the probability of guessing it is computationally negligible.

Each unit of bitcoin is subject to a cryptographic spending condition (often described as an "encumbrance") that prevents it from being spent unless the required conditions are met. To transfer bitcoin, a user constructs a transaction that consumes previously unspent outputs and creates new outputs subject to new cryptographic conditions. This transaction includes a proof —in the form of a digital signature— that the sender is authorized to spend the referenced outputs. The signed transaction is then submitted to the network for validation.

Submitting a transaction places it into a pool of other unconfirmed transactions, commonly referred to as the "mempool" (short for memory pool). These pending transactions await inclusion in a block, and the time required for confirmation can vary significantly. Transactions in the mempool are not globally ordered, and their eventual inclusion in a block depends on factors such as transaction fees, network congestion, and miner or validator selection policies. Once a transaction is included in a valid block and accepted by the network, it becomes part of the canonical transaction history.

2.3. CONSENSUS MECHANISMS

Any proposed addition to the blockchain ledger is subjected to cryptographic validation under the predefined consensus protocol. This is to confirm the transaction's validity and to ensure agreement across the network before the transaction is permanently added to the ledger. Within this framework, one of the central challenges in blockchain design is the development of a reliable *consensus mechanism* to ensure that the version of the ledger agreed upon by the majority of participants is treated as authoritative.

Implementing a system that can consistently reach consensus under real-world conditions is complex. It requires a mechanism that allows all participants —most of whom do not know and almost certainly do not trust each other— to agree on the current state of the ledger. This challenge is particularly acute in the context of a monetary ledger, where the integrity of the system is critical. Not all participants act in good faith. Some may attempt to manipulate, disrupt, or undermine the system. Additionally, many disruptions may result from unintended causes, such as accidents, hardware failures, network interruptions, or latency-induced inconsistencies. A robust consensus protocol must, therefore, be resilient to both malicious attacks and unintentional mistakes, ensuring that the ledger remains accurate and trustworthy despite adverse conditions.

2.3.1. Proof of Work

Bitcoin employs a consensus mechanism known as *proof of work* (PoW), which plays a central role in establishing and maintaining agreement across the network on a valid and consistent record of transactions. Proof of work (PoW) performs several key functions: It provides a method for selecting which node is granted the right to append a new block to the blockchain. It offers economic incentives to participants who contribute to the network's

decentralization and security, thereby aligning their financial interests with the maintenance of an accurate and tamper-resistant ledger. And it ensures that any malicious actor who attempts to promote an invalid version of the ledger is likely to expend significant resources in vain, as the network will reject blocks that deviate from consensus rules.

2.3.1.A. The Proof-of-Work Mechanism

Proof of work provides a probabilistic method for selecting the node entitled to append a new block to the ledger. This selection is not random in a strict sense, but rather weighted by computational power: Nodes with greater hashing capacity are more likely, over time, to be selected. To participate, a node must demonstrate the expenditure of computational resources, and its probability of success is approximately proportional to its share of the total computational power of the network.[182]

For each new block, participating nodes (commonly referred to as *miners*) independently construct a candidate block. This process begins once the previous block has been added to the blockchain. Each candidate block includes standard metadata, such as a reference to the cryptographic hash of the preceding block, a timestamp, a coinbase transaction specifying the block reward payable to the miner, and other protocol-defined fields.[183] Miners also select and order transactions from the pool of pending transactions submitted by users. An honest miner will construct a block that complies with protocol rules, whereas a malicious miner may attempt to include invalid transactions, such as those involving double-spending. The network will reject such blocks, however, upon verification.[184] Although candidate blocks typically share much of their structure —particularly the block header— they may differ in the selection and ordering of transactions or in other variable fields. As a result, multiple distinct candidate blocks are constructed and completed simultaneously.

Once a candidate block is assembled, the miner enters the proof-of-work phase. This involves repeatedly computing cryptographic hash functions over the block header while varying a value known as the *nonce* (and, where applicable, other mutable fields), in an attempt to produce a hash output that satisfies a predefined difficulty target. The difficulty target specifies an upper bound on acceptable hash values and is commonly expressed (for ease of exposition) as requiring a certain number of leading zeros in the hash output.[185]

Finding such a hash is computationally demanding and effectively requires a brute-force search. The first miner to discover a hash that meets the difficulty requirement is deemed to have successfully completed the proof of work. That miner gains the right to append its candidate block to the blockchain and broadcast the block to the network. Other nodes independently verify the validity of the block and, if it complies with the protocol rules, accept it as the next block in the chain. The process then repeats for the subsequent block.

Fundamentally, PoW is a mechanism for demonstrating, with an extremely high degree of certainty, that a participant has "performed a certain amount of computational work in a specified interval of time."[186] In this context, "work" takes the form of computing power, whereas other consensus mechanisms may rely instead on financial stake, storage capacity, or time.

182 *See* Nakamoto, *supra* note 125, at 2-3.

183 Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies, 23-25 (2016) (describing the structure of a block header and the included metadata fields), https://www.lopp.net/pdf/princeton_bitcoin_book.pdf.

184 *See* Nakamoto, *supra* note 125, at 3–4 (describing the chain of proof-of-work as containing «the history of control» and requiring verification of all prior blocks).

185 Technically, this is slightly inaccurate. In Bitcoin, the goal is not to find a hash with a specified number of leading zeros, it is to find a hash output that is lower than a specified value. However, this correlates pretty closely to the number of leading zeros. Saying "X number of leading zeros" is easier to visualize, so it is a good way to think about what is actually happening in Proof-of-Work.

186 Markus Jakobsson & Ari Juels, *Proofs of Work and Bread Pudding Protocols (Extended abstract)*, *in* Secure Information Networks 258, 259 (Bart Preneel ed., 1999), https://doi.org/10.1007/978-0-387-35568-9_18.

2.3.1.B. Economic Incentives to Mining

Bitcoin's proof-of-work mechanism creates strong economic incentives for participation in mining. Miners who successfully append a new block to the blockchain receive a reward composed of newly issued bitcoins and transaction fees. This reward structure encourages competition among miners, as the probability of obtaining the reward is proportional to the miner's share of the network's total computational power.

Mining is, however, a capital- and energy-intensive activity. The expected cost of producing a block depends on several factors, including the price of electricity, the efficiency and depreciation of specialized mining hardware, cooling and infrastructure expenses, and the prevailing network difficulty. These costs vary widely across jurisdictions and operators, giving rise to geographic and industrial concentration in regions with access to inexpensive energy and favorable operating conditions.

At any given time, mining is economically rational only if a miner's expected rewards —realized probabilistically and often through participation in mining pools— exceed its operating and capital costs. Consequently, mining activity is overwhelmingly undertaken by profit-seeking entities, and the level of participation in the network adjusts dynamically in response to changes in bitcoin prices, block rewards, transaction fees, and mining difficulty.

FIGURE 7.

Bitcoin's monetary policy

In the original codebase, Satoshi Nakamoto set a hard cap of 21 million bitcoins, ensuring that the total supply would be finite. Between its launch in 2009 and 2025, nearly 20 million bitcoins were issued. New bitcoins are introduced into the system through the process of mining. For each new block, the entity that first solves a cryptographic puzzle earns the right to append that block to the end of the blockchain and receive a block reward of newly created bitcoins.

Satoshi Nakamoto was almost certainly the first entity to run the Bitcoin software, thereby bootstrapping the network and mining the first block, known as the Genesis Block.[187] This block specified a reward of 50 bitcoins. In Bitcoin's original design, the block reward was set to decrease over time according to a predetermined schedule. Specifically, the reward is reduced by half every 210,000 blocks —approximately every four years— in a process commonly referred to as a *halving*. As a result, the block reward fell from 50 bitcoins to 25 bitcoins in 2012, then to 12.5 bitcoins in 2016, and to 6.25 bitcoins in 2020. In 2024, the most recent halving further reduced the reward to 3.125 bitcoins per block.

By front-loading issuance in the early years of the network, this reward structure provided strong incentives for early participation at a time when the value of bitcoin was highly uncertain, while ensuring that the rate of new bitcoin creation would decline predictably over time.[188] Under the issuance schedule, the block reward will continue to decline and is expected to cease entirely around the year 2140.[189]

187 Benedict George, *The Genesis Block: The First Bitcoin Block*, CoinDesk (Jan. 3, 2023), https://www.nasdaq.com/articles/the-genesis-block:-the-first-bitcoin-block. Technically, this is a quick sketch of the process. To really conceptualize the early days of Bitcoin, it is probably easiest to think about these coins as being owned by Satoshi, as this is the common practice. In reality, for reasons that are not clear, Satoshi chose to send these first 50 bitcoins to an address that does not have an associated private key and, therefore, is not controlled by anyone.

188 Fidelity International, Bitcoin Halving: A Tale of Limitless Innovation 1 (Mar. 2024), https://www.fidelity.fi/static/master/media/pdf/download-material/bitcoin-halving-a-tale-of-limitless-innovation.pdf

189 Bitcoin Block Reward Halving Countdown, Bitcoin Block Half, https://www.bitcoinblockhalf.com/ (last visited Jan. 15, 2026).

2.3.1.C. Reliability of PoW

Proof of work creates a system in which rational actors are, under normal assumptions, incentivized to behave honestly. The high cost associated with finding and submitting a valid block creates a strong financial incentive to comply with the protocol rules. If a node mines a block with a valid proof of work but includes invalid transactions —such as transactions lacking the required digital signatures or attempting double-spending— that block will almost certainly be rejected by other nodes during verification. In such cases, the miner receives no reward, and the computational resources expended in producing the block are wasted. Given the substantial cost of the computation required to mine a block, a miner with the capacity to participate competitively in Bitcoin mining is unlikely, as a matter of expected value, to expend significant resources on producing a block that is highly likely to be rejected. In this sense, protocol violations are discouraged, not through formal sanctions, but through the loss of rewards and the opportunity cost of wasted computation.

Moreover, in Bitcoin, miners follow *Nakamoto Consensus*, under which the default rule is to build on the chain that represents the greatest cumulative proof of work. As originally described by Nakamoto, "The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it"[190] *(See Figure 9)*. Under the Nakamoto consensus, an adversary who attempts to alter the transaction history —for example, by reversing a past transaction— must construct an alternative version of the blockchain that grows faster than the chain produced by honest miners. This would require the attacker to control a majority of the network's total hashing power, a scenario commonly referred to as a *51% attack*.[191] On a large network such as Bitcoin, mounting such an attack is generally considered economically prohibitive: Acquiring and operating sufficient computational resources would entail substantial and ongoing costs, with no guarantee of success.

An attacker controlling less than half of the network's hash power is statistically unlikely, over time, to outpace the combined efforts of honest miners, causing the attacker's competing chain to fall behind and, ultimately, be discarded by the network. Consequently, while dishonest behavior is not impossible in proof-of-work systems, it is both extremely costly and highly prone to failure, making honest participation the most rational and feasible strategy for miners under standard conditions.[192]

2.3.2. Proof of Stake

Proof of stake (PoS) is an alternative to proof of work that has become increasingly adopted in modern blockchain systems and has demonstrated sufficient security and reliability in practice to serve as a consensus mechanism in several major networks.

2.3.2.A. The Proof-of-Stake Mechanism

A proof-of-stake blockchain replaces computational effort with economic stake as the critical resource underpinning consensus. As its name implies, proof of stake relies on stake —typically a quantity of the blockchain's native cryptocurrency— to determine participation in block production and validation. At a high level, PoS replicates the economic logic of proof of work but substitutes computational expenditure with stake (i.e., the network's native token) as the basis for securing the network.

190 Nakamoto, *supra* note 125, at 3.

191 Andreas M. Antonopoulos & David A. Harding, Mastering Bitcoin: Programming the Open Blockchain, 288-289 (3rd ed. 2023), http://103.203.175.90:81/fdScript/RootOfEBooks/E%20Book%20collection%20-%202025%20-%20C/AI/Mastering_Bitcoin_Programming_the_Open_Blockchain,_3rd_Edition.pdf

192 However, powerful mining pools may destabilize the system., Malik, et al. (2022) showed that when large miners dominate PoW mining, they may tacitly collude to drive up transaction fees and extract economic rents, Nikhil Malik, et al. *Why Bitcoin Will Fail to Scale?* (Jan. 11, 2022), https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2021.4271

In a PoS system, participants who wish to take part in consensus "stake" a quantity of tokens as collateral. The likelihood of being selected to propose or validate the next block is generally proportional to the amount of stake committed. Those who participate in this process are known as "validators," as they attest to the validity of transactions and blocks recorded on the blockchain. Because validators' financial exposure is directly tied to the value of the network's native token, PoS mechanisms may create strong incentives for participants to act in ways that preserve the integrity and long-term value of the system.

In a simplified PoS model, validators deposit tokens into a smart contract, and block proposal rights are allocated in proportion to each validator's share of the total staked tokens. For example, if a total of 100 tokens are staked across multiple validators, a validator who has committed 20 tokens would, all else equal, have a 20 percent probability of being selected to propose the next block.[193] The selected validator typically receives transaction fees and, in some systems, an additional block reward. In practice, modern PoS systems employ more complex mechanisms involving randomness, validator committees, and time-based epochs, but the underlying principle of stake-weighted participation remains central.

The stake committed in a PoS system serves as a scarce, valuable, and verifiable resource that can be bonded and placed at risk in exchange for participation in consensus.[194] As in proof-of-work systems, the threat of unrecoverable losses operates as a deterrent against dishonest or malicious behavior. In PoS, however, these losses arise not from wasted computational effort but from explicit penalties imposed on staked assets. Absent such penalties, PoS systems would be vulnerable to what is known as the "Nothing at Stake" problem, whereby validators could rationally attempt to support multiple competing chains at little cost.[195] To address this risk, modern PoS designs incorporate enforcement mechanisms —most notably "slashing"— under which validators who propose or attest to invalid or malicious blocks forfeit a portion of their staked assets or are excluded from future participation.[196] These mechanisms introduce real economic consequences for misconduct and are central to the security of contemporary proof-of-stake systems.

2.3.2.B. Ethereum Proof of Stake

The Ethereum blockchain was launched on July 30, 2015. Originally, it operated as a proof of work (PoW) blockchain, similar to Bitcoin.[197] However, its developers designed a proof of stake (PoS) system and completed the full transition to PoS on September 15, 2022.[198] This event, commonly referred to as "The Merge," marked a pivotal milestone both for Ethereum and for the broader blockchain ecosystem.[199] As of January 2026, Ethereum is the largest proof-of-stake blockchain worldwide, both in terms of market capitalization and overall economic activity.[200] Understanding the mechanics of Ethereum's PoS system is, therefore, essential for comprehending contemporary developments in blockchain technology.

193 These numbers are, of course, extremely simplistic. In the real world, there will be thousands of nodes, most of which have staked a tiny fraction of a percent of the total tokens staked.

194 Vitalik Buterin et al., *Combining GHOST and Casper*, arXiv, 3 (May 11, 2020), https://arxiv.org/abs/2003.03052; Vitalik Buterin, *Ethereum*: A Next-Generation Smart Contract and Decentralized Application Platform (2014), https://ethereum.org/en/whitepaper.

195 Léonard Lys et al., *Defending Against the Nothing-at-Stake Problem in Multi-Threaded Blockchains*, arXiv, 1 (Feb. 23, 2023), https://arxiv.org/abs/2302.10009.

196 *See* Ethereum Found., *Staking*, https://ethereum.org/en/staking/, Ethereum (last updated Oct. 8, 2025), https://ethereum.org/en/staking/ (describing «slashing» as the primary mechanism to enforce consequences for malicious validator behavior).

197 *See* Ethereum Found., *History of Ethereum*, Ethereum (last updated Dec. 4, 2025), https://ethereum.org/en/history/

198 *The Ethereum Merge: What It Is and Why It Is Important*, Holland & Knight (Sept. 15, 2022), https://www.hklaw.com/en/insights/publications/2022/09/the-ethereum-merge-what-it-is-and-why-it-is-important.

199 *Id.*

200 *See Top Proof of Stake (PoS) Coins Today By Market Cap*, Forbes, https://www.forbes.com/digital-assets/categories/proof-of-stake-pos/?sh=6916ae1f26f7 (last visited Jan. 8, 2026) (demonstrating that Ethereum has, by far, the largest market capitalization).

Ethereum's proof-of-stake consensus combines two distinct mechanisms: a *fork choice rule* for identifying the most current valid block, and a *finality mechanism* that determines which blocks are effectively irreversible. Under the fork choice rule, nodes select as canonical the chain that reflects the greatest weight of validator attestations.[201] In addition, under Ethereum's finality mechanism, a block becomes finalized once a supermajority of validators attest to it across multiple "epochs."[202] Finalized blocks are economically secured against reversal unless a substantial portion of the total ether staked is forfeited through slashing penalties (i.e., penalties for validators who acted inappropriately during the validation process).

This design offers stronger guarantees of irreversible consensus compared to the probabilistic finality inherent in PoW systems, such as Bitcoin. Indeed, in Bitcoin, transactions become increasingly secure as additional blocks are added on top of them, a process commonly quantified by waiting for a set number of "confirmations" (usually six in Bitcoin for the probability of reversal to become vanishingly small). In other words, in PoW systems, the deeper a transaction is embedded in the chain, the more difficult it is to undo, although a small probability of reversal always remains.

2.3.3. Other Consensus Mechanisms

While proof of work and proof of stake are probably the two consensus mechanisms with the most impact, a range of other mechanisms have been developed and adopted to varying degrees. Below are a few other consensus mechanisms:

- **Proof of Authority (PoA):** Proof of Authority is a consensus mechanism typically employed in permissioned or consortium-based networks *(See above, section 2.1.4.)*.[203] In this model, the responsibility for validating transactions lies with a limited set of pre-approved and identifiable validators who are selected on the basis of their reputation or institutional affiliation. In practice, validators —often referred to as authorities— do not stake a native token but their real-world identity and credibility, often subject to off-chain accountability mechanisms. PoA offers relatively high efficiency, as it is fast and does not demand intensive computational resources. Nevertheless, it is less decentralized than other mechanisms and requires participants to place significant trust in a small number of validators who exercise effective control over the consensus process.
- **Practical Byzantine Fault Tolerance (pBFT):**[204] Practical Byzantine Fault Tolerance reaches consensus by subjecting validators to multiple rounds of message exchange and voting. This architecture offers protections against a bounded number of malicious or malfunctioning nodes. pBFT is relatively fast and provides strong fault tolerance, but the consensus mechanics scale poorly as the number of validators increases, which in practice constrains the size of the validator set and limits decentralization.

201 *But see* Bessie Liu, *Ethereum Is Not Under Attack: Understanding MEV-Boost Relays*, Blockworks (Oct. 21, 2022), https://blockworks.co/news/ethereum-is-not-under-attack-understanding-mev-boost-relays. Many blocks on Ethereum today, before they are vetted by validators through proof of stake, pass through Maximum Extractable Value-Boost relays, which are intermediaries that verify and pre-build blocks for validators. There have been censorship concerns associated with these relays because some of them unilaterally screen and reject blocks with transactions they believe could be suspicious. *Id.* In some way, Ethereum is not fully uncensored, but its decentralized nature still aims to be censorship-resistant by design.

202 In blockchain systems, an "epoch" is a defined period of time or a fixed number of blocks during which the network performs specific operations related to consensus. In proof-of-stake Ethereum, an epoch currently consists of 32 slots (each slot lasting 12 seconds), making one epoch about 6.4 minutes. During an epoch, validators are assigned duties, such as proposing blocks and attesting to others' proposals. At the end of an epoch, the protocol aggregates these attestations to help determine finality.

203 *See generally* Shu-Ping Lu, Chin-Laung Lei & Meng-Han Tsai, *An Efficient Proof-of-Authority Consensus Scheme Against Cloning Attacks*, 228 Comput. Commc'ns 1 (2024), https://doi.org/10.1016/j.comcom.2024.107975.

204 *See generally* Miguel Castro & Barbara Liskov, *Practical Byzantine Fault Tolerance and Proactive Recovery*, 20 ACM Transactions on Comput. Sys. 398 (2002), https://doi.org/10.1145/571637.571640; Xu Hao et al., *Dynamic Practical Byzantine Fault Tolerance*, 2018 IEEE Conf. on Commc'ns & Network Sec. 1 (2018), https://doi.org/10.1109/CNS.2018.8433150.

- **Delegated Proof of Stake (DPoS):**[205] Delegated Proof of Stake is best thought of as a variant within the broader proof-of-stake family. In DPoS, token holders elect delegates (i.e., validators) who then validate transactions. This validator group is often fewer in number than in other PoS variants, thus enabling speed and scalability, while simultaneously concentrating validation and governance power and functionally centralizing the consensus process.
- **Proof of Burn**: An occasionally controversial consensus mechanism, Proof of Burn allows participants to earn validation rights by "burning" a certain amount of cryptocurrency (often by sending it to an address from which the tokens are irretrievable).[206] Participants demonstrate their investment in the blockchain by permanently destroying a portion of their cryptocurrency. By burning coins, participants signal their commitment to the network and obtain the right to compete for block validation. The more coins a participant burns, the more probabilistic validation power they hold and the higher their probability of being selected as the next block validator. Participants do not have to invest physical resources to show their commitment to the network, but the burning process relies on irreversible capital destruction as a security signal, raising concerns about economic efficiency and contributing to its limited practical adoption.[207]
- **Proof of Capacity, or Proof of Space**:[208] Proof of Space uses storage space as a scarce resource, such that validators are required to prove that they have allocated and pre-committed a certain amount of storage space to the network. As in other consensus mechanisms, the greater the amount of storage space allocated, the greater the probability of being selected as a validator. Proof of Space is often coupled with a time-based component designed to prevent intermittent participation to "ensure[] network security by verifying that participants are consistently maintaining their storage commitments rather than only providing space intermittently,"[209] creating the Proof of Space and Time (PoST) consensus mechanism. This approach reduces energy consumption relative to proof-of-work systems, though it still entails hardware-based participation costs.

2.3.4. Forking

In software development, "forking" refers to creating a copy of an existing codebase —that is, the entire body of source code for a particular software program, component, or application system. Typically, the motivation behind forking is to modify or extend the software in a different direction than the software developers originally intended. In the context of blockchains, forking carries a related but distinct meaning: It denotes the divergence of a single blockchain into two separate chains, each sharing a common history up to the point of divergence, after which their records evolve independently.

205 *See generally* Wangchun Li et al., *Delegated Proof of Stake Consensus Mechanism Based on Community Discovery and Credit Incentive*, 25 Entropy 1320 (2023), https://doi.org/10.3390/e25091320.

206 *See* Kostis Karantias, Aggelos Kiayias & Dionysis Zindros, *Proof-of-Burn*, *in* Financial Cryptography and Data Security 525-28 (Joseph Bonneau & Naia Heninger eds., 2020), https://www.research.ed.ac.uk/en/publications/proof-of-burn/.

207 *See Proof of Burn Explained*, Binance Acad. (Dec. 4, 2018), https://www.binance.com/en/square/post/43029.

208 *See generally* Giuseppe Ateniese et al., *Proofs of Space: When Space Is of the Essence*, *in* Security and Cryptography for Networks 538-57 (Michel Abdalla & Roberto De Prisco eds., 2014), https://ilariobonacina.github.io/publications/2014-ABFG-scn.pdf.

209 *Proof-of-Spacetime*, Ledger Acad. (May 26, 2025), https://www.ledger.com/academy/glossary/proof-of-spacetime.

2.3.4.A. Accidental Forks

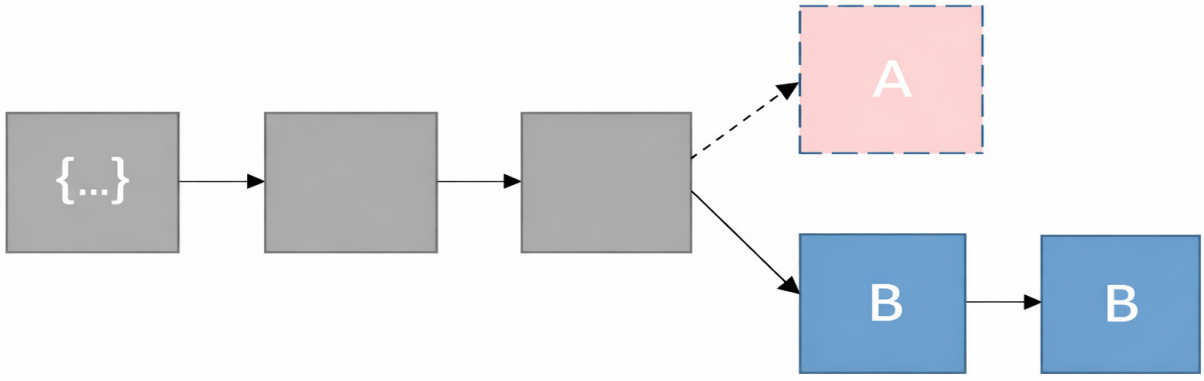
Accidental forks are temporary divergences that arise when two valid blocks are added to the blockchain at nearly the same time. Such forks occur occasionally as a result of network latency and the decentralized nature of block propagation. Blockchain protocols are designed to resolve these divergences automatically through their consensus mechanisms by determining which version of the blockchain is canonical.

Below is a simple representation of a blockchain with a single, linear sequence of blocks:

FIGURE 8. Linear relationship among blocks

In an idealized setting, once a miner finds a valid block, this information would be instantaneously propagated across the network, allowing all nodes to verify the block and immediately build upon it. In practice, however, block propagation takes time, and different miners may discover competing blocks referencing the same parent block (i.e., at roughly the same height).[210] As a result, different parts of the network may temporarily build on different branches.[211] When two blocks are broadcast to the network almost simultaneously, a temporary fork may occur, resulting in two competing versions of the blockchain. If such a situation were to persist indefinitely, it would lead to a permanent network split.

FIGURE 9. Orphaned blocks



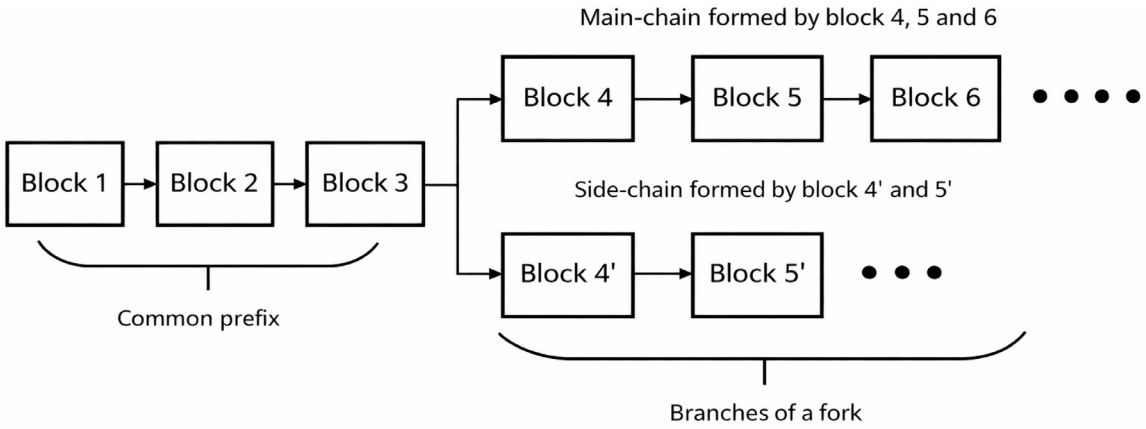
The blockchain above shows an "orphaned block" (A), following a fork in the original blockchain. For economical reasons, most miners will continue building on the canonical chain. Source: NIST, Blockchain Technology Overview, NISTIR 8202 (2018), Figure 5. Public domain.

210 Block height refers to a block's position in the chain, measured as the number of blocks preceding it (with the genesis block typically at height 0).

211 *See* Narayanan et al., *supra* note 183, at 60-61 (explaining that network latency and propagation delays inevitably lead to temporary forks when multiple miners find blocks nearly simultaneously).

During such temporary forks, it is possible for transactions to appear in one branch but not the other. For example, if Alice has 14 bitcoins in Block 2 and the chain splits after Block 3, one branch may record a transaction in which she transfers those bitcoins while the other does not:

FIGURE 10. A chain fork



The above diagram shows a blockchain with a clear chain fork after Block 3. Part of the network has accepted Block 4 as canonical and is continuing to build off of mini-chain formed by blocks 4, 5, and 6; the other half has accepted Block 4' as canonical and is continuing to build off of side-chain formed by blocks 4' and 5'. Source: Kaiyu Wang, Yan Wang & Zhenzhou Ji, Defending Blockchain Forking Attack by Delaying MTC Confirmation, IEEE Access, 2020, Figure 2. CC BY 4.0.

However, it is extremely rare for a chain to split exactly in half, and blockchain mechanics dictate that a chain with more resources (hashpower, stake, social weight, etc.) will almost certainly prevail. For instance, in PoW blockchains, one branch typically accumulates additional proof of work more quickly than the other and becomes the statistically dominant chain.

Ultimately, the protocol's consensus rules determine which branch prevails. In the Bitcoin network, nodes follow a consensus rule under which the chain representing the greatest cumulative proof of work is treated as canonical. When one branch receives an additional block before the other, it gains a probabilistic advantage and is recognized as the valid chain. Economically rational miners then switch to building on that chain, and the alternative branch is abandoned. The block on the losing branch remains a valid block but does not become part of the canonical chain. Such blocks are commonly referred to in non-technical discussions as "orphaned" blocks, though they are more precisely described in the technical literature as "stale" blocks.[212] Transactions included in these non-canonical blocks are returned to the "mempool" and may be confirmed again in subsequent blocks.

2.3.4.B. Intentional Forks

Intentional forks are deliberate modifications to a blockchain protocol, typically introduced to achieve specific objectives such as adding new features, improving functionality, correcting flaws or vulnerabilities, mitigating the effects of security breaches or exploits, or resolving ideological disagreements or conflicting visions within the community

212 Syamsul Rizal & Dong-Seong Kim, *Enhancing blockchain consensus mechanisms: A comprehensive survey on machine learning applications and optimizations*, 6(4) Blockchain: Research and Applications, 9 (Dec. 2025), https://doi.org/10.1016/j.bcra.2025.100302.

or among developers. Such forks are generally intended to be permanent and, when successful, result in two parallel chains that share a common transaction history up to the point of divergence and evolve independently thereafter. Intentional forks are commonly categorized as either "hard" forks or "soft" forks.

A *hard fork* involves protocol changes that are not backward-compatible. Nodes that do not adopt the updated software and continue running the previous version of the protocol are unable to validate blocks produced under the new rules. If both versions of the software continue to be used, the network splits into two separate and independent blockchains, each following its own consensus rules while sharing a common history up to the fork point. Notable examples include the divergence of Ethereum Classic (ETC) from Ethereum (ETH) following the DAO incident *(See below section 6.2.1.A. and below Figure 11)*[213] and Bitcoin Cash (BCH) forking from Bitcoin (BTC) to increase block size.[214]

A *soft fork*, by contrast, introduces changes that are backward-compatible. Nodes that have not upgraded can continue to participate in the network and accept newly produced blocks as valid because those blocks still satisfy the pre-existing protocol rules, even if non-upgraded nodes do not enforce the new constraints. As a result, the blockchain continues on a single chain, with the updated rules effectively enforced by a majority of upgraded participants. Notable examples in Bitcoin include Segregated Witness (SegWit) *(See below Figure 24)* and Pay-to-Script-Hash (P2SH).[215]

FIGURE 11.

The DAO fork (2016)

In 2016, an attacker exploited a vulnerability in the smart contract code of The DAO, allowing them to divert approximately one-third of the DAO's assets (about $60 million).[216] The DAO controlled roughly 14% of all circulating ETH at the time, raising concerns about the viability of the Ethereum network itself.[217] In response, a majority of participants to the Ethereum network —not just The DAO's members— adopted a "hard fork," a blockchain update that altered the transaction history to restore the network to its state prior to the attack. This created a new blockchain, forked off from the original, and effectively reversed the transactions associated with the hack. The original chain continued as "Ethereum Classic," while the majority of users followed the hard fork under the name "Ethereum."[218] As of Jan 9, 2026, one ETH is worth approximately $3,100 USD,[219] while one Ethereum Classic coin is worth approximately $12.5 USD.[220]

Because forking requires a sufficient degree of social coordination, it can function as a powerful governance mechanism within blockchain ecosystems. Regardless of how entrenched a project may appear, participants retain the ability to attempt to redirect its trajectory if they oppose the direction in which it is evolving. In practice, this dynamic has manifested on multiple occasions. For

213 A.K.M. Najmul Islam, Matti Mäntymäki & Marja Turunen, *Why Do Blockchains Split? An Actor-Network Perspective on Bitcoin Splits*, 148 Tech. Forecasting & Soc. Change 1, 1-2 (2019), https://doi.org/10.1016/j.techfore.2019.119743 (describing the Ethereum hard fork).

214 *Id.* at 2 (explaining the Bitcoin hard fork).

215 Cristina Pérez-Solà et al., *Analysis of the SegWit Adoption in Bitcoin* (2019), https://deic.uab.cat/~guille/files/papers/2018.recsi.segwit.pdf (explaining that SegWit was introduced in particular as a security enhancement feature to Bitcoin, but became controversial, leading to a split between users who adopted SegWit and those who did not).

216 Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 34-81207, 117 SEC Docket 745 (July 25, 2017), https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

217 *See Ethereum DAO Hack*, Bitstamp Learn (July 17, 2023), https://www.bitstamp.net/learn/crypto-101/ethereum-dao-hack/.

218 Ernesto Frontera, *A History of 'The DAO' Hack*, Coin Mkt. Cap, https://coinmarketcap.com/academy/article/a-history-of-the-dao-hack (last visited Jan. 15, 2026).

219 Historical Data for ETH-USD, Yahoo Finance, https://finance.yahoo.com/quote/ETH-USD/history/ (last visited Jan. 9, 2026).

220 Ethereum Classic Price, CoinMarketCap, https://coinmarketcap.com/currencies/ethereum-classic/ (last visited Jan. 9, 2026).

example, when a subset of Bitcoin participants sought to increase the maximum block size, they initiated a fork that resulted in Bitcoin Cash. Similarly, when members of the Steem community perceived a threat from a centralized actor acquiring a controlling share of the network's native tokens, they forked the blockchain to create Hive.[221]

2.4. BLOCKCHAIN ASSETS

At their core, blockchains operate as ledgers that record specific categories of information. This information may include records of ownership, transactional history, or the state of a computer program. In practice, however, public blockchains are most commonly used to record transactions involving the transfer of digital units between addresses. These digital units are not physical objects but data entries on the blockchain ledger. Despite being purely informational, they can carry functional significance. They may represent assets external to the blockchain (such as physical goods, claims, or legal rights) or acquire economic value within the blockchain ecosystem through supply and demand dynamics, thereby functioning as a form of money, a store of value, or a unit of account. As blockchain technologies have evolved, distinct categories of crypto-assets have become widely recognized. These assets can be classified broadly as either fungible or non-fungible coins or tokens.

2.4.1. Fungible Coins and Tokens

The majority of blockchain-based assets are fungible, meaning that each unit of the asset is interchangeable with any other unit of the same type. One bitcoin is identical in function and value to any other bitcoin, just as one euro is functionally equivalent to any other euro. If an individual places three bitcoins in escrow, that individual does not expect that the exact same three bitcoins will be returned; any three bitcoins of equivalent value will suffice. This principle of fungibility also applies to physical U.S. dollars, where lending a ten-dollar bill and receiving a different ten-dollar bill, or two five-dollar bills, is entirely acceptable. The same holds true for most commodities, publicly traded securities, and other standardized financial instruments.

Blockchain-based digital assets —commonly referred to as "crypto-assets," "cryptocurrencies," "cryptos," "coins," or "tokens"— do not have a single, universally accepted definition.[222] Terminology varies significantly across regulatory bodies, governments, and organizations worldwide. While the term "cryptocurrency" is widely used, the technical distinction between "coins" and "tokens" is often blurred in public discourse, even though these terms have distinct technical meanings.

2.4.1.A. Native Assets or Coins

Coins, such as bitcoin (BTC) and ether (ETH), are digital assets that are native to a particular blockchain protocol.[223] Native assets are created as an integral component of a blockchain and are directly governed by that chain's consensus and validation rules. In most cases, such assets are associated with their own blockchain and consensus mechanism, although newer architectures (such as layered or modular systems) may blur these distinctions. Coins typically serve as a medium of exchange, a store of value, and, in some cases, a unit of account within their respective ecosystems.[224] Historically, however, they have exhibited high price volatility, with significant fluctuations in market value *(See section 5.1.1.A.)*.[225]

221 *Hive*, https://hive.io/ (last visited Jan. 15, 2026).

222 Carla L. Reyes, *Emerging Technology's Language Wars: Cryptocurrency*, 64 Wm. & Mary L. Rev. 1193, 1197–98 (2023), https://scholarship.law.wm.edu/wmlr/vol64/iss4/8 (explaining cryptocurrencies and the different meanings attributed to the term "cryptocurrency" by legislators, practitioners, and academics).

223 *Network or Protocol? Token or Coin? Deciphering the Difference*, Coinbase (Jan. 26, 2022), https://www.coinbase.com/developer-platform/discover/dev-foundations/networks-protocols-tokens-coins.

224 *Coins vs Tokens: Differences Explained*, Paxful (Aug. 30, 2024), https://paxful.com/university/what-are-tokens-coins-virtual-currencies.

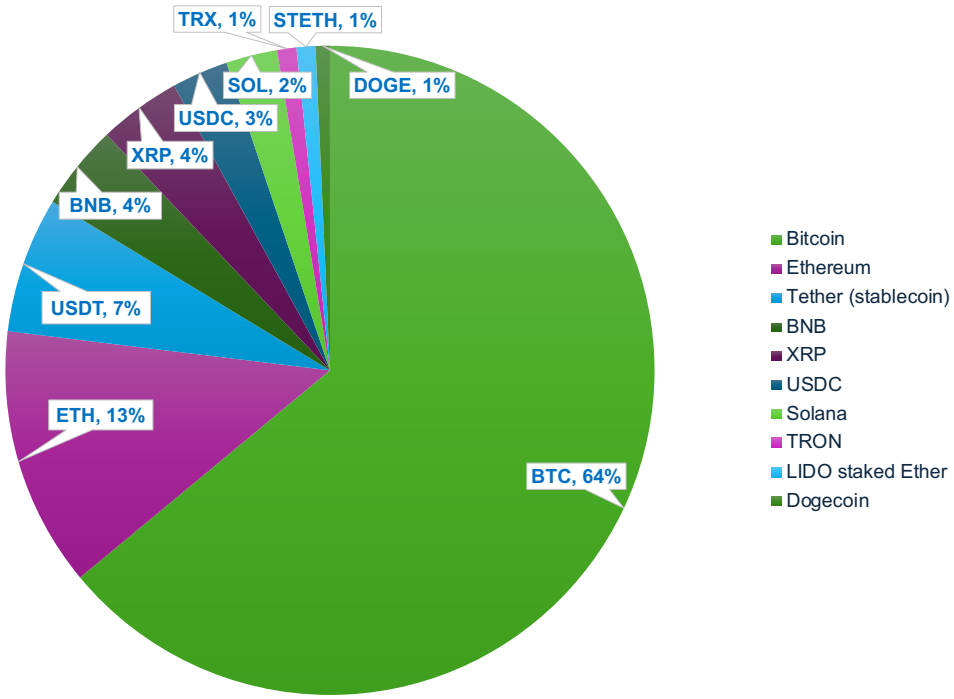
225 Pablo Azar, et al., *The Financial Stability Implications of Digital Assets*, N.Y. Fed. Rsrv. (Sept. 2022), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1034.pdf.

Coins are often grouped according to their underlying consensus mechanisms, most notably proof of work (PoW) and proof of stake (PoS). As of December 2025, Bitcoin accounted for approximately 64% of total crypto-asset market capitalization. Ethereum accounted for approximately 13%, ranking second overall *(See Figure 12)*.[226] This distribution highlights Bitcoin's continued dominance relative to other crypto-assets. As the first widely adopted public blockchain, Bitcoin has achieved a unique degree of global recognition. Its decentralized architecture, censorship-resistant design, and ability to facilitate relatively fast and low-cost cross-border transactions explain its success. In 2021, El Salvador became the first country to adopt Bitcoin as legal tender, but repealed this status in 2025.[227]

2.4.1.B. Tokens

Over time, blockchain technology has evolved beyond native cryptocurrencies to support tokens, which function as programmable representations of assets, rights, or access. The Colored Coins protocol established in 2012 enabled parties using the Bitcoin network to enter a transaction for a nominal amount and attach some additional data to it. The data specified what the transaction represented —for example, a share of stock, a property title, or a vote— to

FIGURE 12. Market share (%) of 10 leading cryptocurrencies



Source: Chart drafted using data from CoinGecko (https://www.coingecko.com) as of December 19, 2025

226 According to data provided by CoinGecko as of December 19, 2025, https://www.coingecko.com.

227 *See* the Salvadoran law that established Bitcoin as a legal tender in the country in 2021: L. 57, June 9, 2021, [431] Diario Oficial [D.O.] 13-15 (El Sal.). However, in 2025, El Salvador agreed to abolish Bitcoin as legal tender partly because of pressure from the International Monetary Fund and because it had never become popular among the public. *See Bitcoin Is No Longer Legal Tender in El Salvador*, The Digit. Watch (Feb. 7, 2025), https://dig.watch/updates/bitcoin-is-no-longer-legal-tender-in-el-salvador; Rebecca Beyer, *El Salvador Adopted Bitcoin as an Official Currency; Salvadorans Mostly Shrugged*, Yale Insights (Jan. 29, 2024), https://insights.som.yale.edu/insights/el-salvador-adopted-bitcoin-as-an-official-currency-salvadorans-mostly-shrugged (describing research by David Argente and Diana Van Patten showing that Bitcoin never really took off among Salvadorans).

indicate that the transaction represented the transfer of ownership of a particular asset.[228] Late in 2013, Mastercoin, later renamed Omni, similarly adopted the use of smart contracts as an overlay on the Bitcoin network which allowed users to trade an even greater variety of digital assets on the blockchain.[229] These early systems foreshadowed later token standards but were limited in flexibility and adoption.

A clearer distinction between coins and tokens emerged with the rise of smart-contract-enabled blockchains, such as Ethereum.

FIGURE 13.

Coins versus tokens

While the terms are often used interchangeably, "coins" and "tokens" are technically distinct. Coins are "digital assets that are native to their own blockchain" and "primarily function as a medium of exchange."[230] Tokens, by contrast, are "digital assets that operate on an existing blockchain network."[231] They are created and managed on top of an existing blockchain through smart contracts.

Tokens are created using the infrastructure of an existing blockchain but are not its native asset. They are a category of crypto-assets that can embody rights or functions linked to a wide range of assets or services, extending beyond the role of a mere medium of exchange.[232] For instance, *utility tokens* may grant access to specific services or functions, such as the ability to use or purchase a decentralized service.[233] *Governance tokens* confer voting rights within blockchain networks or decentralized autonomous organizations (DAOs).[234] Non-fungible tokens (NFTs), discussed separately below *(See below section 2.4.2.)*, represent unique digital identifiers rather than interchangeable units of value.

There are many ways to create these "secondary" assets. Tokens do not have their own blockchain but are built on existing blockchains using standards like ERC-20 (Ethereum) or BEP-20 (Binance Smart Chain).[235] Ethereum introduced the ERC-20 token in 2015,[236] standardizing the way tokens operate on its blockchain. This standardized template has been vetted and adopted into the system such that most (possibly all) blockchain applications recognize tokens created under this standard. Such tokens are often called "ERC-20 tokens" to distinguish them from native coins.[237]

228 Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 30 (2018), https://doi.org/10.2307/j.ctv2867sp (using as an example the transfer of a nominal amount of Bitcoin that constitutes the transfer of some Google's stock).

229 *SenorSamuel/spec-1 (Omni Protocol Specification (formerly Mastercoin))*, GitHub, https://github.com/SenorSamuel/spec-1 (last visited Jan. 15, 2026) ("We claim that the existing bitcoin network can be used as a protocol layer, on top of which new currency layers with new rules can be built without changing the foundation.").

230 *Coins vs Tokens*, Paw Documentation, https://www.pawchain.net/doc/coins-vs-tokens (last visited Jan. 15, 2026).

231 *Id.*

232 Miles Jennings et al., *Defining Tokens*, a16z Crypto (Mar. 5, 2025), https://a16zcrypto.com/posts/article/defining-tokens/; Akira Summers, Understanding Blockchain and Cryptocurrencies: A Primer for Implementing and Developing Blockchain Projects 135-36 (2022), https://doi.org/10.1201/9781003187165; José M. Garrido, *Digital Tokens: A Legal Perspective, WP/23/151*, Int'l Monetary Fund 53 (July 2023), https://www.imf.org/-/media/Files/Publications/WP/2023/English/wpiea2023151-print-pdf.ashx. *See also* Timothy Chan, *The Nature of Property in Crypto-assets*, 43 Legal Stud. 480, 480, n.1 (2023), https://doi.org/10.1017/lst.2022.53 (noting that the term crypto-assets includes tokens).

233 Kyle Bersani, *Separating Governance Tokens from Securities: How the Utility Token May Fall Short of the Investment Contract*, 43 Cardozo L. Rev. 1305, 1317 (2022), http://cardozolawreview.com/wp-content/uploads/2022/04/9_Bersani.43.3.2.Final_.pdf.

234 *Id.* at 1307.

235 Summers, *supra* note 232, at 136.

236 This stands for Ethereum Request for Comment #20. Requests for Comment are a common way to propose standards for adoption by the network.

237 There are various community-proposed modifications to these standards that enable additional features, including reversible transactions, for example. *See generally* Kaili Wang, Qinchen Wang & Dan Boneh, *ERC-20R and ERC-721R: Reversible Transactions on Ethereum*, arXiv (Oct. 11, 2022), https://arxiv.org/abs/2208.00543; Kaili Wang et al., *R-Pool and Settlement Markets for Recoverable ERC-20R Tokens*, DeFi'23: Proc. of the 2023 Workshop on Decentralized Fin. & Sec. 49-54 (Nov. 27, 2023), https://doi.org/10.48550/arXiv.2312.14375.

2.4.1.C. Stablecoins

The persistent volatility of most crypto-assets has limited their usefulness in applications requiring a predictable store of value. This constraint led to the emergence of *stablecoins*, a category of programmable digital assets designed to maintain a relatively stable price by referencing a stable reference asset, such as the U.S. dollar or a diversified basket of stable assets.[238] The first widely used stablecoins appeared around 2014, with designs evolving significantly since then. Stablecoins seek to combine the efficiency, programmability, and global transferability of blockchain systems with price stability typically associated with sovereign currencies or low-risk financial instruments. Most stablecoins are issued on smart-contract platforms, such as Ethereum and Tron.

Several major stablecoin models have emerged:[239]

Fiat-backed stablecoins are typically pegged 1:1 to a government-issued currency, such as the U.S. dollar (USD) and the Euro (EUR),[240] and supported by reserves held in cash or cash-equivalent assets. USD-denominated Tether (USDT) and USD Coin (USDC) together account for over 80% of stablecoin market capitalization,[241] with USDT alone representing approximately 60% of the market.[242] Euro-denominated examples include Stasis Euro (EURS). [243]

FIGURE 14.

USD Coin (USDC)

USD Coin (USDC) is a U.S. dollar-denominated stablecoin issued by Circle, a money services business, in partnership with the digital currency exchange Coinbase. Each token is designed to be redeemable one-to-one for U.S. dollars and is backed by reserves held in cash and short-term government securities. Although USDC circulates on public blockchains and is widely used in decentralized finance (DeFi), it is centrally issued and administered. Circle controls issuance and redemption and retains the ability to freeze or blacklist addresses, thereby restricting transfers or redemptions. This centralized authority means that, unlike Bitcoin or Ether, USDC's transferability ultimately depends on the policies and decisions of its issuer.

Crypto-Backed Stablecoins are supported by reserves of other cryptocurrencies. To reduce the volatility of the underlying assets, these stablecoins often employ overcollateralization, meaning the value of the reserves exceeds the value of the stablecoins. An example is Dai (DAI), which is backed by cryptocurrencies such as ETH and issued through the MakerDAO protocol. Users deposit collateral to mint Dai, ensuring its stability despite fluctuations in the collateralized cryptocurrencies.[244]

238 Chainalysis Team, *Stablecoins 101: Behind Crypto's Most Popular Asset*, Chainalysis (Dec. 11, 2024) [hereinafter *Stablecoins 101*], https://www.chainalysis.com/blog/stablecoins-most-popular-asset/.

239 Some sources distinguish fractional-algorithmic stablecoins that are a hybrid of algorithmic and collateralized stablecoins. *See* Guneet Kaur, *A Beginner's Guide on Algorithmic Stablecoins*, CoinTelegraph (Mar. 3, 2023), https://cointelegraph.com/learn/articles/a-beginner-s-guide-on-algorithmic-stablecoins (last visited Jan. 15, 2026).

240 *See* Lambis Dionysopoulos & Andrew Urquhart, *10 Years of Stablecoins: Their Impact, What We Know, and Future Research Directions*, 244 Econ. Letters 1, 1 (2024), https://doi.org/10.1016%2Fj.econlet.2024.111939 ("Stablecoins are a type of cryptocurrency that attempt to maintain a stable price against any other asset, but in most cases, the US dollar. They aim to provide exposure to their chosen asset and, in the vast majority of cases, offer a stable asset to hold in the volatile world of cryptocurrencies").

241 Omkar Godbole, *Circle's USDC Outpaces Growth of Tether's USDT for Second Year Running,* CoinDesk (Jan. 6, 2026), https://www.coindesk.com/markets/2026/01/06/circle-s-usdc-outpaces-growth-of-tether-s-usdt-for-second-year-running.

242 *Stablecoin Market Tops $317 Billion as USDT Tightens Its Grip in Early 2026*, MEXC News (Jan. 6, 2026), https://www.mexc.co/news/421705 (reporting USDT at approximately 60.68% stablecoin market share with a market capitalization of $187.0 billion as early January 2026).

243 Eur. Cent. Bank, The International Role of the Euro 6, 34-45 (June 2022), https://www.ecb.europa.eu/pub/pdf/ire/ecb.ire202206~6f3ddeab26.en.pdf.

244 Alice Cooper, *How Does MakerDAO Work*, Hexn (May 22, 2023), https://hexn.io/blog/how-does-makerdao-work-d9lyncoon1swc7p9spnmmow7

Commodity-Pegged Stablecoins are linked to the value of physical assets, such as gold, silver, or other tangible commodities. For example, Tether Gold (XAUT) offers a stablecoin backed by gold.[245]

U.S. Treasury-Backed Stablecoins are digital tokens backed by U.S. Treasury securities and related instruments (such as repurchase agreements) that can offer yield accruing directly to holders. For instance, Usual USD (USD0) is a decentralized stablecoin, pegged 1:1 to the U.S. dollar, uniquely backed by tokenized US Treasury Bills and other real-world assets.[246] Other examples include Ondo's USDY and Hashnote's USYC,[247] which similarly combine dollar stability with income from Treasury-based reserves.

Algorithmic Stablecoins are stabilized by programmed mechanisms that adjust supply based on market demand, without relying on direct collateral. Examples include Ampleforth (AMPL) and Terra USD, which dynamically adjust their supply to maintain price stability. While these models are innovative,[248] they have faced challenges in ensuring long-term stability. The collapse of TerraUSD (UST) in 2022 illustrated the systemic risks of purely algorithmic stabilization mechanisms *(See below Figure 27)*.[249]

In aggregate, on-chain stablecoin transfer volumes have reached levels comparable to or exceeding major card networks, although such figures reflect gross settlement activity rather than consumer payment volumes. Total transfer volume, meanwhile, hit $27.6 trillion in 2024.[250] Today, stablecoins are a vehicle for crypto trading (both automated and human-driven) and are increasingly used for payments, business-to-business transactions, and remittances.[251] In parallel, many governments are exploring central bank digital currencies (CBDCs), digitally-native stablecoins issued by a central bank rather than a private issuer.[252] As of 15 January 2026, Jamaica (JAM-DEX), the Bahamas (Sand Dollar), and Nigeria (e-Naira) have officially launched their digital currency products backed by their central banks.[253] India's e-rupee pilot program, operational since late 2022 in both wholesale and retail segments, has exceeded five million retail users, making it the second largest CBDC pilot in the world, after the Chinese e-CNY *(See Appendix 21)*.

2.4.1.D. Meme Coins

Meme coins represent a distinctive category of crypto-assets whose value is driven primarily by online culture, humor, and social media dynamics, rather than technological innovation. This phenomenon began in 2013 with Dogecoin, which was launched as a parody of speculative digital assets

245 Slobodzean, *What Is Tether Gold and How Does It Work?*, Medium (May 6, 2025), https://medium.com/realsatoshiclub/what-is-tether-gold-and-how-does-it-work-5ee0599662e8.

246 Coinbase, *What Is Usual* USD (USD0)? https://coinmarketcap.com/cmc-ai/usual-usd/what-is/ (last visited Jan. 15, 2026).

247 *Stablecoins 101*, *supra* note 238.

248 *Algorithmic Stablecoins, Explained*, Kraken (Nov. 25, 2024), https://www.kraken.com/learn/algorithmic-stablecoins.

249 CFI Team & Andrew Loo, *What Happened to Terra*, CFI Inst., https://corporatefinanceinstitute.com/resources/cryptocurrency/what-happened-to-terra/ (last visited Jan. 15, 2026).

250 Spencer Feingold, *Stablecoin Surge: Here's Why Reserve-Backed Cryptocurrencies Are on the Rise*, World Econ. F. (Mar. 26, 2025), https://www.weforum.org/stories/2025/03/stablecoins-cryptocurrency-on-rise-financial-systems/; Cuy Sheffield, *Making Sense of Stablecoins*, Visa (July 21, 2025), https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/making-sense-of-stablecoins.html.

251 *See generally* Deloitte, 2025 – The Year of Payment Stablecoins (2025), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-advisory-deloitte-2025-the-year-of-payment-stablecoins.pdf (explaining that consumers are using stablecoins for real-world transactions significantly more now than they have in the past several years).

252 Andrew Stanley, *The Ascent of CBDCs*, Int'l Monetary Fund: Fin. & Dev. Mag. (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs; *Digital Euro*, Eur. Cent. Bank, https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html (last visited Jan. 15, 2026). *See also Anneke Kosse & Ilaria Mattei, BIS Papers No. 136: Making Headway – Results of the 2022 BIS Survey on Central Bank Digital Currencies and Crypto, Bank for Int'l Settlements,* 4-10 (July 2023), https://www.bis.org/publ/bppdf/bispap136.pdf.

253 See an interactive map tracking the current status of CBDCs in different countries at *Central Bank Digital Currency Tracker*, Atlantic Council, https://www.atlanticcouncil.org/cbdctracker/ (last visited Jan. 15, 2026).

and based on the Shiba Inu "Doge" meme.[254] Despite its satirical origins, Dogecoin gained popularity and inspired numerous imitators, such as Shiba Inu (SHIB),[255] Floki Inu,[256] SafeMoon,[257] and later coins tied to political figures or cultural symbols.[258] Initially lacking in financial value, these tokens attracted attention primarily as satire or cultural commentary on cryptocurrency speculation.

Their character shifted dramatically during 2020–2021, when retail investors and online communities — particularly on Reddit and Twitter— embraced meme coins as a hybrid of joke, cultural statement, and speculative investment. In May 2021, high profile public endorsements contributed to Dogecoin briefly reaching a market capitalization exceeding $80 billion, despite limited utility.[259] Subsequent waves of meme coins — such as Pepe, and Snoop Dogg[260] — have originated from internet memes, jokes, or pop culture references.[261] In 2024, renewed speculative interest drove the combined market capitalization of meme coins above $60 billion.[262]

The meme coin phenomenon reveals how the union of community, humor, and social media virality could create immense, though often ephemeral, value in cryptocurrency markets. It challenges conventional finance theory by demonstrating how collective belief and online culture can function as valuation mechanisms independent of technological fundamentals or cash flow expectations. Supporters celebrate meme coins as a democratization of wealth creation and a new way to monetize attention and virality in the social media era.[263] Critics view them as the epitome of speculative excess —"[a] 24-hour casino at your doorstep, in your home."[264] In general, meme coins exhibit extreme price volatility, limited utility, and heightened risk, with value driven by social media hype, celebrity endorsements, and community sentiment.[265]

2.4.2. Non-Fungible Tokens (NFTs)

While fungible crypto-assets are identical and interchangeable, *non-fungible tokens* (NFTs) are designed to be unique and non-interchangeable.[266] Each NFT contains properties or metadata that make it uniquely identifiable

254 Kevin Roose, *He's a Dogecoin Millionaire. And He's not Selling*, N.Y. Times (May 14, 2021), https://www.nytimes.com/2021/05/14/technology/hes-a-dogecoin-millionaire-and-hes-not-selling.html.

255 Shiba Inu, Shiba Inu, https://shibatoken.com (last visited Jan. 15, 2026).

256 Floki Inu - the People's Cryptocurrency, Floki Inu, https://floki.com (last visited Jan. 15, 2026).

257 SafeMoon Meme: A New Community Driven Memecoin, SafeMoon, https://safemoon.meme/ (last visited Jan. 15, 2026).

258 *See* Victoria Turk, *From Dogecoin to $Trump: Everything You Need to Know About the Wild World of Meme Coins*, The Guardian (Feb. 5, 2025), https://www.theguardian.com/technology/2025/feb/09/from-dogecoin-to-trump-everything-you-need-know-about-the-wild-world-of-meme-coins; *Top Memes Tokens by Market Capitalization*, CoinMarketCap, https://coinmarketcap.com/view/memes/ (last visited Jan. 15, 2026).

259 Thakur Dev Pandey, *Impact of Musk's Remarks on Volatility of Bitcoin and Dogecoin amid COVID-19 Pandemic*, 3 J. Digit. Econ. 85, 87 (2024), https://doi.org/10.1016/j.jdec.2024.12.002 ("Dogecoin remained a speculative asset, with its price volatility driven primarily by social media influence and celebrity endorsements, especially Musk's tweets. During the pandemic, Musk's commentary amplified Dogecoin's volatility, spurring swift price fluctuations as retail investors on Reddit and Twitter engaged in speculative trading."). *See also Will Dogecoin Go to the Moon? The Real World Value of Doge*, Commodity, https://commodity.com/cryptocurrency/dogecoin/ (last visited Jan. 15, 2026).

260 Turk, *supra* note 258.

261 Emily Nicolle, *Memecoin Billionares are Back with Bets on Being the 'First Idiot In,'* Bloomberg (Mar. 15, 2024), https://www.bloomberg.com/news/articles/2024-03-15/memecoins-to-buy-now-pepe-dogwifhat-billionaires-evoke-last-crypto-bubble.

262 Muyao Shen, *Memecoin Trading at Levels Last Seen Before Crypto Bubble Burst*, Bloomberg (Mar. 13, 2024), https://www.bloomberg.com/news/articles/2024-03-13/memecoin-trading-volume-rises-to-levels-last-seen-before-crypto-bubble-burst.

263 *See* Charles Wayn, *Memecoins: Shaping Crypto's $10 Trillion Market Through Community and Virality*, Forbes (Dec. 17, 2024), https://www.forbes.com/sites/charleswayn/2024/12/17/memecoins-shaping-cryptos-10t-market-through-community-and-virality/.

264 David Yaffe-Bellany, *A Digital Coin Based on Baby Trump? Yup.*, N.Y. Times (July 27, 2024), https://www.nytimes.com/2024/07/27/technology/memecoins-crypto-surge.html. *See also* Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Rise of Blockchain Egregores*, *in* Defining Web3: A Guide to the New Cultural Economy 130 (Paul Dylan-Ennis, et al. eds., 2024), https://hal.science/hal-04855838v1/document ("Just like Dogecoin, Shiba Inu is a purely recursive token: it does not refer to any external measure of value like a particular asset, it simply refers . . . to itself.").

265 Lucas Ropek, *Slerf Shows the Crypto Crowd's Standards Are Lower Than Ever*, Gizmodo (Mar. 18, 2024), https://gizmodo.com/slerf-memecoin-presales-cryptocurrency-ftx-1851345267.

266 Qin Wang et al., *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*, arXiv 1, 2 (Oct. 25, 2021), https://arxiv.org/pdf/2105.07447.

and, therefore, not interchangeable with any other token.[267] The NFT boom erupted in late 2020 and reached its zenith throughout 2021. The phenomenon gained mainstream attention when digital artist Beeple sold an NFT artwork for $69.3 million at Christie's auction house in March 2021 *(See section 5.1.3.A.)*.[268] The boom was characterized by both genuine artistic innovation and speculative excess. Following a sharp market contraction in 2022,[269] NFT activity has increasingly shifted toward functional and infrastructural applications, including ticketing, digital identity, intellectual property management, gaming assets, and brand engagement.

2.4.2.A. Key Features of NFTs

Unlike cryptocurrencies, which represent fungible units of value, NFTs function as digital identifiers that can represent a wide range of assets, from digital artwork and music to virtual real estate and trading cards. NFTs do not usually "contain" the asset; they reference it. The most common form of NFT is a token on a blockchain network that encodes information about the tokenized object, whether artwork, property, or other assets, with the referenced asset's identifying data (metadata) often stored off-chain.[270]

At its core, an NFT is identified by two elements: the Token ID and the Contract Address.[271]

- The Token ID is a unique numerical identifier assigned at the time the token is created.
- The Contract Address is a hexadecimal string identifying the smart contract that governs the token's ownership and logic.

This combination makes the NFT unique as a blockchain-based identifier: No other NFT can replicate this identifier, although another NFT may include the same metadata. NFTs may also embed the wallet address of their creator.

FIGURE 15.

NFTs as Digital Identifiers

To host metadata, NFTs commonly rely on the InterPlanetary File System (IPFS), a decentralized peer-to-peer storage and retrieval system.[272] NFTs are digital identifiers associated with metadata —such as the token number, title, attributes, and image URL.[273] The metadata that defines an NFT is uploaded to IPFS,[274] then converted into a unique content identifier (CID),[275] which guarantees the integrity of the NFT's information. While IPFS is the common, decentralized method for storing NFTs, some NFTs use a centralized storage system instead.[276]

267 This technology derives from Nick Szabo's smart properties concept. Nick Szabo, *Secure Property Titles with Owner Authority*, Satoshi Nakamoto Institute (1998), https://nakamotoinstitute.org/library/secure-property-titles/.

268 Jacob Kastrenakes, *Beeple Sold an NFT for $69 Million*, The Verge (Mar. 11, 2021 10:09 AM EST), https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million.

269 Sara Gherghelas, *NFT Art's Shocking Collapse: From $2.9 Billion Boom to $23 Million Bust—What Went Wrong?*, DappRadar (Mar. 27, 2025), https://dappradar.com/blog/nft-arts-shocking-collapse-from-2-9-billion-boom-to-23-8-million-bust-what-went-wrong.

270 Corinne Tan, *Rights in NFTS and the Flourishing of NFT Marketplaces*, 32 Int'l J.L. & Info. Tech. 1, 2-3 (2024), https://doi.org/10.1093/ijlit/eaae018; Hamza Salem, *Hidden Risks: The Centralization of NFT Metadata and What It Means for the Market*, arXiv (Aug. 22, 2024), https://arxiv.org/html/2408.13281v1.

271 Wang et al., *supra* note 266, at 7-8.

272 *Id.* at 13-14.

273 *Id.* at 2, 7 (noting that most ERC-721 has been popularized over time, and commenting specifically on the importance of the ERC-721 standard in relation to NFTs); Hoon Ko, Juhee Oh & Sung Uk Kim, *Digital Content Management Using Non-Fungible Tokens and the Interplanetary File System*, 14 Applied Sci. 315, 321 (2024), https://doi.org/10.3390/app14010315 (finding the same); Leonhard Balduf et al., *Dude, Where's My NFT: Distributed Infrastructures for Digital Art*, 2022 Proc. of the 3d Int'l Workshop on Distributed Infrastructure for the Common Good 1-2 (Nov. 18, 2022), https://doi.org/10.48550/arXiv.2210.11166 (indicating the same).

274 Balduf et al., *supra* note 273, at 4-5.

275 Ko, Oh & Kim, *supra* note 273, at 5.

276 Devin Finzer, *The Non-Fungible Token Bible: Everything You Need to Know About NFTs*, OpenSea (Jan. 10, 2020), https://opensea.io/blog/guides/non-fungible-tokens/#What_is_a_non-fungible_token.

Most NFTs are developed under either the ERC-721 or ERC-1155 standard.[277] ERC-721 defines unique, indivisible tokens, each with distinct metadata, making them suitable for digital art, collectibles, and other one-of-a-kind assets. By contrast, ERC-1155 allows both unique and fungible tokens to be managed within a single contract, enabling more efficient transactions and complex asset structures, such as in gaming environments.[278]

NFTs are designed to be tamper-resistant and, under typical implementations, they cannot be altered once minted. Their on-chain identifiers cannot be forged, even though a malicious actor can still create copycat NFTs using identical metadata. With these caveats, NFTs provide a powerful mechanism for authenticating digital assets, preventing duplication at the identifier level, and establishing clear provenance of ownership. While NFTs do not inherently confer copyrights or licenses, they can be linked to rights through external contractual arrangements or off-chain licenses.[279] Smart contracts may facilitate automated transactions, such as royalty payments to artists, although enforceability usually depends on marketplace rules rather than protocol-level guarantees.[280] The ability to receive compensation from secondary market sales makes NFTs particularly attractive to digital artists and investors.

2.4.2.B. The NFT Use Cases

Over the past few years, the focus of NFTs has shifted from speculative trading of digital art and collectibles to more practical applications. The infrastructure supporting NFTs has significantly improved, with more advanced marketplaces,[281] lower transaction costs, and, in limited cases, enhanced security features.[282] Companies have adopted NFTs for various applications, including loyalty programs,[283] physical and digital collectibles,[284] event ticketing, digital identity solutions, creative industries,[285] innovative gaming experiences,[286] and metaverse (virtual world) projects, such as Sandbox and Axie Infinity.[287] In general, the level of NFT adoption varies across industries, with sectors such as sports, ticketing, luxury goods, gaming, consumer products, and art leading in both implementation and the development of new use cases. In finance, too, there has been talk of the potential for NFTs to represent stock ownership.[288]

277 *ERC-1155 vs ERC-721: NFT Standards Explained*, De.Fi (July 21, 2023), https://de.fi/blog/erc-1155-vs-erc-721-nft-standards.

278 In video games, players often must interact with both fungible assets like gold coins and non-fungible assets like unique swords or armor.

279 It is common for an NFT to link to a location on the InterPlanetary File System (IPFS) or another storage service that hosts the associated asset. This asset is typically intended to represent the "original" digital item, such as a photograph or artwork. However, this convention is a matter of custom, and in practice, it is difficult to determine what constitutes an "original" asset in the digital world.

280 *What Are NFT Royalties?*, Coinbase [hereinafter *What Are NFT Royalties?*], https://www.coinbase.com/learn/your-crypto/what-are-nft-royalties (last visited Jan. 15, 2026).

281 *How NFT Checkout Enhances NFT Marketplaces: Faster Transactions, Better UX & Higher Sales*, TransFi (Feb. 18, 2025), https://www.transfi.com/blog/how-nft-checkout-enhances-nft-marketplaces (the "NFT checkout" system is used by payment gateways to streamline transactions).

282 Ellie Farrier & Oliver Buxton, *NFTs Explained: What Are They and Are They Still Relevant?*, AVG Signal Blog (Aug. 4, 2025) (mentioning that some event tickets, like the Coachella Music Festival in 2024, were sold by ticket providers as NFTs for additional security), https://www.avg.com/en/signal/nfts-explained. Despite the long way NFTs have come, NFTs still have security issues and are susceptible to smart contract vulnerabilities and social engineering. *See* Oleh Malanii, *NFT Smart Contract Audit: Ultimate Guide*, Hacken (June 30, 2025), https://hacken.io/discover/security-audit-for-nft-guide-for-founders-and-managers/.

283 Sophie Hares, *These Blockchain Experts Are Transforming Loyalty, One NFT at a Time*, Mastercard (Nov. 15, 2022), https://www.mastercard.com/news/perspectives/2022/uptop-startup-story/; Toju Ometoruwa, *How to Build a Brand NFT Loyalty Program: A Comprehensive Guide*, MagicLabs (July 12, 2023), https://magic.link/posts/how-to-build-brand-nft-program.

284 Allie Grace Garnett & Karl Montevirgen, *NFT Use Cases: 8 Innovative Ways to Use Non-Fungible Tokens*, Britannica Money, https://www.britannica.com/money/nft-use-cases (last visited Jan. 15, 2026).

285 *See* World Econ. F., Evolution of Non-Fungible Tokens 19-20, 26-36 (Oct. 2023), https://www3.weforum.org/docs/WEF_Evolution_of_NFTs_2023.pdf.

286 Thomson Richard, *How NFTs Revolutionize the Gaming Industry: A Deep Dive into Web3 Gaming*, Medium (Dec. 2, 2023), https://medium.com/@thomsonrichard365/how-nfts-revolutionize-the-gaming-industry-a-deep-dive-into-web3-gaming-847eaccf4411; *Why Do NFTs Matter for Gamers*, Coinbase, https://www.coinbase.com/learn/tips-and-tutorials/why-do-nfts-matter-for-gamers (last visited Jan. 15, 2026).

287 Michelle Legge, *Sandbox vs. Decentraland vs. Axie Infinity*, Koinly (Sept. 19, 2025), https://koinly.io/blog/sandbox-vs-axie-infinity-vs-decentraland/.

288 *Tokenized Stocks & Equities Explained*, Chainlink, https://chain.link/education-hub/tokenized-stocks-equities-explained (last visited Jan. 15, 2026).

FIGURE 16.

Automating royalty payment with NFTs

NFTs have enabled a method for automating royalty payments.[289] The royalty percentage is embedded in the NFT's smart contract, ensuring that the artist receives a royalty payment each time the NFT changes hands.[290] However, many marketplaces have stopped enforcing royalties, citing creditors' reluctance to pay for mandatory royalty payments.[291] Citing this very concern, OpenSea, one of the largest NFT platforms, ceased in March 2023 enforcing royalty fees on NFTs sold on its marketplace.[292] Some critics have referred to the elimination of mandatory royalty payments as part of a "race to the bottom" among NFT marketplaces, which are competing to attract sellers in a volatile art-related NFT market.[293] Similarly, Blur, another major NFT marketplace, now enforces a minimum royalty of just 0.5%,[294] a significant reduction from the industry norm of 5%-10%, unless an artist blocks trading of their work on a competitor marketplace.[295] Some bad actors have attempted to bypass royalty payments through a process called "NFT wrapping,"[296] where buyers "wrap" the NFT in a different technical code, making it undetectable to royalty enforcement systems.[297]

Finally, NFTs are increasingly leveraged to address different social impact issues. For example, Chinese artist Badiucao used his platform to criticize China's human rights policies through an Olympic-themed NFT collection.[298] Similarly, AssangeDAO raised over 17,000 ETH to bid on an NFT titled "Clock," with the proceeds supporting Julian Assange's legal battle against extradition to the United States over his publishing of classified U.S. documents on WikiLeaks.[299]

2.5. SMART CONTRACTS AND DAOS

Smart contracts and decentralized autonomous organizations (DAOs) represent two advanced applications of blockchain technology. Smart contracts are self-executing software programs deployed on blockchains that automatically enforce predefined rules. A DAO is an organizational protocol composed of smart contracts that encode governance functions —such as proposal submission, voting, and fund allocation— directly in executable code, enabling decision making and coordination with reduced reliance on centralized control.

289 Michael Blau et al., *How NFT Royalties Work: Designs, Challenges, and New Ideas*, A16ZCRYPTO (June 26, 2024), https://a16zcrypto.com/posts/article/how-nft-royalties-work/.

290 *What Are NFT Royalties?*, *supra* note 280.

291 Eric James Beyer, *Open Sea: The Ultimate Guide to Its Tools, Features, and Controversies*, NFTNow (Apr. 19, 2023), https://nftnow.com/features/opensea-the-ultimate-guide-to-its-tools-features-and-controversies/.

292 Jacob Kastrenakes, *A Key Feature of NFTs Has Completely Broken*, THE VERGE (Aug. 17, 2023), https://www.theverge.com/2023/8/17/23836440/nft-creator-royalty-fees-are-dead-opensea-optional.

293 *Id.*

294 *How to Earn Royalties on Blur*, BLUR.IO (Feb. 15, 2023), https://mirror.xyz/blurdao.eth/vYOjzk4cQCQ7AtuJWWiZPoNZ04YKQmTMsos0NNq_hYs.

295 *What Are NFT Royalties?*, *supra* note 280.

296 *See* Robert Stevens, *What Are Wrapped Tokens?*, COINDESK (Feb. 4, 2022), https://www.coindesk.com/learn/what-are-wrapped-tokens (last visited Jan. 15, 2026).

297 Casey Anderson, *What are NFT Royalties and How Do They Work?*, NFT EVENING (Jan. 20, 2025), https://nftevening.com/nft-royalties/.

298 *Beijing 2022: A Protest NFT Collection by Badiucao*, BADIUCAO, https://www.badiucao.com/nft (last visited Jan. 15, 2026).

299 Gian M. Volpicelli, *Assange's NFT Clock Sale Rides a Wave of DAO Crowdfunding*, WIRED (Feb. 9, 2022), https://www.wired.co.uk/article/assange-dao-nfts-crypto.

2.5.1. Smart Contracts

In 2015, Ethereum introduced a major innovation in blockchain architecture. In addition to enabling peer-to-peer transfers of its native cryptocurrency ether (ETH), Ethereum incorporated a programming environment that allowed developers to design and deploy decentralized applications (dApps). These applications, implemented through self-executing "smart contracts," extended blockchain functionality beyond value transfer to programmable and automated governance, finance, and other complex transactions.

2.5.1.A. The Emergence of Smart Contracts

"Smart contracts" are computer programs that execute operations according to predefined rules encoded within the programs.[300] These autonomous programs automatically execute when specified conditions are met, thereby reducing the need for human intervention or intermediaries to verify or enforce agreements.[301]

The idea of self-executing agreements predates blockchain technology. In the 1990s, computer scientist Nick Szabo introduced the term "smart contract," describing it first as a "computerized transaction protocol that executes the terms of a contract."[302] Later, he called it "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[303] Szabo emphasized that smart contracts "go beyond the vending machine" by enabling a wide range of digital exchanges.[304] He envisioned that smart contracts would lower the risk of fraud and reduce transaction costs, including losses, arbitration, enforcement, and other inefficiencies commonly associated with traditional legal contracts.

Ethereum operationalized this concept by embedding a Turing-complete programming environment into its blockchain.[305] The Ethereum blockchain can store, execute, and update smart contracts. Deploying a program on Ethereum allows anyone globally to interact with the code of that program and develop their own applications at the protocol level in an open and permissionless manner, subject to technical constraints such as transaction fees and network conditions. Just as Bitcoin allows for censor-resistant financial transactions, the Ethereum network essentially allows separate nodes to independently execute all valid transactions and maintain the same shared, tamper-resistant, state. Since then, numerous other blockchains, including Solana, Cardano, and Polkadot, have introduced their own smart contract frameworks, each offering distinct trade-offs among security, scalability, and functionality. The underlying technology continues to evolve, with the introduction of new programming languages aimed at enhancing both developer usability and system security.

The primary purpose of a smart contract is to encode a program that is deployed on a blockchain and executed automatically once predefined conditions are met. Smart contracts may serve as repositories of governance rules or facilitate the transfer of digital assets between participants.

300 Primavera De Filippi, Chris Wray & Giovanni Sileno, *Smart Contracts*, 10 Internet Pol'y Rev. 1, 2-3 (2021), https://doi.org/10.14763/2021.2.1549.

301 "A smart contract is very similar to a 'persistent script'—a standing computer program—that says 'if event x happens, then execute result'", Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 Wash. & Lee L. Rev. 1521, 1541 (2021), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4745&context=wlulr.

302 Nick Szabo, *Smart Contracts* (1994), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (last visited Jan. 15, 2026).

303 Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (last visited Jan. 15, 2026).

304 Nick Szabo, *The Idea of Smart Contracts* (1997), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (last visited Jan. 15, 2026).

305 Chris Kuiper & Jack Neureuter, Ethereum: Advancing Blockchain with Smart Contracts and Decentralized Applications, Fidelity Digit. Assets, 6, 8 (May 2022), https://www.fidelitydigitalassets.com/sites/g/files/djuvja3256/files/acquiadam/1024435.3.0%20-%20FDA%20Ethereum%20%2805.21%29.pdf (per Vitalik Buterin, "Ethereum . . . [is] a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications . . . [with] their own arbitrary rules for ownership, transaction formats and state transition functions."). "Turing-complete" basically means that a system is able to perform any computation, given enough time and memory.

They also function as foundational building blocks of decentralized applications (dApps) across domains such as finance, governance, and gaming. In practice, smart contracts rarely operate in isolation; rather, they typically form part of a broader application architecture deployed on the blockchain, supporting automated and, in some cases, decentralized system behavior. Some smart contracts incorporate mechanisms designed to enhance transactional security, for example, by placing funds in escrow and releasing payment automatically once specified conditions are satisfied, often based on external inputs or attestations.

2.5.1.B. Key Features of Smart Contracts

1. Automation

A smart contract sets out parameters for how transactions will be executed and, once those parameters are met, the smart contract automatically processes the transactions. This process generates as output a change in the smart contract memory or a new blockchain transaction. Smart contracts differ from standard software programs as they are executed on the blockchain, independently from any centralized operator or trusted third party. Once the programmed conditions are met, the program executes its terms automatically, without human intervention. This mechanism enables a wide range of applications *(See below section 2.5.1.C.)*. Like any other software, its potential is broad, as soon as tasks can be expressed in code and verified by the network.

2. Immutability

Deploying smart contracts on blockchains enhances security for transactions, as blockchain ledgers are designed to be immutable and resistant to unauthorized alteration. By default, once a smart contract's code is deployed to a public blockchain, it cannot be modified retroactively. Any attempt by an unauthorized party to change the code or transaction history would be detected and rejected by the network. As a result, the initial programming of a smart contract cannot be changed in the way legal contracts can be amended through subsequent agreement, unless mechanisms for modification or termination are explicitly provided for in the original program. In other words, it is generally difficult, though not categorically impossible, to prevent the execution of a smart contract once its conditions are satisfied. Exceptions can be where its conditions fail, its execution is deliberately paused, or validators censor or delay the transaction's execution. If a smart contract fails to execute, the transaction typically reverts without altering the state of the blockchain.

By default, smart contracts deployed on public blockchains such as Ethereum are immutable: Once their code is written to the ledger, it cannot be altered.[306] However, developers have found ways to work around this limitation through architectural techniques, most notably the "proxy pattern." This pattern works like a forwarding system. Users interact with a permanent "proxy" contract that remains unchanged on the blockchain. This proxy simply redirects all requests to a separate "implementation" contract that contains the actual program logic. When developers need to upgrade the system, they deploy a new implementation contract with updated code and point the proxy to this new version instead. The proxy itself never changes: It just updates which implementation contract it forwards requests to. From the user's perspective, the system appears upgradeable and changeable. In reality, it is built entirely from immutable pieces; the upgrade happens by swapping out which immutable piece the proxy points to, rather than by modifying any existing code.

306 *See* Daniel Davis & Alexander Kim, *'Smart Contracts' Ruling Forces a Blockchain Development Rethink*, Bloomberg L. (Jan. 30, 2025), https://news.bloomberglaw.com/us-law-week/smart-contracts-ruling-forces-a-blockchain-development-rethink. *See also* Wei Liang et al., *On Identity, Transaction, and Smart Contract Privacy on Permissioned and Permissionless Blockchain: A Comprehensive Survey*, 56 ACM Computing Surveys. 5 (2024), https://doi.org/10.1145/3676164 (discussing the inherent immutability of traditional smart contracts on platforms like Ethereum); Elena Nadolinski, *Proxy Patterns*, OpenZeppelin Blog (Apr. 19, 2018), https://blog.openzeppelin.com/proxy-patterns.

The distinction between immutable contracts —which cannot be altered after deployment— and upgradeable or mutable contracts —which can be modified through pre-defined governance or administrative mechanisms— has become a central focus of recent legal analysis. This issue has featured prominently in recent U.S. litigation, including proceedings involving the Tornado Cash protocol, with important implications for developers, users, and regulators *(See below section 6.5.3.)*

3. Gas

Smart contracts executed on the Ethereum platform require users to pay a fee for the contract to run on the blockchain and the relevant transactions to be added to the blocks. The more complex the transactions in the smart contract, the higher the fee. The fee, known as "gas," refers to the unit of measurement for the computational work required to perform operations on a blockchain network.

Each operation within a blockchain transaction consumes a defined number of gas units. For instance, a simple value transfer might consume approximately 21,000 gas units, while more complex operations —such as those involving smart contracts— require substantially more. Because blockchain networks operate with limited computational capacity, gas functions as a mechanism to allocate these resources efficiently. By assigning a cost to each operation, gas fees prevent users from overloading the system with overly complex or malicious computations —such as infinite loops— which could degrade network performance or facilitate denial-of-service attacks. Additionally, gas fees serve as an economic incentive for validators (in proof-of-stake blockchains) or miners (in proof-of-work blockchains), compensating them for processing transactions and contributing to the network's overall security and functionality.

Gas fees fluctuate based on network demand. During periods of high network activity, gas prices increase as users compete to have their transactions processed quickly. Conversely, during quiet periods, gas prices tend to decrease. This market-based mechanism helps balance network usage and ensures the blockchain remains responsive even during peak times.

4. Oracles

In principle, blockchains are closed systems, including the smart contracts running on them. But one way to allow smart contracts to interact with the off-chain world is through the use of "oracles." Oracles are mechanisms that bridge smart contracts to key real-world and off-chain resources. These can include data feeds (e.g., the weather, the time of arrival of a plane, the arrival of a product at its destination), as well as legally binding e-signatures or bank payments. Oracles can deliver information that triggers the execution of a smart contract or signal off-chain actors or systems to perform contractually agreed actions, such as ordering a financial institution to execute a payment. Oracles can also connect smart contracts to physical things. The development of the Internet of Things and "smart properties" in many modern devices has allowed smart contracts to connect to everyday tools, such as cars, door locks, lights, and more, thereby expanding the realm of digital enforcement.

While these oracles act as bridges between blockchains and external data sources, they also introduce significant risk vectors. If an oracle supplies data which is erroneous or has been manipulated, the oracle can undermine the integrity of the smart contract. For instance, in 2020, the bZx protocol, a decentralized finance (DeFi) platform that enables margin trading and lending through smart contracts, was targeted by several oracle-based attacks.[307] In one such incident, an attacker manipulated the price

307 Giulio Caldarelli & Joshua Ellul, *The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach*, 11 Applied Sci. 1, 19-20 (Aug. 18, 2021), https://doi.org/10.3390/app11167572.

feed by exploiting vulnerabilities in price oracles and the low liquidity of certain trading pairs.[308]

Given this vulnerability, oracles reintroduce a need for trust in external sources of information, precisely what blockchain systems were initially designed to minimize.[309] How do programs running on blockchains get information about the outside world in such a way that it cannot be manipulated? This challenge is commonly referred to as the "blockchain oracle problem."[310] It exposes a paradox: While smart contracts are often praised for their ability to eliminate trusted intermediaries, they ultimately relocate reliance on trust rather than eliminate it — transferring it from traditional institutions to a new set of private actors.[311] Oracle providers thus become the de facto trusted data sources on which automated execution depends.[312]

2.5.1.C. Main Applications

Smart contracts have given rise to entire blockchain-based ecosystems that rely on transparent and immutable protocols. They have found applications in various industries, simplifying transactions and reducing costs by cutting out middlemen. For instance, supply chain management has adopted smart contracts to increase transparency and efficiency *(See below section 4.8.)*. Smart contracts are used to automate payments upon delivery verification, track product origins, and manage complex multi-party agreements across global supply networks.[313]

Beyond their function as automated agreements, smart contracts are increasingly understood as foundational "institutional technologies" —tools for building novel systems of *private* governance.[314] They enable new forms of coordination that economize on transaction costs by replacing centralized intermediaries with decentralized, automated protocols. This transformative potential is most evident in the rise of Decentralized Autonomous Organizations (DAOs) and Decentralized Finance (DeFi). In these ecosystems, smart contracts form the operational backbone, executing rules for governance, managing treasuries, and facilitating financial transactions, such as lending, borrowing, and trading, without relying on traditional corporate structures or financial institutions.

Today, Decentralized Finance is perhaps the most prominent application *(See below section 4.2.3.)*, with smart contracts powering lending protocols, decentralized exchanges, yield farming, and liquidity pools.[315] Lending protocols such as Aave, Compound, and Morpho, as well as decentralized exchanges such as Uniswap, rely on smart contracts to enable financial transactions without intermediaries. Tokenized real-world assets, such as real estate, commodities, and securities, are being managed through smart contracts that handle fractional ownership, dividend distribution, and compliance requirements.

---

308 In February 2020, an unidentified attacker took out a flash loan—a loan that requires nearly instant repayment—from bZx in ETH and split it into two portions. The attacker used the first portion to buy sUSD, a synthetic stablecoin designed to track the value of one U.S. dollar. He used the second portion to buy sUSD on Kyber and Uniswap, with the amount large enough that it inflated the price to more than $2 per sUSD. Since bZx smart contract referenced the price of sUSD on Kyber, it started treating this inflated price as the real one. The attacker then used the previously purchased sUSD from the first transaction as collateral to borrow far more ETH than he should have been permitted. He then paid back the flash loan and took home the profit without repaying the second loan. *See* Kevin Lu, *Why DeFi Needs Real Oracles Beyond DEX*, MEDIUM (Feb. 21, 2020), https://medium.com/bandprotocol/why-defi-needs-real-oracles-beyond-dex-9c80cf192883; *Around the Block #3: Analysis on the bZx Attack, DeFi Vulnerabilities and the State of Debit Cards in Crypto*, COINBASE, https://www.coinbase.com/learn/market-updates/around-the-block-issue-3 (last visited Jan. 15, 2026).

309 *See* Giulio Caldarelli, *Understanding the Blockchain Oracle Problem: A Call for Action*, 11 INFORMATION 509, 509 (2020), https://doi.org/10.3390/info11110509 (noting that oracles resolve the trust problem introduced by blockchains originally).

310 *The Blockchain Oracle Problem*, CHAINLINK, https://chain.link/education-hub/oracle-problem (last visited Jan. 15, 2026).

311 Darcy W. E. Allen & Aaron M. Lane, *Smart Contracts as Private Governance Tools,* 3 (Oct. 11, 2023) (unpublished manuscript), https://ssrn.com/abstract=4598625.

312 *Id.* at 7, 14, 19,

313 EURO. SEC. & MKTS. AUTH., DECENTRALISED FINANCE: A CATEGORISATION OF SMART CONTRACTS 12 (2023), https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3351_TRV_Article_Decentralised_Finance_A_Categorisation_of_Smart_Contracts.pdf.

314 Allen & Lane, *supra* note 311, at 3.

315 *Id.* at 7–11.

Moreover, Non-Fungible Token (NFT) marketplaces rely heavily on smart contracts to manage ownership, royalties, and transfers of digital assets. Digital identity systems *(See below Section 4.5)* leverage smart contracts to give users control over their personal data, allowing selective disclosure of information without revealing everything to every service provider.

Despite the advantages of smart contracts, their potential as governance tools is tempered by several limitations. First, as previously discussed with respect to oracles *(See Section 2.5.1.B.4.)*, smart contracts can act only on data that already exist on the blockchain. To respond to real-world events —such as the outcome of a sports game or fluctuations in stock prices— they must rely on external sources of data provided by oracles. The execution of the smart contract thus depends entirely on the accuracy and integrity of the oracle's data, which reintroduces a point of centralization and vulnerability.[316]

Second, the immutable nature of smart contracts means that, once deployed, any bug or security vulnerability can be exploited with permanent and irreversible consequences. The 2016 hack of the DAO, which resulted in the theft of millions of dollars' worth of ether and ultimately led to a contentious hard fork of the Ethereum network, remains the canonical example of this risk.[317] Because of their autonomous execution, errors in code may also trigger continuous loops of faulty transactions.

Finally, smart contracts suffer from inherent incompleteness *(See section 6.5.2.B.)*: They cannot specify all future contingencies or events that may affect their execution.[318] As a result, coded agreements are often rigid and unable to account for unforeseen circumstances, which may lead to inequitable outcomes when the unexpected occurs.[319] Moreover, while smart contracts automate performance, they do not automatically constitute legally binding contracts under traditional law, raising unresolved questions about enforceability, liability, and jurisdiction *(See below section 6.5.)*.

2.5.2. Decentralized Autonomous Organizations

One of the most wide-reaching use cases of smart contracts has been the formation of Decentralized Autonomous Organizations, or DAOs. DAOs are blockchain-based organizations that aspire to decentralized governance structures as an alternative to conventional hierarchical and centralized forms of control. They are member-run collectives that form for a common purpose, such as investing in start-ups, managing DeFi protocols, or purchasing and managing assets such as crypto-assets, NFTs, or real-world assets.[320] According to industry trackers and academic estimates, there are tens of thousands of DAOs in existence and, as of January 2026, they are estimated to collectively manage more than $13.6 billion in assets, although these figures fluctuate significantly with market conditions and methodological assumptions.[321] The first widely recognized large-scale DAO, which was simply referred to as "The DAO," was launched in 2016 on the Ethereum platform to facilitate the crowdfunding of diverse projects *(See sections 1.2. and 6.2.1.)*[322]

316 Allen & Lane, *supra* note 311, at 7; Peter L. Michaelson & Sandra A. Jeskie, *Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts*, 74(4) Disp. Resol. J. 89 (2020), at 93, https://ssrn.com/abstract=3720876.

317 Muhammad Mehar et al., *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack,* 21(1) J. Cases Info. Tech., 19-32 (November 26, 2017), http://dx.doi.org/10.2139/ssrn.3014782.

318 Massimiliano Vatiero, *Smart contracts vs incomplete contracts: A transaction cost economics viewpoint*, 46 Comp. L. & Sec. Rev., 1 (Sept. 2022), http://dx.doi.org/10.2139/ssrn.3259958. *See also* Jesse Walden, *Incomplete Contracts (and Scaling Crypto)*, a16zcrypto (July 22, 2019), https://a16zcrypto.com/posts/article/incomplete-contracts/.

319 Allen & Lane, *supra* note 311, at 19

320 Kevin Roose, *What are DAOs?*, N.Y. Times (Mar. 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/what-are-daos.html.

321 *Organizations*, DeepDAO, https://deepdao.io/organizations (last visited Jan. 15, 2026).

322 Youssef Faqir-Rhazoui, Javier Arroyo & Samer Hassan, *A Comparative Analysis of the Platforms for Decentralized Autonomous Organizations in the Ethereum Blockchain*, 12 J. Internet Servs. & Applications 1, 4 (2021), https://doi.org/10.1186/s13174-021-00139-6.

2.5.2.A. What Is a DAO?

DAOs can be seen as computerized organizations that leverage smart contracts for both treasury and operational management. There are different definitions of what constitutes a DAO. One definition, from an academic, provides that a DAO "is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralised (i.e., independent from central control)."[323] Another definition, by a preeminent entrepreneur, characterizes DAOs as "an amalgamation of pieces of investment banks, companies, and social clubs stitched together via cryptographic commitments."[324]

Whichever definition one uses, DAOs, as their name implies, aim to be both decentralized (i.e., to reduce reliance on centralized management or control) and autonomous (i.e., to increase reliance on automated execution). They do so by operating primarily "in accordance with the rules encoded in self-executing code (smart contracts), rather than traditional articles of association or shareholder agreements."[325] The smart contracts, connected together, semi-autonomously operate a DAO's governance scheme with limited need for central leadership or human intervention. Instead, they rely on peer-to-peer network processes involving all stakeholders, often combined with off-chain coordination mechanisms, such as forums, proposal systems, or delegated voting structures.

DAO proponents, often dissatisfied with traditional corporate and governmental institutions, propose the sharing of power within a computerized organization as an alternative governance model. One of the central objectives of DAOs is to mitigate the principal-agent problem —a persistent challenge in corporate governance.[326] In essence, the principal-agent problem arises whenever a "principal" relies on actions taken by their "agent" that will ultimately affect the principal. At its core, this problem is closely linked to information asymmetries and misaligned incentives, which make it difficult for principals to monitor or control agents' behavior. In economics, the problem, at its most general level, is: how does one induce an agent to act in the interests of the principal, rather than in their own self-interest? DAO advocates argue that this problem may be mitigated by structuring participation such that members simultaneously act as principals and decision makers, thereby theoretically aligning interests more directly and reducing agency-related inefficiencies.[327] In practice, however, DAOs may only reconfigure agency problems through mechanisms such as token concentration, delegation, or voter apathy *(See section 3.2.2.C.)*.

DAOs may also allow for more secure, transparent, and accountable governance. The security features of blockchain technology provide greater certainty to stakeholders regarding the governance scheme and voting rights and can reduce certain types of abuse. Similarly, many aspects of DAO governance are recorded on-chain, from the code to decisions, allowing for enhanced transparency and auditability. Should the DAO be run on a public blockchain, any interested party may, in principle, audit on-chain

323 Samer Hassan & Primavera De Filippi, *Decentralized Autonomous Organization*, 10 Internet Pol'y Rev. 1, 2 (2021), https://doi.org/10.14763/2021.2.1556.

324 Tarun Chitra, *Building and Running a DAO: Why Governance Matters*, a16zcrypto (Mar. 11, 2021), https://a16zcrypto.com/posts/article/building-and-running-a-dao-why-governance-matters/. More facetiously, some refer to them as "financial flash mobs" or as "group chats with a bank account." Wenting Yu, *What the DAO? Why Everyone is Talking about Decentralized Autonomous Organizations*, O'Melveny & Myers (Apr. 11, 2022), https://www.omm.com/insights/alerts-publications/what-the-dao-why-everyone-is-talking-about-decentralized-autonomous-organizations/.

325 Int'l Org. of Sec. Comm'ns, Policy Recommendations for Decentralized Finance (DeFi) 70 (Sept. 2023) [hereinafter IOSCO Sept. 2023 Report], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

326 The principal-agent problem arises when one party (the agent) is authorized to act on behalf of another (the principal) but their respective interests are not fully aligned. This divergence in incentives can lead agents to prioritize their own objectives over those of the principal, resulting in conflicts of interest, inefficiencies, and, in some cases, exploitation. *See* John Armour, Henry Hansmann & Reinier Kraakman, *Agency Problems and Legal Strategies*, *in* The Anatomy of Corporate Law: A Comparative and Functional Approach 29-48 (Reinier Kraakman, et al. eds., 3d ed. 2017) (describing in brief the principal-agent problem).

327 Wulf A. Kaal, *Blockchain-Based Corporate Governance*, 4 Stan. J. Blockchain L. & Pol'y 3, 27 (2021), https://stanford-jblp.pubpub.org/pub/blockchain-corporate-governance.

activities, although significant elements of governance may occur off-chain. Finally, because of their informality and relatively low administrative overhead, DAOs may be more nimble and agile than traditional companies.

Overall, proponents describe DAOs as a means to "help course correct the internet back to its original, idealistic vision: power and money pushed to the edges, networks growing and flourishing together, a level playing field for talent anywhere in the world, a thriving creative middle class, and a generally diverse and interesting place."[328] This vision remains aspirational and unevenly realized in practice, as decentralization may introduce coordination costs that affect efficiency and decision-making.

2.5.2.B. The Organization of a DAO

The governance structures, membership criteria, and operational procedures of DAOs are encoded in smart contracts. Each smart contract is programmed to perform specific functions and, when interconnected, they can collectively execute complex organizational tasks. Once the governing rules are programmed, the DAO can operate according to the computer code. It often does so with a high degree of automation, though most DAOs continue to rely on some level of human oversight, intervention, or emergency control mechanisms. Although early DAOs relied heavily on human coordination, recent technological advancements have enabled greater degrees of automation, even if fully autonomous DAOs remain rare in practice.

Where human involvement remains necessary, DAOs are commonly managed through "governance tokens" *(See below section 3.2.2.A.)*, which make tokenholders participants in governance that can resemble a hybrid with shareholders and managers. Tokenholders interact according to the protocol by voting and providing input on decisions to be made. DAOs differ in structure and complexity, but, in principle, governance participation is open to all tokenholders, including decisions on how common funds are used for the DAO's activities or allocated to other investments.[329] Each token typically grants voting power. In some designs, it may be associated with economic rights, such as protocol rewards or revenue-sharing mechanisms. Many DAOs explicitly avoid ownership-like rights for legal and regulatory reasons. In most cases, token-weighted governance means that larger token holdings translate into greater voting power, raising questions about effective decentralization.

DAOs may be accompanied by a formal legal entity, which can take the form of limited liability companies or assume a variety of other structures, such as offshore foundations, non-profit associations, or trusts *(See below section 6.4.1.)*.[330] Such legal "wrappers" are often used to provide liability protection, regulatory clarity, or operational capacity, including the ability to contract with service providers or open bank accounts. Some DAOs choose offshore jurisdictions —such as the Cayman Islands or Panama— because of flexible corporate laws, perceived regulatory neutrality, or tax considerations.[331] This choice, however, may also raise legal, regulatory, and reputational risks, particularly in the United States and European Union.

328 Roose, *supra* note 320 (quoting Chris Dixon, a venture capitalist and crypto investor).

329 *See* David Kerr & Miles Jennings, Andreessen Horowitz, A Legal Framework for Decentralized Autonomous Organizations: Entity Structure V2 8 (June 2022), https://d2hguprl3w2sje.cloudfront.net/uploads/2022/06/dao-legal-framework-part-1.pdf.

330 Chris Brummer & Rodrigo Seira, *DAO Strategy and Legal Wrappers*, Paradigm (Aug. 6, 2022), https://www.paradigm.xyz/2022/06/dao-strategy-and-legal-wrappers; Chris Brummer et al., *DAO Legal Entity Matrix*, Paradigm, https://daos.paradigm.xyz/ (last visited Jan. 15, 2026); Kerr & Jennings, *supra* note 329, at 1, 17.

331 Bessie Liu & Jack Kubinec, *DAOs Favor Classic Tax Havens, Pass Up Crypto-Friendly US States*, Blockworks (Oct. 29, 2022), https://blockworks.co/news/daos-favor-classic-tax-havens-passing-up-crypto-friendly-us-states.

2.6. PRIVACY ENHANCING TECHNIQUES

Blockchain systems have historically placed a strong emphasis on privacy, a concern often associated with the cypherpunk movement. This emphasis is evident in the foundational use of public key cryptography in Bitcoin, as well as in more advanced systems specifically designed to protect user privacy. At the same time, there is an inherent tension between privacy and the principles of transparency and openness that also characterize blockchain systems. Nevertheless, various cryptographic techniques can be employed to obscure transaction data in ways that enhance privacy while maintaining the integrity of the ledger.[332]

There are numerous methods for protecting user privacy, but most fall into a few distinct categories.[333] The following sections examine Privacy Enhancing Technologies (PETs) that provide privacy through one or more of the following mechanisms: by obscuring the identity of the participant, often through the use of pseudonymity; by obscuring which stakeholder —whether known or unknown— performed a particular action; or by obscuring the specific details of the action itself.

2.6.1. Pseudonymity

Most public blockchains offer a basic form of privacy known as pseudonymity, which is among the simplest PETs. The goal of pseudonymity is to conceal the real-world identity of a participant so that, even if the details of an action —such as a transaction or vote— are publicly visible, it remains difficult (and ideally impossible) to link those actions to a specific individual or entity. In this model, blockchain users interact using pseudonymous public addresses rather than their real-world identifiers. Although all activity associated with a given public address is fully transparent and accessible on the blockchain, these addresses are not readily associated with any natural or legal person.

This system does not provide complete anonymity, i.e. the complete obscurity of a user's identity. While public blockchains do not store any information about a user's offline identity, transaction records associated with blockchain addresses remain accessible and persistent over time. Depending on the blockchain architecture, these addresses may be directly derived from public keys (as in Ethereum) or may be hashes of public keys that are revealed only upon spending (as in Bitcoin). In either case, blockchain analysis can potentially link addresses to real identities: A connection between an individual and their public key *can* be uncovered through external means, such as behavioral pattern analysis or voluntary disclosure. This is why blockchains can be said to provide only pseudonymity.[334]

Blockchain transactions are inherently linked to traceable identifiers, such as wallet addresses and public keys. These identifiers allow observers to analyze a user's transaction history over time. Such analysis can reveal behavioral patterns, including frequent trading activity on specific exchanges, participation in governance votes, or repeated interaction with decentralized finance (DeFi) protocols. In many cases, wallet activity can also provide insight into a user's financial condition, interests, or organizational affiliations, as it reflects the types of assets held, the nature of engagements with various platforms, and the regularity of transactions. Over time, this data can be used to identify patterns, map behavioral trends, and infer relationships between different participants on the network. In some

332 *See* Muhammad Al-Abdullah et al., *Designing Privacy-Friendly Data Repositories: A Framework for a Blockchain that Follows the GDPR*, 22 Digit. Pol'y, Regul. & Governance 389, 405 (2020), https://doi.org/10.1108/DPRG-04-2020-0050.

333 *See* Maisha Boteju et al., *SoK: Demystifying Privacy Enhancing Technologies Through the Lens of Software Developers*, arXiv (Dec. 30, 2023), https://arxiv.org/html/2401.00879v1 (software developers implement a variety of long-established privacy enhancing technologies, including pseudonymization, zero-knowledge proofs, and others).

334 Article 4(5) of the General Data Protection Regulation (GDPR) defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information . . . ." Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 4(5) [hereinafter GDPR].

instances, such patterns may enable third parties to de-anonymize users. The development of advanced blockchain forensics and re-identification tools —such as those produced by Chainalysis and utilized by law enforcement agencies such as the U.S. Federal Bureau of Investigation (FBI)— has significantly expanded the capacity to conduct such analyses. This is raising important implications for user privacy and data protection on public blockchains.[335]

FIGURE 17.

Privacy, Pseudonymity, and Anonymity

While closely related, the terms *privacy*, *pseudonymity*, and *anonymity* have distinct meanings, particularly in the context of digital systems.

- *Privacy* refers broadly to "the right of a party to maintain control over and confidentiality of information about itself."[336]
- *Pseudonymity,* in a general sense, is to use a fictitious identity to mask one's identity.[337] In the digital context, pseudonymity has a rather similar definition. A pseudonym is "an identifier of a subject other than one of the subject's real names."[338] Pseudonymization involves the use of a modifier that obscures the identity of the end user or the individual that accessed a particular piece of information.[339] The General Data Protection Regulation (GDPR) in the European Union defines pseudonymity as the use of a pseudonym so the end user cannot be revealed without an additional piece of information linking the pseudonym to the end user.[340] This implies that the user's identity can be revealed with additional information. Importantly, under the GDPR, pseudonymized data remain personal data and therefore continue to be subject to data protection obligations.
- *Anonymity*, by contrast, is the ability of a user to operate without the possibility of being identified, even with additional information. Because it is usually difficult to obtain true anonymity in digital environments, scholars have turned to defining degrees of anonymity.[341] But an anonymous digital actor can operate without the possibility of being identified. Generally, to achieve maximum anonymity, a digital user might use unique internet browsers, proxies, or VPNs.[342] One of the "most established anonymity-granting technologies is The Onion Router" which "provide[s] layers of encryption between the user and the information source, making it very unlikely for someone to trace back both sides."[343] Anonymity, thus, eliminates the possibility of real-world identifiability while pseudonymization requires one to take an additional step before identifying a user's real-world identity.

335 *See* Chainalysis, The 2025 Crypto Crime Report 83-93 (Feb. 2025). *See also How to Use Blockchain Intelligence to Investigate Crypto Crime*, Chainalysis (May 9, 2024), https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/ (explaining that new tools have significant implications for user privacy on the blockchain).

336 Arthur E. Oldehoeft, *Foundations of a Security Policy for Use of the National Research and Educational Network*, Nat'l Inst. of Standards & Tech. 43 n. 11 (1992), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf.

337 *See Pseudonym*, Merriam-Webster, https://www.merriam-webster.com/dictionary/pseudonym (last visited Jan. 15, 2026).

338 Andreas Pfitzmann & Marit Hansen, *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* 21 (Aug. 10, 2010), https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

339 Miranda Mourby & Elaine Mackey, *Identity, Profiles and Pseudonyms in the Digital Environment*, *in* The Boundaries of Data 275, 280-81 (Bart van der Sloot & Sascha van Schendel eds., 2024).

340 GDPR, *supra* note 334, art. 4(1).

341 *See e.g.*, Claire Vishik & Giusella Finocchiaro, *Relative Anonymity: Measuring Degrees of Anonymity in Diverse Computing Environment*, *in* ISSE 2009 Securing Electronic Business Processes 200-03 (Norbert Pohlmann et al. eds., 2010), https://doi.org/10.1007/978-3-8348-9363-5_19 (defining absolute and relative anonymity and strategies for measuring data anonymity and anonymity in processes and transactions).

342 Thais Sardá et al., *Understanding Online Anonymity*, 41 Media, Culture & Soc'y 557, 559 (2019), https://doi.org/10.1177/0163443719842074.

343 *Id.,* at 559.

2.6.2. Techniques for Transaction Anonymization: Mixers and Tumblers

Another basic form of privacy involves concealing which individual entity, from a defined set of possible participants, performed a particular action. This approach ensures that, even when observers know that one entity within a known group carried out a specific action, they cannot determine which entity it was, similar to the example of the bank robbery *(See below Figure 18)*.

FIGURE 18.

The Bank Robbery

One particularly notable bank robbery involved a suspect dressed in a highly conspicuous outfit: "a dayglo vest, safety goggles, a dust mask, and a blue shirt . . . ."[344] At first glance, such attire would seem ill-suited to a robbery, given its visibility. However, the robber in this case employed an unusual tactic, reminiscent of the film *The Thomas Crown Affair*. Prior to the robbery, the robber posted an advertisement on Craigslist "offering a potential job for people showing up in the vicinity of the bank dressed as he planned to be dressed at the time of the robbery." As a result, when the robbery occurred, there were "a number of similarly dressed people in the area of the bank . . . ."[345] When the police showed up at the crime scene, they found more than a dozen individuals matching the suspect's description, causing significant confusion and obscuring which individual was the actual criminal.

The technique known as a "mixer" or "tumbler" is designed to obscure the true originator of a blockchain transaction by disrupting the traceability of funds. Rather than allowing assets to flow directly from a sender's wallet to a recipient's address, mixing services reroute these assets through a complex network of pooled and randomized transactions. This process "mixes" the inputs and outputs from multiple users, concealing the true identities of the transacting parties. The effectiveness of this privacy mechanism depends heavily on the size of the anonymity set —that is, the total number of participants involved. The larger the set, the more difficult it becomes to isolate and identify individual users.

Mixers also enhance the fungibility of blended cryptocurrencies. Fungibility refers to the interchangeability of an individual cryptocurrency with a cryptocurrency of the "same type and value."[346] The obfuscation of "mixed" transactions ensures that individual transactions in the "mixed" pool are indistinguishable from each other. As a result, the fungibility of the entire pool is enhanced because no individual crypto unit can be traced back to its original wallet address.

There are two general types of mixing services. The first consists of cryptocurrencies that integrate mixing mechanisms directly into their transaction process, often as optional privacy features rather than mandatory protocol-level guarantees. Dash, for example, offers an optional feature that allows users to mix funds but does not provide default or comprehensive anonymity comparable to purpose-built privacy coins.[347] These mechanisms are embedded at the protocol level and

344 Austin Modine, *Cops Collar Craigslist* Thomas Crown, The Reg. (Nov. 6, 2008), https://www.theregister.com/2008/11/06/police_catch_craigslist_robber_suspect/.

345 Press Release, Fed. Bureau of Investigation, *U.S. Att'y's Off., W.D. Wash., Former High School Star Athlete Sentenced to Prison for Armored Car Robbery Defendant Used Ad on Craigslist and Flotation Device to Make Escape Following Monroe Robbery* (July 27, 2009), https://archives.fbi.gov/archives/seattle/press-releases/2009/se072709.htm.

346 Tim Copeland, *What Is Fungibility and What Cryptocurrencies Are Fully Fungible?*, The Block (Sept. 10, 2023), https://www.theblock.co/learn/249529/what-is-fungibility-and-what-cryptocurrencies-are-fully-fungible.

347 *How to Buy Dash in 3 Simple Steps – A Beginner's Guide*, Dash (July 11, 2017), https://www.dash.org/news/3simplesteps/.

provide users with enhanced privacy features as part of the native transaction process. The second type of mixing service consists of privacy-preserving protocols that operate as independent applications layered on top of existing blockchain networks, such as Bitcoin or Ethereum. These services —commonly referred to as tumblers or mixers— pool and distribute users' transactions in a manner that obscures their origin and destination. CoinJoin, a protocol that operates on the Bitcoin blockchain, is an example of this second type *(See Figure 19)*.[348] While the first model embeds privacy within the design of the protocol itself, the second enables privacy functionalities across a broader ecosystem by offering optional services to users of otherwise transparent blockchains.

Like CoinJoin, Tornado Cash is an example of a mixer of the second type (For regulatory actions against Tornado Cash, *see below section 6.5.3.B.*). It is conceptually similar to CoinJoin but implemented for Ethereum and other smart contract-enabled blockchains. It also enables users to make their transactions private by obfuscating the link between the sender's address and the recipient's address. Users deposit ETH or ERC-20 tokens into the contract, which pools them and allows withdrawals to new addresses, thereby breaking the on-chain link between sender and recipient. Tornado Cash is generally labelled a mixer but, technically, it does not mix coins in the same way as the other mixers: Users withdraw an equivalent amount to a fresh address rather than receiving back their original coins. Like many other systems, it relies on a technology called Zero-Knowledge Proofs *(See below section 2.6.3.)* and a sufficiently large anonymity set.

FIGURE 19.

CoinJoin: a standalone privacy protocol

The CoinJoin privacy protocol provides the mechanism by which multiple users can combine their inputs into a single Bitcoin transaction and then distribute the outputs in a manner that obscures the link between any specific input and a specific output.[349] Because CoinJoin is not embedded in the Bitcoin protocol itself, it is implemented through applications and wallets (e.g., Wasabi Wallet, Samourai Wallet) that coordinate the process among participants. These applications operationalize CoinJoin by enabling users to combine and "blend" their transactions, thereby breaking the direct link between sender and recipient wallet addresses.

In each round of CoinJoin, only the aggregate set of inputs and outputs is visible, with no indication of which input corresponds to which output. A notable variant, Chaumian CoinJoin, enhances privacy through the use of blind signatures, which allow transactions to be signed without disclosing their origin or destination.[350] Users may also participate in multiple rounds of CoinJoin with different groups, further obscuring the provenance of their assets by mixing them with an expanding set of potential inputs.

348 Greg Maxwell, *CoinJoin: Bitcoin Privacy for the Real World*, Bitcoin F. (Aug. 22, 2013), https://bitcointalk.org/?topic=279249.

349 Tom Barbereau et al., *Beyond a Fistful of Tumblers: Toward a Taxonomy of Ethereum-based Mixers*, in Proceedings of the 44th Int'l Conf. on Info. Sys., 1 (Hyderabad, India Dec. 2023), https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/13.

350Ádám Ficsór et al.,*WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts*, 2 (unpublished manuscript) (Feb. 2021) https://eprint.iacr.org/2021/206.pdf.

2.6.3. Zero-knowledge Proofs

Zero-knowledge proofs (ZKPs) are a class of cryptographic protocols that enable one party, known as the *prover*, to mathematically prove to another party, called the *verifier*, that a certain piece of information is true. It might also seek to prove that the prover holds some combination of public or private data, without revealing *anything else* about that piece of information.[351] In essence, ZKPs allow for verification without requiring the underlying data to be revealed.[352]

ZKPs possess key properties:

- *Completeness*. This property covers the idea that "it should be possible to 'prove' a true theorem."[353] In other words, the protocol should allow the prover to do something that convinces the verifier that the statement is true. If the prover and the verifier are honest, the verifier ought to be convinced.
- *Soundness*. The protocol should be sound —"it should not be possible to 'prove' a false theorem."[354] In other words, a dishonest prover should not be able to convince a verifier of an untrue statement.
- *Zero-knowledge*. With zero-knowledge, nothing about the private data is revealed, aside from the fact that the private data can satisfy the claim that is being proven. In other words, the prover can prove to the verifier that the prover knows a specific piece of information without revealing the information itself (or, more expansively, anything else about the statements).
- *Succinctness*. While not strictly a ZKP property, many ZKP protocols prioritize succinctness. Succinctness suggests that the proof is short (in bytes) and can be verified very quickly, *even if* the underlying claim being proven involves a heavy and time-consuming computation.

These properties make ZKPs particularly powerful in blockchain contexts, where participants need to validate transactions or prove compliance with protocol rules without exposing sensitive data about amounts, identities, or account balances.

351 Vitali Bestolkau & Ignas Apšega, *Zero Knowledge Proof—How it Works and the Alibaba Cave Experiment*, Byont Labs, https://www.byont.io/blog/zero-knowledge-proof-how-it-works-and-the-alibaba-cave-experiment (last visited Jan. 15, 2026); Oleksandr Kuznetsov et al., *Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms*, 12 IEEE Access 49228, 49231-34 (2024), https://doi.org/10.1109/ACCESS.2024.3384705.

352 There are many subtleties involved. For instance, a more precise definition might more narrowly specify the types of information that can be proven or clarify that the "proof" often reflects an extremely high statistical probability rather than absolute certainty. However, the core concept—that it is possible to demonstrate the truth of a statement without disclosing any additional information—is sufficient for most purposes. A well-constructed zero-knowledge proof yields a mathematical proof that can be verified efficiently by the verifier.

353 Shafi Goldwasser, Silvio Micali & Charles Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, 18 Soc'y for Industrial & Applied Mathematics J. Computing 186, 189 (1989). https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.

354 *Id.,* at 189.

FIGURE 20.

Practical value of Zero-Knowledge Proof for privacy

In daily life, individuals frequently disclose more personal information than necessary. For example, when purchasing age-restricted goods in the United States, a buyer (the prover) must convince a seller (the verifier) that the buyer is above a certain age. A simple binary confirmation should suffice. However, the current system typically requires the buyer to present an identification card that reveals not only the buyer's date of birth but also their address, photograph, and other biometric data.

Similarly, when proving one has sufficient income for purposes such as renting an apartment or securing a mortgage, the requirement is often just to show that one's income exceeds a specified threshold. Nonetheless, individuals are routinely asked to provide full account statements that expose much more, including precise bank account balances and other financial details. In the context of voting, the essential criteria are that the individual be registered to vote at the given polling place and confirmation that they have not already voted in the current election. Yet in many systems, such as mail-in voting, a voter's identity is linked to their ballot in ways that may compromise the privacy of their vote.

In all of these scenarios, the ability to prove the truth of a specific claim —such as being over a required age— without disclosing the underlying data —such as the person's exact birthdate— would represent a significant improvement in privacy protection. This is precisely the type of functionality that ZKPs are designed to support.

In a digital currency context, the most widely used implementation of ZKPs has been around the ability to make confidential transactions. Some blockchains use ZKPs to provide transaction privacy[355] when performing certain on-chain actions. Tornado Cash and RAILGUN rely on zero-knowledge proofs (specifically Zero-Knowledge Succinct Non-Interactive Argument of Knowledge or zk-SNARKs) within Ethereum smart contracts to enable private transactions on-chain.[356] In these systems, ZKPs allow a participant to prove the validity of a transaction (e.g., things like proof that sufficient funds exist for a payment) without disclosing information about the precise amount or the identities of the parties.[357]

ZKPs have also been used or proposed for things like proving membership in a set (i.e., showing that a user is on a whitelist without revealing which member of the set the user is). They can also be used to prove *non-membership* in a set (i.e., showing that an address is not associated with a known set of illicit addresses). ZKPs can

355 It could be discussed whether they really provide full anonymity, since external factors (such as timing or metadata) may still reveal information: technically they provide *obfuscation of transaction linkage.*

356 *See* Thomas Chen et al., *A Review of zk-SNARKs*, ARXIV 14-17 (Oct. 25, 2023), https://arxiv.org/abs/2202.06877 (discussing the Tornado Cash protocol and its use of a liquidity pool where coins get "mixed" with each other); Vladimir Popov et al., Blockchain Privacy and Self-Regulatory Compliance: Methods and Applications 15-16 (Apr. 1, 2024) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4787693 (discussing the RAILGUN protocol). Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) are cryptographic proof that enables parties to verify the "truth" of a statement without revealing any information about the statement. Maksym Petkus, *Why and How zk-SNARK Works*, ARXIV 1, 4 (June 17, 2019), https://arxiv.org/pdf/1906.07221.

357 *See* Aritra Banerjee, Michael Clear & Hitesh Tewari, *Demystifying the Role of zk-SNARKs in Zcash*, 2020 IEEE CONF. ON APPLICATION, INFO. & NETWORK SEC. 12, 16-17 (Nov. 2020); Zooko Wilcox & Josh Swihart, *Zcash, the HTTPS of Blockchains*, NAKAMOTO (Jan. 2, 2020), https://nakamoto.ghost.io/zcash-the-https-of-blockchains/.

show proof of reserves (i.e., an exchange proving that a user can cover their liabilities, without revealing the user's actual assets, liabilities, or wallet address). At this point, ZKPs are being integrated into essentially every level of digital currency infrastructure. ZKPs are used for on-chain identity; for instance, Worldcoin uses ZKPs as part of their identity protocol. ZKPs are also used to improve scalability. For example, projects such as zkSync and StarkNet employ *zero-knowledge rollups*,[358] which perform computations off-chain and then submit a succinct proof of those transactions on-chain.[359]

2.6.4. Privacy Coins

As the name suggests, "privacy coins" (also known as "anonymity-enhancing cryptocurrencies")[360] are designed from the ground up to render the tracing of a transaction exceedingly difficult, akin to traditional cash transactions.[361] They employ advanced cryptographic techniques —such as ZKPs (discussed above, section 2.6.3.), ring signatures, stealth addresses, and confidential transactions— to obfuscate transaction details, including sender and/or receiver addresses, asset type, quantity, and the transaction timeline.[362] Cryptocurrencies, such as Zcash and Monero, were explicitly designed to provide effective privacy protections outside of an Ethereum context.

1. Monero

Monero conceals the identity of the parties to a transaction and the transaction amount by default,[363] through three privacy enhancing technologies —ring signatures, stealth addresses, and ring confidential transactions (RingCT).[364]

Monero's ring signatures are a cryptographic mechanism that obfuscates a transaction's origin by combining a user's transaction input with those of several other users. When a transaction occurs, Monero's blockchain incorporates a ring of possible signers, mixing the true sender's public key with several decoy keys that are selected according to algorithms designed to mimic real spending behavior, rather than being purely random draws from the blockchain. The fact that transactions are signed by multiple possible signers makes it computationally infeasible to determine which member of the ring is the actual sender, thereby ensuring transactional unlinkability.[365] This feature depends on the number of participants in the ring signature set. As Monero has evolved, the number of participants in each mix has increased, expanding the anonymity set and the number of plausible historical outputs from which any given transaction input could have originated.[366] However, the use of repeated small-group mixing methods carries inherent risks of data leakage.[367]

358 A *zero-knowledge rollup* (zk-rollup) bundles many on-chain transactions, delegates computation and state changes of these transactions to an off-chain network and then validates these on-chain transactions in batches using zero-knowledge proofs. This protocol allows for blockchain scalability because it moves computation to an outside system "while storing transaction data on-chain." *See What Are Zero-Knowledge Rollups (ZK Rollups)?*, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-are-zero-knowledge-zk-rollups (last visited Jan. 15, 2026).

359 *See* Chen, et al., *supra* note 356, at 17-21.

360 *Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies*, Chainalysis (Apr. 18, 2023), https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/.

361 In defense of privacy blockchains, see Jerry Brito, *The Case for Electronic Cash: Why Private Peer-to-Peer Payments Are Essential to an Open Society*, Coin Center (Feb. 2019), https://www.coincenter.org/app/uploads/2020/05/the-case-for-electronic-cash-coin-center.pdf.

362 *See* Pablo Marcello Baquero, *Layers of Privacy in the Blockchain: From Technological Solutionism to Human-Centred Privacy-Compliance Technologies*, 19 Int'l J.L. Context 51, 57 (2022), https://doi.org/10.1017/S1744552322000465.

363 Tao Zhang, *Privacy Evaluation of Blockchain Based Privacy Cryptocurrencies: A Comparative Analysis of Dash, Monero, Verge, Zcash, and Grin*, 8 IEEE Transactions Sustainable Computing 574, 575 (2023).

364 *What is Monero (XMR)?*, Monero, https://www.getmonero.org/get-started/what-is-monero/ (last visited Jan. 15, 2026). *See also Id.*

365 Zhang, *supra* note 363, at 575.

366 *See* Brandon Goodell, Sarang Noether & Arthur Blue, *Concise Linkable Ring Signatures and Forgery Against Adversarial Keys*, Cryptology ePrint Archive 4-5, 8-11 (2019), https://eprint.iacr.org/2019/654 (when transactions are repeatedly mixed within small groups, overlapping membership and decoy keys make it easier for observers to narrow down the real participant).

367 Malte Möser, et al., *An Empirical Analysis of Traceability in the Monero Blockchain*, Proc. of the 18th Privacy Enhancing Techs. Symp. 1, 6-7 (Apr. 23, 2018), https://arxiv.org/pdf/1704.04299.

Coupled with sender obfuscation, Monero generates one-time destination addresses for each transaction recipient —so-called "stealth addresses." These stealth addresses are unique, single-use public keys derived from the recipient's address and generated by the transaction sender, such that only the intended recipient can recognize and spend the output. As a result, stealth addresses prevent third parties from linking multiple transactions to the same recipient address, enhancing recipient privacy.[368]

Additionally, Monero transaction amounts are hidden by default through Ring Confidential Transactions (RingCT).[369] While block rewards (newly minted XMR) follow specific protocol rules, once outputs are spent, the amounts are concealed in the same manner as other transactions.[370] Transaction values are therefore confidential and not publicly visible on the blockchain, yet the protocol still enables network nodes to verify the validity of transactions —including that inputs equal outputs and that no new value is created— without revealing the underlying amounts.

2. Zcash

Zcash is an open-source privacy cryptocurrency which utilizes privacy features, such as ZK-SNARKs, to encrypt users' transaction information.[371] While Zcash[372] uses ZKPs, it integrates, as a Layer 1 blockchain, proof mechanisms directly into the protocol to support shielded transactions in which the sender, receiver, and amount are hidden. Zcash facilitates the confidential ownership and transfer of data, including transaction metadata.[373]

Zcash provides two types of transactions:

- transparent transactions, in which users transact using public addresses, and
- shielded transactions, in which parties utilize private addresses that are encrypted to obscure information on their identities and the transaction amount.[374]

Privacy-focused cryptocurrencies, such as Monero and Zcash, have been delisted from certain exchanges, including OKX,[375] because of concerns that their privacy features could facilitate illicit activities, such as money laundering or terrorism financing. Nevertheless, these cryptocurrencies have not been subject to the same degree of regulatory enforcement as mixers. For example, in 2023, U.S. authorities imposed sanctions on Tornado Cash *(See below section 6.5.3.B.).*[376]

2.7. PROPERTIES AND LIMITATIONS

Blockchain systems are often described as possessing technical and institutional properties that distinguish them from traditional centralized databases. These properties, however, are not absolute guarantees and they operate subject to important limitations.

368 Zhang, *supra* note 363, at 575.

369 This is through a feature called Ring Confidential Transactions. *See RingCT*, MONERO, https://www.getmonero.org/resources/moneropedia/ringCT.html (last visited Jan. 15, 2026).

370 Zhang, *supra* note 363, at 575.

371 *What Is Zcash?*, ZCASH, https://z.cash/learn/what-is-zcash/ (last visited Jan. 15, 2026).

372 *See* Thomas Chen, et al., *supra* note 356, at 11-14.

373 *How Is Zcash Different from Bitcoin?*, Z.CASH, https://z.cash/learn/how-is-zcash-different-than-bitcoin/ (last visited Jan. 15, 2026).

374 Steven McKie, *The Case for Zcash & Privacy*, MEDIUM (Feb. 5, 2019), https://medium.com/amentum/the-case-for-zcash-74fe4b7fbef8; *see also* Thomas Chen et al., *supra* note 356 at 11.

375 OKX *Exchange Delists Privacy Coins, Including Monero, Dash, and ZCash*, CRYPTORANK (Dec. 29, 2023), https://cryptorank.io/news/feed/02f12-okx-delists-privacy-coins-monero-dash-zcash.

376 Press Release, U.S. ATT'Y'S OFF., S.D.N.Y., *Tornado Cash Founders Charged With Money Laundering And Sanctions Violations* (Aug. 23, 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations.

2.7.1. Notable Properties

Blockchain provides four notable properties: fault tolerance, attack resistance, collusion resistance,[377] and censorship resistance. Together, these properties help explain why blockchains are frequently characterized as robust and trustworthy infrastructures in adversarial environments, even though each property is contingent on the underlying consensus mechanism and network conditions.

Fault tolerance refers to the system's capacity to continue functioning correctly despite failures of individual nodes or communication channels.[378] In distributed networks, some participants may behave unpredictably or suffer outages. A blockchain can withstand such failures through its consensus protocol, which ensures that the ledger remains consistent and accessible under defined assumptions as long as a sufficient proportion of nodes operate honestly. In this sense, fault tolerance is closely related to the notion of "liveness," namely the ability of the system to keep processing transactions despite partial failures.[379]

Attack resistance denotes the ability of blockchain systems to resist adversarial attempts to disrupt or manipulate the ledger. Because decentralized systems lack sensitive central points and because transactions are recorded immutably and secured through cryptographic mechanisms, attackers must overcome significant computational or economic barriers in order to alter past records or interfere with consensus. This makes the ledger highly resilient against tampering and double-spending attacks, particularly in public blockchains with large, decentralized participation.

FIGURE 21.

Double-spending attacks

A double-spending attack occurs when someone attempts to spend the same unit of cryptocurrency more than once by broadcasting two conflicting transactions. In a blockchain system, consensus protocols and cryptographic mechanisms prevent such manipulation:

In proof-of-work systems, an attacker would need to have a controlling share, typically more than 50%, of the network's computational power to consistently rewrite the ledger and make a fraudulent transaction appear valid. This high cost makes double-spending economically impractical in most circumstances, particularly on large networks.[380]

In proof-of-stake systems, an attacker would need to hold and risk a very large proportion of the staked assets to override consensus. While the exact threshold depends on protocol design, this again renders sustained double-spending attacks economically irrational for most actors.[381]

Collusion resistance means that most blockchains maintain their integrity as long as a majority of their participants do not coordinate maliciously against the network. Blockchain networks can withstand coordinated efforts by subsets of participants seeking to subvert the system for their collective advantage. The decentralized nature of participation, often involving a large number of pseudonymous or anonymous actors, makes it exceedingly difficult to coordinate such large-scale

377 The three first properties are discussed by Ethereum's co-founder, Vitalik Buterin, *The Meaning of Decentralization*, Medium (Feb. 6, 2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

378 Anil Kumar et al., Advances in Nonlinear Variational Inequalities, ch. *Optimization of Fault Tolerance in Distributed Systems via Consensus Protocol*, 436 (2025), https://doi.org/10.52783/anvi.v28.3909.

379 *Id*. at 457.

380 Gert-Jaap Glasbergen, James Lovejoy & Anne Ouyang, *51% Attacks*, MIT Digit. Currency Initiative, https://www.dci.mit.edu/projects/51-percent-attacks (last visited Jan. 15, 2026).

381 Mikolaj Karpinski et al., *Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus*, 21 Sensors 1, 1, 12 (2021). Some scholars argue that even adversaries that control less than 50% of the computational power may try to launch a double-spend attack. They explain that "high-value transactions can present an incentive for a rational adversary to attempt a double-spend attack if they expect to profit." *See* Yanni Georghiades et al., *Majority is Not Required: A Rational Analysis of the Private Double-Spend Attack from a Sub-Majority Adversary*, arXiv 1, 1-2 (Dec. 12, 2023), https://arxiv.org/abs/2312.07709.

collusion. Specifically, blockchain consensus mechanisms, such as proof of work or proof of stake, are designed to raise the cost of collusion, requiring a coalition to accumulate an impractically large share of computational power or staked assets before it can compromise the ledger's integrity.[382]

From an economic perspective, rational participants in blockchain systems have little incentive to collude.[383] Coordinated attacks carry high costs and uncertain outcomes, with a substantial risk of failure that would result in wasted resources, reputational damage, or punitive loss of coins ("slashing"). At the same time, scholars have noted that collusion may arise indirectly through shared infrastructure, validator concentration, or common intermediaries, even in the absence of explicit coordination.[384] While smaller blockchains have occasionally been attacked via participant collusion,[385] major blockchains —by virtue of their scale, participant diversity, and stronger economic deterrents— are generally considered more robust against this type of threat.

Finally, the decentralized nature of blockchains aims to promote *censorship resistance*. There is no single point of failure or control and no single entity able to unilaterally make decisions that censor or otherwise chill certain transactions. Some scholars consider that the term "censorship resistance" can be used interchangeably with the term "decentralization."[386] For them, decentralization "conveys the meaning of censorship resistance . . . by any third party or through a coordinated effort of third parties,"[387] particularly for the *network* and *protocol* layers of blockchain-based services.[388] At the same time, censorship resistance should be understood as a relative rather than absolute property, as practical constraints — including validator concentration, shared infrastructure, or regulatory pressures— may still enable forms of transaction filtering.

Together, these four properties explain why blockchains are considered robust infrastructures for maintaining a trustworthy and tamper-resistant ledger in adversarial and decentralized environments.

2.7.2. The Blockchain Trilemma

Decentralized blockchain systems may, in some respects, be more resilient than centralized systems that rely on a single server and therefore present a single point of failure. Nevertheless, blockchain systems are not immune to vulnerabilities *(see Chapter 5)*. One of the most frequently identified structural challenges they face is commonly described as the "blockchain trilemma."[389] This

382 However, it is arguably easier to launch such an attack on proof of stake networks. While in proof-of-work systems like Bitcoin the widespread distribution of mining infrastructure makes collusion unlikely, this dynamic does not necessarily carry over to proof-of-stake systems. In proof of stake, collusion depends on accumulating stake rather than coordinating physical hardware, which seems a notably easier path for well-capitalized actors. In Ethereum, for example, the five largest staking entities now control a little over 60% of staked ETH. *See Ethereum Staking Pool Ratings*, Rated Labs, https://explorer.rated.network/?network=mainnet&view=pool&timeWindow=1d&page=1&pageSize=15&poolType=all (last visited Jan. 15, 2026).

383 Yuting Li et al., *Rational Protocols and Attacks in Blockchain System*, 2020 Security & Comm. Networks, 1, 2 (2020), https://onlinelibrary.wiley.com/doi/10.1155/2020/8839047.

384 Hanna Halaburda, *The Hidden Danger of Re-Centralization in Blockchain Platforms*, Brookings (Apr. 10, 2025), https://www.brookings.edu/articles/the-hidden-danger-of-re-centralization-in-blockchain-platforms/; see *also* Stephanie Dunbar, *Evaluating Validator Decentralization: Geographic and Infrastructure Distribution in Proof-of-Stake Networks*, Messari (June 1, 2023), https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks.

385 For the most part, attacks on blockchains have been levied by what many suspect is a small group of individuals who replicate the functionality of a larger attack that required widespread collusion. This is not likely when dealing with larger blockchain networks and is probably economically prohibitive.

386 Huseyin Oguz Genc & Eray Acikgoz, *Constructing an Evaluation Framework for Full Decentralization: A Case Study on DeFi's Stable Currency Issuance Services – CDP Protocols*, 8 Stan. J. Blockchain L. & Pol'y 177 (2025), https://stanford-jblp.pubpub.org/pub/cdp-protocols.

387 *Id.*

388 Meanwhile, the authors also argue that user-facing applications (*application layer*) are the most viable technical component in terms of enforceability of regulations. *See id.*

389 *Blockchain Trilemma: Fast, Secure, and Scalable Networks*, Cryptopedia (June 28, 2022), https://www.gemini.com/cryptopedia/blockchain-trilemma-decentralization-scalability-definition.

concept refers to the widely held view that a blockchain network cannot simultaneously maximize three properties —decentralization, security, and scalability— but must instead make trade-offs among them.[390] The idea is often attributed to Ethereum co-founder Vitalik Buterin.[391]

In this context, scalability may be understood as a question of efficiency—namely, the system's ability to process a high volume of transactions with low latency and cost as usage increases. Systems that prioritize decentralization and security may therefore face slower processing and higher costs, whereas more efficient systems may rely on greater coordination among participants or some degree of concentration of control.

This tension has been particularly evident in the first generation of blockchain applications, namely Layer 1 solutions such as Bitcoin, Ethereum, Solana, or Avalanche. These networks prioritize security and decentralization, or rebalance these objectives in different ways, often at the expense of scalability. As a result, they may experience slower transaction processing and higher fees during periods of congestion. A significant shift, however, has taken place over the past three years with the emergence and growing adoption of Layer 2 solutions, such as Polygon, Arbitrum, and Optimism, as well as other protocols adopting similar architectures. Layer 2 systems seek to address scalability constraints by processing transactions off-chain while anchoring final settlement on the underlying Layer 1 blockchain. This approach can improve throughput and reduce costs, while seeking to preserve the security properties of the base layer.

While the blockchain trilemma continues to shape both theoretical and practical debates, the development of Layer 2 architectures suggests that these trade-offs can be reconfigured. Rather than eliminating the underlying tensions, these approaches redistribute them across different layers of the system, shifting where efficiency gains are achieved and where control, coordination, and risk are concentrated.

390 Nathan Crooks, *What is the Blockchain Trilemma*, The Block (Sept. 19, 2023), https://www.theblock.co/learn/249536/what-is-the-blockchain-trilemma.

391 Vitalik Buterin, *Why Sharding is Great* (April 7, 2021) https://vitalik.eth.limo/general/2021/04/07/sharding.html; *See also*: Vitalik Buterin, *Shardin FAQ* (Dec. 31, 2017), https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html; Taishi Nakai et al., *A Formulation of the Trilemma in Proof of Work Blockchain*, 12 IEEE Access 80559, 80560-61 (2024), http://doi.org/10.1109/ACCESS.2024.3410025.

FIGURE 22.

Layer 1 and Layer 2 solutions

Layer 1 refers to the foundational blockchain layer, where transactions are executed, validated, and permanently recorded directly on the network.[392] Each Layer 1 blockchain operates with its own consensus mechanism and native token, which together provide the security and governance structure of the network. Prominent examples of Layer 1 blockchains include Bitcoin, Ethereum, Solana, Cardano, Avalanche, and Polkadot. These platforms differ in design, but all serve as primary infrastructures on which decentralized applications and protocols can be built.

Layer 2 solutions, by contrast, are secondary protocols, designed to operate on top of a Layer 1 blockchain, most often Ethereum, with the primary aim of improving scalability.[393] Layer 2 systems offload most transaction processing from the base chain, while ultimately relying on the Layer 1 network for security assurances and final settlement. This architecture enables them to increase throughput, reduce congestion on the main chain, and lower transaction fees for users. Notable examples include Polygon (a sidechain network interoperable with Ethereum), Arbitrum and Optimism (Ethereum rollups), the Lightning Network (for Bitcoin), as well as a variety of payment channel and state channel networks.

The efficiency of Layer 2 systems stems from their operational model: They execute the majority of transactions off-chain, submitting only aggregated proofs or settlement data to a Layer 1 blockchain. In this way, Layer 1 functions as the ultimate arbiter of security and dispute resolution, while Layer 2 protocols enhance performance and scalability. Nonetheless, the adoption of Layer 2 introduces new considerations and potential trade-offs, including differences in decentralization, security assumptions, and interoperability, depending on the specific implementation.

392 Ankit Gangwal et al., *A Survey of Layer-Two Blockchain Protocols*, 209 J. Network & Comput. Applications 103539, 103539 (2023), https://arxiv.org/pdf/2204.08032.

393 *Id.* at 103539-40.

KEY TAKEAWAYS

■ A blockchain is a **distributed digital ledger** composed of blocks of data that are cryptographically linked in chronological order. Each **block** contains a cryptographic hash of the previous block, creating a chain in which modifying past data would alter subsequent hashes and be detectable by the network. **Nodes** —computers connected to the network that store, synchronize, and validate copies of the ledger— independently verify transactions and blocks in accordance with the protocol's rules. **Validators or miners** propose new blocks that are appended to the chain once the network's consensus requirements are satisfied.

■ Several interrelated features distinguish blockchain technology from traditional centralized systems. The first of these features is **decentralization**, often identified as blockchain's core principle, since it enables direct peer-to-peer interactions without necessarily relying on traditional intermediaries. Decentralization lacks a single authoritative definition and is better understood as a continuum which broadly denotes the distribution of authority, power, and decision making among network participants. **Transparency** constitutes a second defining feature: blockchain transactions and operations are generally open and verifiable, enabling participants to audit the ledger without relying on a central authority. **Immutability**, closely tied to mechanisms for consensus and incentives for validators, ensures that data, once recorded on the blockchain, cannot be altered or erased without detection. **Cryptography** underpins all of these features: Through hashing and public-private key systems, it ensures the secure identification, verification, and control of digital assets, forming the technical foundation on which decentralization, transparency, and immutability depend.

■ The operation of blockchain networks relies on participants assuming diverse roles. **Core developers** design and maintain the protocol's underlying codebase. **Miners or validators** execute transactions, secure the ledger, and sustain network consensus. **Intermediaries** —such as exchanges, custodians, and wallet providers— facilitate market access by mediating between the technical infrastructure and end users: Exchanges enable trading of digital assets, while custodians hold those assets and manage the private keys needed to access them. **Users** retain pseudonymous identities, though their on-chain activity remains traceable.

■ The integrity of blockchains rests on two foundational cryptographic principles: hashing and public key cryptography. **Hashing** applies a mathematical function to data to produce fixed-length outputs that serve as cryptographic fingerprints, making any alteration of the underlying data computationally detectable. **Public key cryptography** enables pseudonymous digital identities that allow participants to securely send and receive assets while proving ownership through private keys. Together, these mechanisms ensure both the immutability of records and the authenticity of transactions, though they also introduce a critical vulnerability: The loss or compromise of private keys results in the irretrievable loss of the associated assets.

■ **Consensus mechanisms** enable network participants to reach agreement on the validity and ordering of transactions, thereby allowing blocks to be added to the blockchain without reliance on a central authority. **Proof of work**, pioneered by Bitcoin, secures the network by requiring miners to complete computationally intensive tasks before proposing a new block, making attacks economically costly and, in large networks, generally impractical. **Proof of stake**, adopted by Ethereum among others, replaces computational effort with financial collateral: Validators stake the network's native token and risk losing it if they act dishonestly. Further variants, such as Proof of Authority, Practical Byzantine Fault Tolerance, and Proof of Burn, represent experiments in balancing scalability, efficiency, and decentralization with varying trade-offs.

■ Disagreements or simultaneous block proposals can produce chain splits known as forks. **Forks** may be accidental —arising from network latency— or intentional, when participants deliberately diverge from existing protocol rules to introduce upgrades, correct vulnerabilities, or resolve governance disputes. When intentional forks result in permanent splits, two independent chains emerge, each carrying the shared history up to the point of divergence.

■ Blockchain networks can be public, permissioned, or private. **Public blockchains** maximize decentralization and accessibility, allowing anyone to participate without prior authorization. **Permissioned blockchains** restrict participation to verified actors, often within a consortium, offering greater control over governance and data visibility. **Private blockchains** go further by concentrating authority in a single operator or a tightly controlled group and restricting access to both participation and underlying data. Some commentators question whether permissioned and private systems — which reintroduce elements of centralized control— should be classified as 'true blockchains' at all, or whether they are better understood as a subset of distributed ledger technologies more broadly.

■ Beyond their ledger function, blockchains support a wide range of digital assets, including fungible cryptocurrencies, tokens, stablecoins, and non-fungible tokens (NFTs). **Native coins**, such as bitcoin and ether, function as mediums of exchange and stores of value within their respective ecosystems. The volatility of such cryptocurrencies has limited their utility for stable transactions and spurred the creation of **stablecoins** —digital assets pegged to external reference assets, such as fiat currencies or commodities. **Tokens** extend blockchain functionality by enabling utility functions, governance rights, and asset representation on top of existing blockchain infrastructure. **Non-fungible tokens (NFTs)** provide unique on-chain identifiers for digital or physical assets, enabling new economic models in areas such as art, gaming, and identity management, though they reference rather than contain the underlying asset.

■ Blockchain **smart contracts**, introduced by Ethereum in 2015, are self-executing programs that automatically carry out predefined agreements once specified conditions are met. Key features include automation and immutability: Transactions execute exactly as programmed and, by default, the underlying code cannot be altered once deployed, though architectural techniques such as proxy patterns can allow for upgrades under defined conditions. Execution requires users to pay 'gas,' a fee that compensates validators for computational work and deters abuse of network resources. **Oracles** provide smart contracts with access to off-chain information, enabling them to respond to external conditions. However, oracles reintroduce reliance on trusted external actors, thereby partially re-creating the intermediary structures that smart contracts were intended to operate without.

■ Building on smart contracts, **Decentralized Autonomous Organizations (DAOs)** offer new models of governance and collective action. DAOs encode rules of decision making and treasury management into blockchain-based protocols, seeking to reduce reliance on hierarchical structures through participatory, token-based governance. By making members simultaneously principals and decision makers, DAOs aim to mitigate certain agency problems while offering enhanced transparency, accountability, and operational agility compared to traditional organizational forms.

■ Blockchain systems face a structural tension between transparency and confidentiality, which has led to the development of **Privacy-Enhancing Technologies (PETs)**. These include pseudonymity, mixers and tumblers, zero-knowledge proofs, and privacy coins. Rather than forming a strict hierarchy, each technique addresses a distinct dimension of privacy —obscuring identities, concealing which participant performed a given action, or hiding the details of the transaction itself.

■ Blockchain networks exhibit four fundamental properties that underpin their robustness: fault tolerance, attack resistance, collusion resistance, and censorship resistance. **Fault tolerance** allows the network to function reliably even when individual nodes fail or behave unpredictably. **Attack resistance** arises from the cryptographic and consensus mechanisms that make tampering, including double-spending, computationally or economically prohibitive. **Collusion resistance** ensures that the ledger remains secure as long as a majority of participants do not coordinate maliciously, with decentralized participation and economic disincentives reducing the risk of large-scale attacks. Finally, the absence of a single point of control supports **censorship resistance**, making it difficult for any single actor to suppress transactions —though this property is relative rather than absolute, as validator concentration or regulatory pressure may still enable forms of transaction filtering.

■ Despite their advantages, blockchains face inherent trade-offs, often described as the '**blockchain trilemma**,' which posits that no network can simultaneously maximize decentralization, security, and scalability. However, this conclusion should be nuanced in light of the development of Layer 2 solutions —systems built on top of an existing blockchain (Layer 1). Layer 2 architectures address scalability by executing transactions off-chain while anchoring final settlement on the underlying Layer 1. This approach can improve throughput and efficiency, while seeking to preserve the security and decentralization properties of the base layer.

CHAPTER 3

Blockchain Governance

CHAPTER 3 TABLE OF CONTENTS

CHAPTER 3. BLOCKCHAIN GOVERNANCE 86
3.1. What is "Blockchain Governance"? 88
3.1.1. Governance of and by the Infrastructure 89
3.1.2. Eight Areas of Governance 90
3.1.3. Who Makes Governance Decisions? 91
3.2. On-Chain vs Off-Chain Governance 94
3.2.1. Off-Chain Governance 94
3.2.1.A. Off-Chain Governance Actors 94
1. Legal Entities 95
2. Core developers or maintainers 96
3. Market Forces and External Pressures 97
3.2.1.B. Case Studies 98
1. Bitcoin 99
2. Ethereum 101
3. Other Blockchains 103
a. Solana 103
b. EOS 104
c. EigenLayer 104
d. Algorand and Avalanche 104
3.2.2. On-Chain Governance 105
3.2.2.A. Mechanisms and Dynamics 105
1. Token-Weighted Voting 106
a. Direct Token Governance 106
b. Staked-Based Governance 108
c. Delegate-Based Governance (Proxy Voting) 109
2. Automated Execution via Code 110
3.2.2.B. Case Studies 113
1. Tezos 113
2. Polkadot 113
3. Cosmos 113
4. Uniswap 113
3.2.2.C. Challenges of On-Chain Governance 114
1. Vote Buying 114
2. Majority Governance Attacks 115
3. Social Pressures and Informal Negotiations 118
3.3. Conclusion 121
KEY TAKEAWAYS 124

CHAPTER 3
Blockchain Governance

The ideal of operating without trusted intermediaries presents a fundamental paradox: Blockchain systems still require governance. As software systems, blockchains must be designed, deployed, maintained, and periodically modified. These updates may address security vulnerabilities, improve performance, implement more efficient cryptographic methods, or add new functionalities. The central challenge, therefore, is how to implement these necessary changes within a system explicitly designed to function without central authority —where no single individual or entity holds definitive control over the operations of the system.

3.1. WHAT IS "BLOCKCHAIN GOVERNANCE"?

Blockchain governance encompasses the processes by which the rules of a blockchain network are established, interpreted, and amended (if at all).[394] This includes both the technical protocols encoded in software and the broader ecosystem of formal and informal practices that guide the system's evolution.

While the term "blockchain governance" may evoke comparisons to "corporate governance"[395] —with its focus on decision-making authority, power structures, and organizational hierarchies—[396] this analogy must be qualified.[397] Unlike corporations, where authority flows through ownership, appointment, or delegation among clearly defined roles (owners, managers, workers), blockchain systems operate primarily through software code and the mechanisms for modifying that code.[398] Governance in this context is not limited to allocating decision-making power among actors, but also involves defining and updating the technical infrastructure that constitutes the system itself. At the same time, certain blockchain-based organizations —particularly token-based DAOs, where governance tokens confer voting rights comparable to shareholder voting— may exhibit features analogous to public corporations.

At its core, blockchain governance must address several key questions: Who can propose changes to the protocol? How are these proposals evaluated and approved? What mechanisms exist for implementing updates? And how are disputes resolved when community members disagree? The challenge is that these governance decisions

394 *See generally* Primavera De Filippi, Wessel Reijers & Morshed Mannan, Blockchain Governance (2024), https://direct-mit-edu.stanford.idm.oclc.org/books/book/5817/Blockchain-Governance. *See also* Huseyin Oguz Genc & Eray Acikgoz, *Constructing an Evaluation Framework for Full Decentralization: A Case Study on DeFi's Stable Currency Issuance Services–CDP Protocols*, 8 Stan. J. Blockchain L. & Pol'y 177 (2025), https://stanford-jblp.pubpub.org/pub/cdp-protocols/release/1 (for how blockchain governance is applied in the decentralized autonomous organizations (DAOs) context to manage different tasks for decentralized finance (DeFi) protocols.)

395 Corporate governance is generally defined as "the study of power and influence over decision making within the corporation, which defines the rights and responsibilities of different stakeholders toward the firm." Ying-Ying Hsieh, Jean-Philippe (JP) Vergne & Sha Wang, *The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies*, *in* Bitcoin and Beyond: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 48, 49 (Malcolm Campbell-Verduyn ed., 2017), https://ssrn.com/abstract=2966973

396 *See generally Id*.

397 *See* Rowan van Pelt et al., *Defining Blockchain Governance: A Framework for Analysis and Comparison*, 38 Info. Sys. Mgmt. 21, 25-28 (2021), https://doi.org/10.1080/10580530.2020.1720046; *see also* Wessel Reijers, Fiachra O'Brolcháin & Paul Haynes , *Governance in Blockchain Technologies & Social Contract Theories*, 1 Ledger 134 (2016), https://doi.org/10.5195/ledger.2016.62.

398 Amber Seira et al., *Governance of Permissionless Blockchain Networks*, FEDS Notes (Feb. 9, 2024), https://doi.org/10.17016/2380-7172.3443.

must be made within systems explicitly designed to be decentralized and "trustless." This creates a unique tension: networks built to minimize reliance on central authorities nevertheless require coordinated decision-making to adapt, improve, and survive. Understanding blockchain governance, therefore, requires examining both the code and the complex interplay among technical architecture, economic incentives, social norms, and the communities that maintain these systems.[399]

Blockchain governance is not a monolithic concept but rather a multifaceted phenomenon that operates across technical, social, and economic dimensions. While blockchain systems promise governance without central authorities, the reality is far more complex —involving multiple types of governance, various decision domains, and diverse stakeholders competing for influence. The following sections unpack these different layers to reveal how governance functions in supposedly "ungoverned" systems like blockchain.

Throughout this chapter, it is important to distinguish between different layers of blockchain governance. Governance may operate at the level of the protocol itself (i.e. the core technical rules governing the network), at the level of application-layer organizations such as decentralized autonomous organizations (DAOs), and at the level of a broader ecosystem that may include foundations, corporate entities, and user interfaces. While these layers are distinct, in practice they are deeply intertwined, forming hybrid governance structures that combine code-based mechanisms with organizational and market-based coordination.

3.1.1. Governance *of* and *by* the Infrastructure

The term "blockchain governance" encompasses two distinct but related concepts that are often conflated in practice: governance *of* the infrastructure and governance *by* the infrastructure.

Governance *of* the infrastructure[400] refers to how blockchain systems are governed —the process through which protocols are maintained or updated. This can occur through two primary mechanisms:

1. *Internal governance*: Some blockchains incorporate governance mechanisms directly into their code. These systems enable on-chain decision making for protocol upgrades, parameter adjustments, and resource allocation through native tokens. Decentralized Autonomous Organizations (DAOs) exemplify this approach, where many governance processes are automated and executed through smart contracts.[401]
2. *External governance:* Many blockchains implement off-chain coordination mechanisms, where protocol changes require human intervention through external tools, community discussions, and social consensus. In the case of Bitcoin, for instance, this includes processes like Bitcoin Improvement Proposals (BIPs), core developers' meetings, and the role of foundations or other community leaders.

Governance *by* the infrastructure refers to using blockchain technology as a tool to govern activities beyond the blockchain itself. In this model, blockchain

399 Hanna Halaburda, *The Hidden Danger of Re-Centralization in Blockchain Platforms*, Brookings Inst. (Apr. 10, 2025), https://www.brookings.edu/articles/the-hidden-danger-of-re-centralization-in-blockchain-platforms/.

400 *See e.g.*, Gabriella Laatikainen et al., *A System-Based View of Blockchain Governance*, 157 Info. & Software Tech. 1, 3 (2023), https://doi.org/10.1016/j.infsof.2023.107149. *See generally* Primavera De Filippi & Greg McMullen, Coal. of Automated Legal Applications, Blockchain Rsch. Inst., Governance of Blockchain Systems: Governance of and by Distributed Infrastructure (2018), https://coala.global/wp-content/uploads/2019/02/BRI-COALA-Governance-of-Blockchains.pdf; Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*, 5 Internet Pol'y Rev. 1 (2016), https://doi.org/10.14763/2016.3.427.

401 Johnnatan Messias et al., *Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts,* 1-2 (2023) (unpublished manuscript), https://arxiv.org/abs/2305.17655.

serves as an infrastructure for coordination and decision making in various contexts:[402]

- Decentralized Autonomous Organizations (DAOs) that coordinate human activities[403]
- Blockchain-based voting systems for organizational decisions
- Supply-chain management systems that automate compliance through smart contracts
- Decentralized attestation or credential systems that govern access to services.

While both dimensions are important, "blockchain governance" typically refers to governance *of* the infrastructure —how blockchain protocols themselves evolve and adapt. This focus reflects the fundamental challenge facing decentralized systems: how to coordinate necessary changes without central authority. Understanding this distinction is crucial for analyzing different blockchain systems and their approaches to the governance paradox.

3.1.2. Eight Areas of Governance

Blockchain governance encompasses fundamental decisions about how these systems operate and evolve. A recent analysis[404] of major blockchain networks identified eight key "governance areas" where critical decisions shape both technical architecture and power distribution within the ecosystem:

- **Meta-governance:** The meta-governance framework determines how governance rules are created, modified, or abolished. These "rules about making rules" (also known as "secondary rules") establish how authority is exercised, contested, and legitimized in decentralized systems —analogous to constitutional processes in traditional governance.
- **Block production:** These are the mechanisms for validating transactions and adding new blocks to the ledger. Typically predefined through consensus algorithms (e.g., proof-of-work, proof-of-stake, etc.), these rules fundamentally determine who can participate in securing the network and how.
- **Monetary policy:** Monetary policy decisions govern the creation, distribution, and management of native tokens (also known as "tokenomics"). This includes token generation, maximum supply caps, burning mechanisms, and inflation rates.
- **Software upgrades:** The processes for implementing technical upgrades, from minor parameter adjustments to contentious hard forks, can split communities and create entirely new networks. These processes determine how quickly and smoothly a blockchain can adapt to new challenges.
- **Treasury allocations:** Blockchain governance includes the management of community treasuries and development funds, including decisions about funding priorities, grant distributions, and strategic investments in ecosystem growth.
- **Rewards to contributors:** Governance typically includes mechanisms for rewarding work on block production and beyond, including development, documentation, community building, and governance participation.
- **Standards and interoperability:** Specifications enable interoperability with third-party applications, wallets, and other blockchains. These standards

402 Laatikainen et al., *supra* note 400; Maxat Kassen, *Prospects of Blockchain Governance: Understanding Key Public Values, Principles, Challenges, and Opportunities*, 16 Pol'y & Internet 33 (2024), https://doi.org/10.1002/poi3.365; *see also* De Filippi & Loveluck, *supra* note 400.

403 Fabrice Lumineau, Wenqian Wang & Oliver Schilke, *Blockchain Governance—A New Way of Organizing Collaborations?*, 32 Org. Sci. 500 (2021), https://doi.org/10.1287/orsc.2020.1379.

404 Primavera De Filippi et al., Project Liberty Inst. & BlockchainGov, The Blockchain Governance Toolkit: A Cookbook for a Resilient and Robust Ecosystem (2024), https://www.projectliberty.io/wp-content/uploads/2024/06/PL_Toolkit_Report_v7.pdf.

determine how open and accessible the ecosystem becomes.

- **Security measures and breach responses:** Governance measures intended to reduce the risk of vulnerabilities (e.g., bug bounties, audit requirements) and respond to breaches, attacks, or critical vulnerabilities. These measures create resilience and protect against catastrophic failure.

Beyond these core areas, governance must also address broader questions: How to prevent flawed or malicious code from entering the codebase? Can governance mechanisms evolve without betraying the founding principles of the network? How do technical possibilities align with community values? These questions reveal the ongoing tension between the need for adaptation and the desire for immutability that defines blockchain governance.

3.1.3. Who Makes Governance Decisions?

With blockchain systems, the promise of "decentralized governance"[405] confronts a fundamental challenge: In a system where no one owns the code, who has the right to change it? This question becomes critical when blockchains secure billions in value and where a single flawed update could trigger catastrophic losses.

Blockchain systems face competing imperatives. On the one hand, their ethos demands openness —anyone should be able to participate in governance decisions. On the other hand, unrestricted modification of the code would render the system unstable: Malicious actors could exploit this openness for personal gain; well-intentioned contributors might inadvertently introduce critical software bugs; and contentious changes could destabilize the entire system. This tension between openness and security shapes how governance power is actually distributed.

Early blockchain projects regarded governance as a purely technical matter, mostly operating without formalized governance structures. Bitcoin exemplifies this approach, with a protocol that includes no official governance mechanisms or designated authority. Yet, informal coordination inevitably emerged: Core developers, mining pools, cryptocurrency exchanges, and major token holders began wielding disproportionate influence through opaque, ad-hoc decision-making processes.

This situation has increasingly clashed with the decentralization ideals of blockchain communities. Many communities now pursue "governance formalization," documenting their implicit practices into written documents or "constitutions."[406] While these documents aim to legitimize decision-making processes, significant gaps remain between formal rules and actual power dynamics.[407] This evolution has given rise to the emergence of "blockchain constitutionalism"[408] —the recognition that blockchain systems can be understood as constitutional orders, operating under a dual constitution:

- *formal* constitution: the on-chain rules encoded in protocols and smart contracts, and a
- *material* constitution: the off-chain social norms, values, and shared principles of the community.

405 Michael Abramowicz, *The Very Brief History of Decentralized Blockchain Governance*, 22 Vanderbilt J. Ent. & Tech. L. 273, 275-76 (2020), https://scholarship.law.vanderbilt.edu/jetlaw/vol22/iss2/2/; Benito Arruñada & Luis Garicano, *Blockchain: The Birth of Decentralized Governance* 31-33 (Pompeu Fabra Univ., Econ. & Bus. Working Paper No. 1608), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3160070.

406 Primavera De Filippi, Sofia Cossar, Morshed Mannan, Kelsie Nabben, Tara Merk & Jamilya Kamalova, *Report on Blockchain Governance Dynamics*, Project Liberty & BlockchainGov 46 (May 2024), https://ssrn.com/abstract=5112585. *See also:* De Filippi, Reijers & Mannan, Blockchain Governance, *supra* note 394, at 161-166; Eric Alston, Wilson Law, Ilia Murtazashvili & Martin Weiss, *Blockchain Networks as Constitutional and Competitive Polycentric Orders*, 18 J. Institutional Econ. 707 (2022), https://ideas.repec.org/a/cup/jinsec/v18y2022i5p707-723_1.html.

407 De Filippi et al. *Report on Blockchain Governance Dynamics, supra* note 406 at 46.

408 Morshed Mannan, Primavera De Filippi & Wessel Reijers, *The Emergence of Blockchain Constitutionalism*, *in* The Oxford Handbook of Digital Constitutionalism, 5-7 (Giovanni De Gregorio, Oreste Pollicino & Peggy Valcke eds., 2024). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5071985 [hereinafter *The Emergence of Blockchain Constitutionalism*].

The 2016 DAO attack *(See above Figure 11)* exemplified this duality. While the attacker's actions were technically valid under Ethereum's protocol rules, the community deemed them illegitimate. The resulting hard fork —reversing the attacker's actions despite "code is law" principles— demonstrated how social consensus can override technical rules.

Legal theorist H.L.A. Hart's distinction between *primary rules* (which govern conduct) and *secondary rules (*which govern how rules are made: "rules about making rules") is useful in understanding blockchain governance.[409] As legal scholar Eric Alston has argued,[410] in the context of blockchain systems:

- Secondary rules (at the constitutional level) include consensus algorithms, transaction validity criteria, and on-chain or off-chain mechanisms for protocol upgrades (i.e., forks),[411]
- Primary rules (at the operational level) include specific transactions and state changes recorded according to the blockchain protocol.

Governance operates at both levels. While most governance decisions are aimed at modifying primary rules (e.g. transaction fees, gas costs, etc.), the most significant changes alter secondary rules (e.g. improvement proposals altering the governance framework itself). In Ethereum, for instance, changes to the protocol are proposed through the Ethereum Improvement Proposal (EIP) process. This process is defined in EIP-1, the foundational Ethereum Improvement Proposal that establishes the structure, format requirements, and processing guidelines for all subsequent EIPs.[412] EIP-1 sets out the procedure for proposing and implementing changes to the Ethereum protocol, including the standardized format for proposals, the various lifecycle statuses, and the respective responsibilities of authors and editors. [413]

Understanding blockchain governance requires recognizing blockchains as "polycentric" systems, with multiple autonomous decision-making centers operating under a common set of rules.[414] Different actors dominate different decisions:

- Protocol developers shape technical architecture
- Node operators enforce consensus rules
- Token holders influence economic parameters
- Users and applications drive adoption pressures
- Miners/validators secure and maintain the network

Power distribution varies by governance domain, blockchain design, and community culture. A protocol change on Bitcoin, for example, might require implementation by the core developers, adoption by miners, and acceptance by users and large commercial operators (e.g. cryptocurrency exchanges or custodian wallets). Each actor preserves the ability to refuse a change, even if it is accepted by others. This complex interplay of stakeholders, rather than any single decision maker, determines how blockchain systems evolve.[415]

409 H.L.A. Hart, THE CONCEPT OF LAW 77–96 (2nd ed. 1994).

410 *See* Eric Alston, *Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets*, 11 Case W. Res. J.L. Tech. & Internet 131, 135 (2020). https://scholarlycommons.law.case.edu/jolti/vol11/iss1/6.

411 *Id*.

412 EIP-1 was authored by Martin Becze and Hudson Jameson and was based on Bitcoin's BIP-1 (Bitcoin Improvement Proposal 1). Martin Becze & Hudson Jameson, *EIP-1: EIP Purpose and Guidelines*, Ethereum Improvement Proposals (Oct. 27, 2015), https://eips.ethereum.org/EIPS/eip-1.

413 Ethereum, *EIP-1*, GitHub, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md (last visited Jan. 15, 2026).

414 De Filippi, Reijers & Mannan, Blockchain Governance, *supra* note 394, at 16; Primavera de Filippi, Morshed Mannan, Sofia Cossar, Jamilya Kamalova, Tara Merk, *Blockchain Technology and Polycentric Governance*, 19-25 (2024), https://ssrn.com/abstract=5029034.

415 De Filippi, Reijers & Mannan, Blockchain Governance, *supra* note 394, at 148.

These elements undergo continuous modification to enhance performance, address security vulnerabilities, and improve overall network efficiency. As such, blockchain governance must be understood as a dynamic and collective process, rather than a set of fixed technical procedures. Thus, there is no simple answer to the question, "Who makes governance decisions?" Power in blockchain systems is contested, contextual, and constantly negotiated among stakeholders with different capabilities, incentives, and influence. Understanding this complexity is essential for analyzing how these systems function, versus how they aspire to operate.

FIGURE 23.

Protocol change terminology

While there are some general conventions, there is no concrete rule that all blockchains follow in how changes are proposed, vetted, and accepted. The terminology can be somewhat confusing.

- **"PR" stands for "pull request."** This term comes from the world of Git, a version control system used in the software world; but, it has been generalized somewhat to mean a proposal to change a codebase. For example, in open-source development, an independent developer may write a new feature but not have permission to directly integrate this code, so they will open a PR (on Github or similar). Even if the developer does have the authority to directly change the codebase, a PR is still good practice as it allows others to review and test the code before it gets implemented.
- Many blockchains have **formal improvement proposals**: Bitcoin has Bitcoin Improvement Proposals (BIPs), Ethereum has Ethereum Improvement Proposals (EIPs), Cardano has CIPs, etc.
- Other chains use other language that implies something similar: NEAR uses Near Enhancement Proposals (NEPs), Polkadot uses Requests for Comment (RFCs), Cosmos uses Architecture Decision Records (ADRs).[416]

416 Notably, protocol-specific improvement proposals and other types of proposals are not always mutually exclusive. Ethereum, for example, makes heavy use of EIPs, but also has Ethereum Requests for Comment (ERCs), some of which have been standardized into protocols (such as ERC-20 tokens). *Ethereum Improvement Proposals (EIPs)*, Ethereum.org, https://ethereum.org/en/eips/ (last updated Oct. 2, 2025)

3.2. ON-CHAIN VS OFF-CHAIN GOVERNANCE

How blockchain systems make decisions depends on where authority is encoded and exercised. Some governance mechanisms are embedded directly into the blockchain's code —through smart contracts that automatically execute decisions, decentralized autonomous organizations (DAOs) that enable token-based voting, or protocols that adjust parameters based on predefined rules. Others rely on traditional coordination outside of the blockchain —in developer debates on GitHub, foundation board meetings, or community discussions on forums and social media.

This distinction between on-chain governance (rules executed through code) and off-chain governance (decisions made through social processes) shapes how power flows through blockchain systems.[417] On-chain mechanisms promise transparency and automation: Every decision is visible, verifiable, and enforced by the protocol itself. Off-chain processes offer flexibility and nuance: Complex issues can be debated, edge cases considered, and human judgment applied.

The choice between on-chain and off-chain governance involves significant trade-offs. On-chain governance offers transparency and automation but can be rigid and susceptible to plutocracy, where influence is concentrated among wealthy token holders.[418] Off-chain governance, reliant on social consensus and informal processes, provides flexibility and can be more participatory but often lacks transparency and can obscure the true distribution of power.[419] Most blockchains employ both, creating hybrid systems where code and community interact in complex ways.

Understanding this duality is crucial because it reveals how blockchain governance actually works, versus how it is often portrayed. While advocates may emphasize trustless, automated decision making, the reality is that even the most sophisticated on-chain systems depend on off-chain coordination. And supposedly "ungoverned" protocols often concentrate significant power in informal structures. The following sections examine how these parallel governance tracks operate, intersect, and sometimes conflict.

3.2.1. Off-Chain Governance

Despite blockchain's automation aspirations, most governance decisions still happen the old-fashioned way: through human coordination outside the protocol itself. Some governance decisions are deliberately kept off-chain —for example, protocol updates— while others are simply unsuitable for on-chain mechanisms, such as reaching consensus on community leadership.

3.2.1.A. Off-Chain Governance Actors

The governance of blockchain systems, despite being operated through code, relies heavily on human actors and institutions operating outside the blockchain itself. These off-chain actors —ranging from legal entities and core developers to market participants and regulators— wield significant influence over protocol evolution through informal coordination, resource control, social consensus, and external pressures. Understanding who these actors are and how they exercise power within a blockchain network illustrates how even the most decentralized systems ultimately depend on traditional forms of human organization and power dynamics.

417 Laatikainen et al., *supra* note 400; *see also* Wessel Reijers, Iris Wuisman, Morshed Mannan et al., *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, 40 Topoi 821 (2021), https://doi-org.stanford.idm.oclc.org/10.1007/s11245-018-9626-5;

418 De Filippi et al., *Report on Blockchain Governance Dynamics*, *supra* note 406, at 35-36.

419 *Id*. at 36.

1. Legal Entities

While Bitcoin operates without any formal organizational structure, virtually every other major blockchain has established legal entities (typically non-profit foundations or corporations) to manage operational aspects that code cannot address.[420] These organizations, often registered in crypto-friendly jurisdictions, such as Switzerland or Singapore, serve multiple functions: They manage treasury funds, coordinate development efforts, interface with regulators, hire core developers, fund ecosystem growth, and provide legal protection for contributors.

They also wield considerable influence through their resources and institutional positions. Most hold significant token reserves from initial distributions. They control development funding and research, and they shape strategic direction through grant programs and research initiatives. Yet, their power remains contested and limited. They cannot unilaterally impose protocol changes on a decentralized network, and their decisions may face community pushback if not aligned with community values. This creates an ongoing tension: Blockchain systems need these organizations to function in the traditional world, yet their very existence challenges narratives of pure decentralization.

Foundations are an attempt at accommodating this tension: maintaining decentralized networks while navigating a world that demands legal entities, bank accounts, and responsible parties. These organizations are typically created during a network's launch and, consequently, wield significant influence early on through their token reserves, funding control, and strategic positioning.[421] For instance, the Avalanche, Cardano, Filecoin, Optimism, Polygon, Tezos, and Zcash foundations play crucial roles in funding research, managing community treasuries, and guiding ecosystem development.[422]

The critical question is whether this influence diminishes over time. Some foundations pursue "progressive decentralization"[423] —gradually ceding control as the network matures, distributing tokens, and transitioning decision making to the community. Others retain substantial token holdings and seek to retain their governance powers indefinitely ("persistent centralization").[424] The actual distribution of tokens over time ultimately determines whether a blockchain achieves genuine decentralization or merely pretends to be decentralized while maintaining a significant degree of political centralization.

Real-world examples illustrate this spectrum. The Ethereum Foundation has progressively reduced its influence, focusing on research and development while avoiding direct protocol control.[425] In contrast, other foundations maintain stronger oversight through ongoing funding decisions and strategic initiatives. The Tezos saga exemplifies the risks: A bitter legal battle between founders and foundation nearly derailed the project, highlighting how traditional power struggles can infect supposedly decentralized systems.[426]

Some networks attempt novel solutions to this tension. Zcash splits authority between two entities —the Electric Coin Company and the Zcash Foundation— bound by a

420 *Id*. at 11, 20.

421 *Id*. at 21-22.

422 *Id*. at 20.

423 *Id*. at 21.

424 *See, e.g.*, Halaburda, *supra* note 399.

425 *See* Siamak Asnavi, *Ethereum Foundation Starts New AI Team to Support Agentic Payments*, CoinDesk (Sept. 15, 2025), https://www.coindesk.com/tech/2025/09/15/ethereum-foundation-launches-ai-team-to-support-agentic-payments.

426 After a record-breaking $232 million ICO, Tezos's founders Arthur and Kathleen Breitman and Tezos Foundation president Johann Gevers engaged in a legal battle over control of funds and governance. *From a $232m ICO to Lawsuits – The Tezos Story*, CoinBureau (Mar. 29, 2023), https://coinbureau.com/ico/256m-ico-lawsuits-tezos-story/.

trademark agreement that requires mutual consent for major changes.[427] This creates checks and balances but also poses potential for deadlocks. Similarly, the blockchain Optimism experiments with bicameral governance, balancing the voting power of all token holders against a limited number of members that form a "Citizens' House," initially selected by the foundation.[428]

These varied approaches reveal an uncomfortable truth: Most "decentralized" networks depend on centralized entities that control resources, coordinate development, and interface with the traditional world. While foundations may be intended to lose relevance once the network matures, their embedded advantages —in terms of funding, expertise, and relationships— often perpetuate their influence long after networks supposedly mature.

2. Core developers or maintainers

While foundations provide institutional structure, the actual power to change blockchain protocols often rests with a small group of core developers who maintain the codebase. These individuals —typically fewer than a dozen for major blockchains— wield extraordinary influence not only because of their technical expertise but also because they hold exclusive control over the official code repository of their respective blockchain projects.

Core developers occupy a unique position in blockchain governance because they translate community discussions into code, decide which proposals merit implementation, and ultimately determine what changes make it into production. Their power is both technical and social: They write the code that thousands of nodes run, but they also shape narratives about what changes are "technically feasible" or "philosophically aligned" with the protocol.[429]

Bitcoin clearly exemplifies this dynamic. While anyone can propose changes through Bitcoin Improvement Proposals (BIPs), a small group of maintainers controls what gets merged into the reference implementation.[430] These maintainers insist they merely implement community consensus, yet their interpretation of that consensus —and their ability to delay, modify, or reject proposals— grants them effective veto power over protocol evolution.[431] The 2015-2017 block size debate demonstrated this influence: Despite significant miner and business support for larger blocks, core developers' opposition effectively killed the proposal.[432]

Other blockchains attempt different models. Ethereum does not have a rigid maintainer hierarchy like Bitcoin. Ethereum's "core devs" are a diverse group of engineers and developers who are recognized for their sustained, high-quality contributions to Ethereum's protocol or codebase and are invited to participate in regular "All Core Devs calls."[433] Some newer protocols rotate developer responsibilities or require multiple signatures for code commits (recorded changes to the source code). Yet across all models, technical expertise creates natural

427 De Filippi et al., *Report on Blockchain Governance Dynamics*, *supra* note 406, at 21.

428 *Welcome to the Optimism Collective*, Optimism, https://community.optimism.io/welcome/welcome-overview (last visited Jan. 15, 2026); *Citizens' House Overview*, Optimism, https://community.optimism.io/citizens-house/citizen-house-overview (last visited Jan. 15, 2026).

429 *See* Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, *in* Regulating Blockchain: Techno-Social and Legal Challenges 61-77 (Philipp Hacker et al. eds., 2019), https://ssrn.com/abstract=3203198

430 Kevin Werbach et al., *Blockchain Governance in the Wild*, 3 Cryptoecon. Sys. (Apr. 22, 2024), https://cryptoeconomicsystems.pubpub.org/pub/blockchain-governance-wild/release/1.

431 *See* Primavera De Filippi & Xavier Lavayssière, *Blockchain Technology: Toward a Decentralized Governance of Digital Platforms?*, *in* The Great Awakening 185, 187 (Anna Great & David Bollier eds., 2020), https://ssrn.com/abstract=3760483.

432 Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*, 5 Internet Pol'y Rev. (Sept. 30, 2016), https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure.

433 Paul Dylan-Ennis, Donncha Kavanagh & Luis Araujo, *The Dynamic Imaginaries of the Ethereum Project*, 52 Econ. & Soc'y 87, 87–109 (2023), https://doi.org/10.1080/03085147.2022.2131280.

centralization —few people possess the skills and context to meaningfully contribute to protocol development.[434]

This poses important questions for blockchain governance, as core developers and maintainers often form tight-knit communities with shared philosophies, potentially creating echo chambers resistant to outside perspectives. Core developers are also criticized for leveraging their influence to resist changes that would diminish their influence, framing opposition in technical rather than political terms and relying on the claim of "rough consensus" to implement changes that often reflect their own interpretations, rather than genuine community will.[435]

The irreplaceable nature of experienced protocol developers further entrenches their power. When disagreements arise, the threat of key developers leaving can override other governance mechanisms —as seen when contentious decisions have been reversed after developers threatened to exit. For instance, the Programmatic Proof-of-Work (ProgPow) controversy in the Ethereum community saw core developers initially approve a mining algorithm change, only to indefinitely postpone it after key stakeholders in the blockchain threatened to leave if it was implemented, citing inadequate community consensus despite prior technical approval.[436] This reveals how human relationships and dependencies play an important governance role, even in supposedly trustless systems.

3. Market Forces and External Pressures

While on-chain governance focuses on protocol rules, the ultimate power in blockchain systems often lies with actors who never touch the code: exchanges, users, and regulators who determine which chains have value and which have not.

Cryptocurrency exchanges wield perhaps the most immediate influence. When contentious forks occur, exchanges decide which chain receives the original ticker symbol, where liquidity flows, and, ultimately, which version survives. During the 2017 fork of Bitcoin Cash (BCH), exchanges like Coinbase initially refused to support BCH, effectively constraining its adoption.[437] Conversely, when major exchanges threatened to label any SegWit2x fork as "B2X" rather than "BTC," the proposal lost critical momentum.[438] These listing decisions —made by centralized entities— can override years of technical development and community debate.

Economic stakeholders create additional pressure points. Custodial wallets, payment processors, and major merchants shape governance by choosing which upgrades to support. When BitPay advocated for larger Bitcoin blocks, its merchant network created real pressure for scaling solutions.[439] Similarly, when Tesla announced Bitcoin acceptance (then reversal), it influenced development priorities around energy efficiency.[440] These actors lack formal governance power yet exercise effective vetoes through their economic weight.

---

434 Werbach et al., *supra* note 430.

435 Some scholars describe the influence of core developers on the Bitcoin blockchain as a form of "developer oligarchy." Balázs Bodó & Alexandra Giannopoulou, *The Logics of Technology Decentralization – the Case of Distributed Ledger Technologies*, *in* Blockchain and Web 3.0: Social, Economic, and Technological Challenges 114, 121 (Massimo Ragnedda & Giuseppe Destefanis eds., 2019), https://ssrn.com/abstract=3330590. *See also* Angela Walch, *Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems*, *in* Crypto-assets: Legal, Regulatory, and Monetary Perspectives 39, 58-61 (Christ Brummer ed., 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244.

436 Hudson Jameson, *ProgPoW: The Ethereum Community Speaks*, Hudson James Blog (Mar. 2, 2020), https://hudsonjameson.com/posts/2020-03-02-progpow-the-ethereum-community-speaks/. *See also* Turner Wright, *Ethereum Community Comes out Against Controversial ProgPOW*, CoinTelegraph (Feb. 26, 2020), https://cointelegraph.com/news/ethereum-community-comes-out-against-controversial-progpow.

437 Eric D. Chason, *A Tax on the Clones: The Strange Case of Bitcoin Cash*, 39 Va. Tax Rev. 1 (2019), https://ssrn.com/abstract=3475368.

438 *To B2X or Not to B2X: How Exchanges Will List the SegWit2x Coin*, NASDAQ (Oct. 28, 2017), https://www.nasdaq.com/articles/to-b2x-or-not-to-b2x-how-exchanges-will-list-the-segwit2x-coin-2017-10-28.

439 De Filippi & Loveluck, *supra* note 432.

440 Lauren Packard, Ariana K. Singh & Olamide Oguntoye, *Crypto Has an Emissions Challenge: Here's What Leaders Can Do About It*, 1 Future Tech. 6, 6–13 (2022), https://doi.org/10.55670/fpll.futech.1.3.3.

Users themselves, though often dismissed as passive participants, collectively determine a blockchain's fate through their choices. The Ethereum/Ethereum Classic split demonstrated this power: Despite Ethereum Foundation support for the fork, a significant user contingent maintained the original chain, creating medium-term fragmentation.[441] Users, thus, have the power to render technical changes meaningless if the community refuses adoption.

Regulatory authorities add another layer of indirect influence. While regulators cannot alter blockchain code, they profoundly shape governance by constraining off-chain actors. When China banned mining *(See below section 7.4.1.)*, Bitcoin's hash rate redistributed globally, altering the geographic balance of network control.[442] When the SEC targeted the public issuance of blockchain tokens *(See below section 7.2.2.A.)*, priorities shifted toward ensuring that blockchain platforms are "sufficiently decentralized" to avoid qualification as securities.[443] The mere threat of regulatory action can influence the design of blockchain governance, as illustrated by Zcash, which made its privacy features optional rather than mandatory, partly to avoid regulatory backlash.[444]

This web of influences reveals a paradox: Blockchains designed to operate independently of traditional power structures remain deeply embedded within them. Technical consensus means little without exchange support, user adoption, and regulatory acceptance. Off-chain governance, thus, extends far beyond developer forums and foundation meetings to encompass market dynamics and state power —external forces that no amount of decentralization can fully escape.

3.2.1.B. Case Studies

While blockchain governance cannot be exhaustively described, the following case studies illuminate how specific networks handle decision making. They capture only snapshots of systems which are constantly evolving. Governance processes that appear formal and structured on paper often dissolve into ad hoc negotiations during crises. What projects describe in white papers rarely matches what happens in developer chat rooms, board meetings, or emergency forks.

Documenting these governance realities presents additional challenges. Many critical decisions occur in private conversations, undocumented meetings, or informal agreements between key stakeholders. Projects have incentives to overstate their decentralization while obscuring where power actually concentrates. Even well-intentioned efforts at transparency —governance forums, recorded calls, public proposals— reveal only the final performance of consensus, not the backroom dealings that shaped it.

The following analysis draws from the available literature and empirical studies that gathered data directly from teams, supplemented by public documentation and observable on-chain actions.[445] These cases reveal a consistent pattern: Virtually all blockchain governance blends elements of traditional corporate control, informal social consensus, and automated protocols in ways that defy both the pure decentralization narrative and simple centralization critiques. Understanding these hybrid realities —rather than the idealized models— is essential for grasping how blockchain governance actually functions.

441 Stijn Van Hijfte, Blockchain Platforms: A Look at the Underbelly of Distributed Platforms 147-89 (2022), https://catalog.library.vanderbilt.edu/permalink/01VAN_INST/16p9s3g/alma991043727851903276.

442 Nattanon Tovanich, Nicolas Soulié, Nicolas Heulot & Petra Isenberg, *The Evolution of Mining Pools and Miners' Behaviors in the Bitcoin Blockchain*, 19 IEEE Transactions on Network & Serv. Mgmt. 3633, 3633–44 (2022), https://doi.org/10.1109/TNSM.2022.3159004.

443 Jin J. Park & Hyung H. Park, *Regulation by Selective Enforcement: The SEC and Initial Coin Offerings*, 61 Wash. U. J.L. & Pol'y 99, 117, 124 (2020), https://ssrn.com/abstract=3478661.

444 *See* Alex Gladstein, *Financial Freedom and Privacy in the Post-Cash World*, 41 CATO J. 271, 287-88 (2021), https://www.cato.org/sites/cato.org/files/2021-05/cj-v41n2-7.pdf.

445 De Filippi et al., *Report on Blockchain Governance Dynamics*, *supra* note 406; Werbach et al., *supra* note 430. *See also*: Liu, Yue, Qinghua Lu, Hye-young Paik and Liming Zhu. "Defining Blockchain Governance Principles: A Comprehensive Framework." *Inf. Syst.* 109 (2021): 102090, https://arxiv.org/abs/2110.13374.

1. Bitcoin

Bitcoin's governance illustrates how "decentralized" systems, despite their ethos of distributed governance, often rely on centralized platforms. The development of Bitcoin protocol centers on a single GitHub repository (i.e. a resource for managing and sharing software code operated by Microsoft). This repository acts as the "primary codebase"[446] for the reference implementation that over 80% of Bitcoin nodes run. The process appears open and meritocratic. Anyone can propose changes through Bitcoin Improvement Proposals (BIPs) or GitHub pull requests.[447] These proposals trigger public debates across GitHub comments, Reddit forums, Internet Relay Chat (IRC) channels, and mailing lists. Proposed code undergoes extensive review, testing, and modification through community feedback. In theory, this represents a good example of consensus-based governance.

In practice, however, power concentrates dramatically. While anyone can comment or propose a change (an upgrade, a bug fix, refactored code, etc.), only a handful of maintainers (ranging between three to seven at any given time) can merge code into Bitcoin Core for these changes to be incorporated into the canonical version of the protocol.[448] This arrangement provides a measure of oversight and stability but also introduces a potential point of tension as the official maintainers effectively gatekeep all protocol changes. During Bitcoin's scaling debates, for instance, maintainers' philosophical opposition to block-size increases effectively vetoed proposals that had substantial miner and business support.[449]

Bitcoin's governance model faces several persistent criticisms. The most fundamental critique is that the current structure is *overly* centralized:[450] A system designed to eliminate trusted intermediaries concentrates protocol development in the hands of five to seven maintainers. This reveals a dilemma: While such concentration seems to contradict Bitcoin's ethos, it might be a necessary tradeoff for Bitcoin to function effectively. Whether or not the current "maintainer" architecture is acceptable is an individual decision and, luckily, Bitcoin arguably caters equally to both sides of the debate. For those who see five to seven maintainers as a valid tradeoff, the infrastructure to support this system already exists.

Beyond the maintainer bottleneck, Bitcoin's governance-by-GitHub creates additional dependencies that further compromise decentralization. Bitcoin's development process is vulnerable to GitHub's policies, platform changes, or potential censorship. The community's discussions are scattered across corporate platforms — Reddit, Twitter, Telegram— each with its own moderation policies and points of failure.

For those who view these tradeoffs as acceptable, the current infrastructure provides a functioning, if imperfect, governance system. For those who would prefer a different setup, Bitcoin's open-source nature introduces a structural check on centralization: the possibility of forking. Anyone who disagrees with Bitcoin Core's direction can freely download the software, synchronize with the network, and create a fork —effectively launching a new version of Bitcoin with different governance

446 "Primary codebase" is possibly a sticky term. In any event, at the moment, there appears to be strong social consensus around the code at https://github.com/bitcoin/bitcoin.

447 For example, the current list of open pull requests can be found here: https://github.com/bitcoin/bitcoin/pulls. Anyone is free to read the debate and jump in.

448 The group of maintainers is composed of developers who have been invited to the maintainer role by current maintainers due to a track record of demonstrated sustained, high-quality contributions to Bitcoin. Each maintainer has been entrusted by the community to uphold the values and standards of Bitcoin. The Bitcoin maintainers are ultimately charged with making the best decision possible regarding new code changes, ideally considering factors such as the purpose of the change, the technical strength of the submission, community sentiment, and the somewhat nebulous ideology behind Bitcoin. Based on this consensus, they either reject the pull request or approve it by changing the code.

449 De Filippi & Loveluck, *supra* note 432.

450 *See, e.g.*, De Filippi & Loveluck, *supra* note 432; Jack Parkin, *The Senatorial Governance of Bitcoin: Making (De)centralized Money*, 48 Econ. & Soc'y 463 (2019), https://www.researchgate.net/publication/337586730_The_senatorial_governance_of_Bitcoin_making_decentralized_money.

principles. While such forks rarely achieve significant adoption (Bitcoin Core retains dominant market position), the technical capacity to exit remains universally accessible. In this respect, Bitcoin's design treats forking not as failure but as a governance mechanism —a form of protest that underscores its foundational commitment to permissionless innovation and institutional contestability.

FIGURE 24.

The SegWit Saga

The Segregated Witness (SegWit) upgrade[451] exemplifies both the promise and the peril of Bitcoin's governance model. Proposed in 2015 to address Bitcoin's scalability limitations by separating signature data from transaction data, SegWit triggered a governance debate that nearly split the community permanently.[452]

Unfolding publicly across numerous decentralized channels (including Reddit,[453] GitHub, and IRC), the debate revealed how different stakeholder groups represent different vested interests. Core developers championed SegWit as an elegant technical solution. Some large mining pools resisted, concerned about fee revenue and preferring simpler block size increases. Businesses needing higher transaction throughput grew increasingly frustrated with the deadlock.

In 2017, a coalition of miners and exchanges spearheaded what became known as the New York Agreement (NYA) —an attempt at breaking the stalemate through industry-led coordination, negotiated largely outside the traditional open-source development process.[454] Major miners and exchanges met privately to forge a compromise: Activate SegWit immediately, then double the block size within six months (SegWit2x). This agreement, negotiated without core developers, demonstrated how independent actors can mobilize to exert influence within the ecosystem, attempting to override technical authority with economic power.

Yet the outcome revealed the limits of such power. Core developers rejected SegWit2x. In a context marked by strong user-led pressure and broader ecosystem resistance, the NYA coalition ultimately cancelled SegWit2x in November 2017, citing lack of consensus. SegWit activated through a user-led procedure (User-Activated Soft-Fork), while opponents forked to create Bitcoin Cash, permanently fragmenting the community.

The SegWit saga is a consequential example of the intertwined nature of protocol evolution and stakeholder governance in blockchain systems. Rather than reaching genuine consensus, the community split into two separate chains —Bitcoin with SegWit and Bitcoin Cash without it — each claiming to be the "true" Bitcoin. This pattern of governance-by-forking continues to define how blockchain systems "resolve" fundamental disagreements.

451 *What Is Segregated Witness (Segwit)*, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-is-segregated-witness-segwit (last visited Jan. 15, 2026).

452 *See* Alastair Berg, Chris Berg & Mikayla Novak, Crypto Public Choice 7 (Aug. 30, 2018), https://ssrn.com/abstract=3236025.

453 With subreddit r/bitcoin generally supporting SegWit and r/btc emerging in response to perceived censorship on r/bitcoin. r/btc was established in direct response to concerns that the moderators of r/bitcoin were unduly biased in favor of Core developers.

454 Aaron Van Wirdum, *Bitcoin Miners Are Signaling Support for the New York Agreement: Here's What that Means*, Bitcoin Mag. (June 20, 2017), https://bitcoinmagazine.com/technical/miners-are-signaling-support-new-york-agreement-heres-what-means; *SegWit2x*, Bitcoin Wikipedia, https://en.bitcoin.it/wiki/SegWit2x (last visited Jan. 15, 2026); Patrick Thompson, *2x or No 2x, that Was the Question*, Cointelegraph (Nov. 13, 2017), https://cointelegraph.com/news/2x-or-no-2x-that-was-the-question.

2. Ethereum

Similar to Bitcoin, Ethereum's governance is decentralized and informal. Ethereum's founder, Vitalik Buterin, has advocated for a pragmatic approach to blockchain governance that integrates both formal mechanisms and informal community processes.[455] Ethereum's governance structure attempts to embody these principles, seeking to balance the technical expertise of core developers with the broader community's perspectives —though, in practice, technical voices often dominate the debate.

Ethereum's key governance processes include:

- Ethereum Improvement Proposals (EIPs), which serve as formal design documents specifying proposed changes to the protocol;
- All Core Developer calls, where developers from various client teams discuss technical changes and coordinate upgrades; and,
- Community consensus mechanisms, as major protocol changes theoretically require widespread agreement among validators, node operators, and (prior to the Merge in 2022) miners.[456]

Ethereum Improvement Proposals (EIPs) go through a predominantly off-chain governance process that combines formal documentation with informal, consensus-oriented deliberation. Any individual may propose an EIP by submitting a pull request to the public GitHub repository and suggesting changes, ranging from minor technical improvements to fundamental protocol modifications. Various people and groups discuss the submitted proposals across various venues —technical debates on GitHub, higher-level deliberation on the Ethereum Magicians forum, implementation-focused exchanges in client-specific channels and community calls, and broader community sentiment expressed on social media. Progression depends not only on technical merit but also on the ability to attract support from core development teams responsible for implementation.

Once tentative agreement is reached, a proposal enters a "Last Call" phase allowing final community input, though this stage rarely alters outcomes for proposals that have already secured core developer support. Absent unresolved objections, an EIP may advance to "Final" status, which indicates specification maturity rather than guaranteed deployment. Implementation ultimately reveals where decision-making authority resides. Core developers from major client teams —such as Geth, Nethermind, and Erigon— must independently implement the agreed changes in their software clients,[457] with discrepancies resolved through testing and coordination on dedicated test networks. Developers then jointly schedule network activation, typically by block number or timestamp, several months in advance. The upgrade takes effect only if a critical mass of validators chooses to adopt the updated software.[458]

Since 2020, the processes have become increasingly formalized and structured,[459] particularly after transitioning to proof of stake (On the Merge, *see above section 2.3.2.B.*). This formalization is evident in Ethereum's systematic approach to protocol upgrades through hard forks. Unlike Bitcoin's contentious and rare hard forks, Ethereum has normalized regular network upgrades:

455 *See* Vitalik Buterin, *Moving Beyond Coin Voting Governance*, Vitalik Buterin's Website (Aug. 16, 2021), https://vitalik.eth.limo/general/2021/08/16/voting3.html; Vitalik Buterin, *Governance, Part 2: Plutocracy Is Still Bad*, Vitalik Buterin's Website (Mar. 28, 2018), https://vitalik.eth.limo/general/2018/03/28/plutocracy.html; Vitalik Buterin, *Notes on Blockchain Governance*, Vitalik Buterin's Website (Dec. 17, 2017), https://vitalik.eth.limo/general/2017/12/17/voting.html; Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (2014), https://ethereum.org/en/whitepaper/.

456 After the Merge in September 2022, Ethereum moved to proof-of-stake, and miners were replaced by validators who must stake 32 ETH to participate in consensus.

457 *Nodes and clients*, ETHEREUM.ORG (last updated Feb. 14, 2025), https://ethereum.org/en/developers/docs/nodes-and-clients/.

458 "How Does Governance Work in Ethereum?," BITCOIN.COM, https://www.bitcoin.com/get-started/how-does-governance-work-in-ethereum/ (last accessed August 22, 2025).

459 *See Introduction to Ethereum Improvement Proposals (EIPs)*, Ethereum Found., https://ethereum.org/eips/ (last visited Jan. 15, 2026).

- London (August 2021),[460] which introduced EIP-1559's fee-burning mechanism, whereby the base transaction fee is burned rather than paid to validators, reducing net ETH issuance;[461]
- the Merge (September 2022),[462] which enabled a shift from proof of work to proof of stake;
- Shanghai (March 2023),[463] enabling staked ETH withdrawals;
- Cancun-Deneb (March 2024), for scaling improvements;[464]
- Pectra (May 2025), raised validator staking limit to 2,048 ETH, enabled wallets to act like smart contracts, and increased data capacity for layer-2s; and
- Fusaka (planned December 2025 / in progress as of publication),[465] which improves data handling and sets new gas limit parameters.

Each follows increasingly standardized processes —from initial EIP discussions through testnet deployments to coordinate mainnet activation— with defined roles for researchers, client developers, and infrastructure providers. The All Core Devs calls shifted from irregular gatherings to scheduled bi-weekly meetings with recorded minutes, formal agendas, and structured decision frameworks. Thus, what began as ad hoc coordination has evolved into regular meetings, defined procedures, and established hierarchies.

Within this structure, the Ethereum Foundation plays an important but strategically understated role.[466] While it officially avoids imposing decisions, the Foundation shapes the ecosystem through strategic funding allocation and coordination efforts. It facilitates collaboration among client teams, funds critical research on scaling and security, and orchestrates the transition to proof of stake (completed with the Merge). The Foundation provides multi-million-dollar grants every year to developers, researchers, and projects that contribute to Ethereum's infrastructure.[467] It also organizes and supports influential events, such as Devcon and ETHGlobal; maintains essential documentation at ethereum.org; and supports educational initiatives through its Ecosystem Support Program to expand the developer community and encourage Ethereum adoption.[468] Thus, although positioned as merely a "support organization," the Ethereum Foundation's control over resources, information flow, and coordination mechanisms gives it substantial indirect influence over Ethereum's trajectory.

Ethereum makes extensive use of GitHub, both for pull requests and tracking Ethereum Improvement Proposals (EIPs) *(See Figure 23.)*. The EIP process has become one of the most influential standards for blockchain governance, with blockchains like Binance Smart Chain (BEPs), Polygon (PIPs), and numerous others directly copying the EIP framework within their own governance system.[469]

460 MacKenzie Sigalos, *Ethereum Just Activated a Major Change Called the 'London Hard Fork' — Here's Why It's a Big Deal*, CNBC (Aug. 5, 2021), https://www.cnbc.com/2021/08/05/ethereum-just-activated-its-london-hard-fork-and-its-a-big-deal.html.

461 Nathan Reiff, *What Does It Mean to Burn Crypto? Practical Applications*, INVESTOPEDIA (Feb. 12, 2025), https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/.

462 David Yaffe-Bellany, *Crypto's Long-Awaited 'Merge' Reaches the Finish Line*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/ethereum-merge-crypto.html.

463 Rahul Nambiampurath, *What Was the Ethereum Shanghai Upgrade*?, INVESTOPEDIA (May 27, 2024), https://www.investopedia.com/what-is-the-ethereum-shanghai-upgrade-7099021.

464*What is the Ethereum Cancun Upgrade?*, BINANCE (May 6, 2024) https://www.binance.com/en/academy/articles/what-is-the-ethereum-cancun-upgrade.

465*Fusaka*, ETHEREUM, https://ethereum.org/roadmap/fusaka/ (last visited Jan. 15, 2026).

466 *See, e.g.*, *What is the EF?*, ETHEREUM FOUND., https://ethereum.foundation/ef (last visited Jan. 15, 2026); Christine Kim, *The Ethereum Government*, GALAXY (June 3, 2024), https://www.galaxy.com/insights/research/ethereum-governance; *Our Story*, ETHEREUM FOUND., https://ethereum.foundation/ourstory (last visited Jan. 15, 2026).

467 Ezra Reguerra, *Ethereum Foundation Distributed $32.6M Grants to Ecosystem in Q1*, COINTELEGRAPH (May 9, 2025), https://cointelegraph.com/news/ethereum-foundation-spent-32-6-m-on-education-community-initiatives-in-q1.

468 *About the Ethereum Foundation*, ETHEREUM FOUND., https://ethereum.org/foundation (last visited Jan. 15, 2026); ETHGlobal, *ETHGlobal: Supporting Ethereum Hackathons Around the World*, MEDIUM (Feb. 14, 2018), https://ethglobal.medium.com/ethglobal-supporting-ethereum-hackathons-around-the-world-5e32fa991a55.

469 *See, e.g.*, *Polygon PIP: A Strong Mechanism for the Dev Community*, POLYGON GOVERNANCE HUB (Sept. 19, 2024), https://governance.polygon.technology/learn/the-101-guide-to-pips.

EIPs constitute the primary mechanism for proposing, deliberating, and implementing protocol changes, following a structured lifecycle from draft through review, last call, and final implementation.

The EIP process operates through "rough consensus" —a deliberately ambiguous standard that requires addressing significant technical objections and achieving broad (though not unanimous) support among key stakeholders.[470] Several actors contribute to this process: Proposal authors draft EIPs following the EIP-1 template; a small group of volunteer editors gatekeep submissions and enforce formatting standards; core developers from major clients[471] (with Geth historically occupying a dominant position)[472] evaluate technical merit and feasibility; and the broader community provides feedback through the Ethereum Magicians forum, Reddit, Twitter, and the official governance calls.

However, although the EIP framework is formally open and participatory, it functions as a *de facto* technocracy. Core developers, particularly those from major client implementations, wield disproportionate influence since their cooperation is necessary for network upgrades: Because major client teams must implement upgrades in a coordinated way, sustained disagreement among them can create a material risk of fragmentation or failed deployment. The power dynamics are ultimately asymmetric. While thousands may comment on proposals, fewer than 50 regular All Core Devs' participants shape critical decisions, and a dozen individuals have effective veto power over protocol changes.

The 2022 Merge *(See above section 2.3.2.B.)* exemplified this concentration of power. Despite being framed as a community consensus, the transition from proof of work to proof of stake was effectively decided by a coalition of core developers, the Ethereum Foundation, and major stakeholders who had been planning it since 2014. Miners, who were once essential security providers controlling billions in hardware, found themselves engineered out of the system with no meaningful recourse. Their objections were dismissed as economically motivated rather than legitimate governance participation. Similarly, because core developers deemed it technically superior, EIP-1559's fee burning mechanism, part of the London network upgrade for Ethereum, passed despite significant miner opposition, fundamentally altering Ethereum's economic model.[473] Technical expertise thus translates directly into governance power, creating (hidden) hierarchies within supposedly flat structures where "rough consensus" could be better described as "core developer consensus."

3. Other Blockchains

While Bitcoin and Ethereum dominate discussions of blockchain governance, examining other major blockchain networks reveals common patterns: initial centralization through foundations or corporations, promises of future decentralization that rarely materializes, and governance structures that mirror traditional organizations. The following cases illustrate how different projects navigate (or fail to navigate) the tension between operational necessities and decentralization ideals.

a. Solana

On the Solana blockchain, validator consensus theoretically serves as the primary governance

470 De Filippi et al., *Report on Blockchain Governance Dynamics*, *supra* note 406, at 51.

471 *Nodes and Clients*, ETHEREUM.ORG https://ethereum.org/en/developers/docs/nodes-and-clients/ (last visited Jan. 15, 2026).

472 *Client Diversity*, ETHEREUM.ORG, https://ethereum.org/en/developers/docs/nodes-and-clients/client-diversity (last visited Jan. 15, 2026).

473 Alex Thorn, *EIP-1559: A Major Upgrade for Ethereum*, GALAXY (Apr. 1, 2021), https://www.galaxy.com/insights/research/eip-1559-major-ethereum-upgrade. EIP-1559 introduced a new transaction pricing mechanism, where a base fee—the minimum amount that must be paid to put a transaction on the blockchain—is effectively destroyed or "burned" instead of going to blockchain participants who mine Ethereum coins or validate transactions. Because the fee increases depending on how busy the network is, it is possible under EIP-1559 for Ethereum to become deflationary when more coins are burned in fees than issued.

mechanism, though the reality is more centralized.[474] The Solana Foundation holds substantial SOL reserves from the initial token distribution; it actively shapes the ecosystem through strategic grants, partnerships decisions, and developer programs.[475] With Solana Labs still developing most core protocol updates and the Foundation funding critical infrastructure, governance on Solana remains highly informal and concentrated compared to some other networks. Major decisions emerge from private discussions among a small group of insiders rather than through a formal transparent process.

b. EOS

The EOS blockchain illustrates how supposedly decentralized systems can be captured by corporate interests. Block.one, the private company that developed the EOSIO software,[476] initially controlled the network through its exclusive development rights and substantial holdings of EOS tokens (worth billions at peak). This corporate dominance became a major point of frustration within the community, which saw Block.one as extracting value while neglecting protocol development. The establishment of the EOS Network Foundation (ENF) in 2021 can be regarded as a community revolt that effectively forked governance away from Block.one. However, the ENF simply replaced one centralized entity with another, coordinating development, funding, and strategic direction with limited community input.

c. EigenLayer

EigenLayer demonstrates how newer protocols attempt to address governance challenges through gradual decentralization. Currently, the protocol operates through upgradeable smart contracts on Ethereum,[477] controlled by a multisig wallet managed by Eigen Labs team members —a highly centralized setup. The Eigen Foundation promises to transfer control to the community eventually through "EigenGov," though specific timelines and mechanisms remain vague. This pattern of "progressive decentralization" —maintaining central control while promising future community governance— has become a standard practice for launching protocols.

d. Algorand and Avalanche

The Algorand and Avalanche foundations illustrate how blockchain governance often mirrors traditional corporate structures despite decentralization rhetoric. The Algorand Foundation maintains substantial influence over protocol upgrades, tokenomics decisions, and ecosystem funding, with founder Silvio Micali's vision dominating technical direction.[478] Similarly, the Avalanche Foundation, which holds a massive amount of AVAX tokens, shapes development priorities through funding decisions, while Ava Labs maintains considerable influence over protocol development.[479] Both foundations claim that efforts are underway to implement more decentralized governance mechanisms, though transfer of power to the community has been limited so far.

---

474 Lostin, *Solana Governance: A Comprehensive Analysis*, Helius (Mar. 26, 2025), https://www.helius.dev/blog/solana-governance--a-comprehensive-analysis.

475 *See generally The Solana Foundation*, Solana Found., https://solana.org/ (last visited Jan. 15, 2026); *Delegation Program*, Solana Found., https://solana.org/delegation-program (last visited Jan. 15, 2026); *About*, Solana Found., https://solana.org/about (last visited Jan. 15, 2026); Lostin, *supra* note 474.

476 *Block.one Will Take Part on EOS Governance and Voting*, EOS Go News (Oct. 26, 2019), https://www.eosgo.io/news/block-one-will-take-part-on-eos-governance/; Andrew Ware, *EOS (EOS): Strengths, Weaknesses, Risks*, CryptoEQ (Dec. 8, 2020), https://www.cryptoeq.io/corereports/eos-abridged; EOS Network Found., *The EOS Network Foundation Urges EOS Community to Reject Block.one Settlement*, EOS Network (July 6, 2023), https://eosnetwork.com/resources/opt-out-2/.

477 Eigen Found., *Overview*, Eigen Found., https://docs.eigenfoundation.org/ (last visited Jan. 15, 2026); Eigen Found., *Introducing EigenGov: Part 1*, Eigen Found. Blog (Nov. 26, 2024), https://blog.eigenfoundation.org/introducing-eigengov-part-1/; abbey, *Introducing the Protocol Council*, EigenLayer Forum (Dec. 4, 2024), https://forum.eigenlayer.xyz/t/introducing-the-protocol-council/14193.

478 Algorand Found., *Algorand Governor Guide*, Algorand, https://algorand.co/resources/governor-guide (last visited Jan. 15, 2026); Algorand Found., *Disclaimers*, Algorand, https://algorand.co/algorand-foundation/disclaimer (last visited Jan. 15, 2026).

479 Jesse Anglen, *Ultimate Guide to Avalanche: Ecosystem, Development, and Implementation*, Rapid Innovation, https://www.rapidinnovation.io/post/ultimate-guide-to-avalanche-ecosystem-development-and-implementation (last visited Jan. 15, 2026); Avalanche Found., *Avalanche Foundation*, Avalanche, https://www.avax.network/about/foundation (last visited Jan. 15, 2026).

3.2.2. On-Chain Governance

On-chain governance refers to the practice of embedding governance decisions directly within blockchain protocols, so that proposals, votes, and their implementation are executed through smart contracts and code rather than through off-chain social coordination. By embedding decision-making processes within protocols themselves, these systems promise to eliminate the informal power structures and backroom dealings that characterize off-chain governance. Yet the reality reveals new forms of plutocracy, technical barriers, and governance theater that often concentrate power more explicitly than traditional systems.

A benefit of on-chain governance is that the entire governance process is transparent, as all proposals, votes, and outcomes are recorded on the blockchain and visible to all. Yet, it has drawbacks. Wealthy actors can accumulate governance power through market purchases, potentially attacking protocols through "governance raids."[480] However, despite promises of global accessibility, on-chain governance erects significant technical barriers. Participants must understand proposal implications, possess sufficient tokens to meet voting thresholds, pay gas fees for participation, and navigate complex interfaces. As a result, many token holders do not participate in voting —the complexity and gas costs of voting often exceed potential benefits for holders of a small amount of tokens, leading to low participation rates that further concentrate power among "whales," (e.g. individuals or entities who hold a large amount of tokens).[481] While this phenomenon may appear problematic, higher participation is not necessarily desirable in all contexts, particularly where participants lack sufficient information or incentives to engage meaningfully in governance.

3.2.2.A. Mechanisms and Dynamics

On-chain governance systems implement decision making through smart contracts that automatically execute based on predefined rules. On-chain governance typically entails stakeholders submitting proposals via a smart contract, often requiring a minimum token deposit to prevent spam. This is followed by a voting period when token holders can signal support or opposition. Once voting concludes, proposals that meet predetermined thresholds are automatically implemented without human intervention. This automation promises to remove corruption and political maneuvering from governance.

The most sophisticated implementations of on-chain governance occur in the context of Decentralized Autonomous Organizations (DAOs) —i.e. organizational structures whose governance rules have been codified into smart contracts *(See Appendix 5.)*. In a DAO, stakeholders possess tokens that confer voting rights, enabling them to propose protocol changes, participate in decision making related to infrastructure, and allocate resources, all without recourse to a centralized authority. DAOs manage digital assets (e.g. cryptocurrency or tokens) through smart contracts that enforce voting outcomes, distribute funds, and sometimes even modify their own rules based on member decisions. Major protocols (like MakerDAO[482]) govern complex financial systems, while

480 The 2022 attempt to hijack Compound's governance by accumulating COMP tokens demonstrated this vulnerability. Samuel Haig, *Compound Community Accuses Notorious Whale of Engineering Governance Attack*, THE DEFIANT (July 29, 2024), https://thedefiant.io/news/defi/compound-community-accuses-notorious-whale-of-engineering-governance-attack.

481 Brett Hemenway Falk, Tasneem Pathan & Andrew Rigas, *Blockchain Governance: An Empirical Analysis of User Engagement on DAOs*, ARXIV (July 15, 2024), https://doi.org/10.48550/arXiv.2407.10945.

482 *See generally* Xiaotong Sun, Charalampos Stasinakis & Georgios Sermpinis, *Decentralization Illusion in Decentralized Finance: Evidence from Tokenized Voting in MakerDAO Polls*, 73 J. FIN. STABILITY 1 (2024), https://doi.org/10.1016/j.jfs.2024.101286.

investment DAOs (like The LAO) make venture capital decisions through on-chain mechanisms.[483]

1. Token-Weighted Voting

Token-weighted voting is one of the foundational governance mechanisms for on-chain systems, creating an explicit link between economic stake and political power.[484] Governance tokens grant voting rights to holders and may confer financial benefits, either through profit sharing or through appreciation in the token's market value.[485] This governance approach assumes that those with the greatest financial exposure to a protocol's success will make decisions in its best interest (because they have "skin in the game"). Depending on its implementation, this mechanism can produce different power dynamics that are more or less aligned with democratic principles and decentralization ideals. If community members are represented only by those who hold tokens, they may be *short-term* oriented and exclusively *profit*-oriented and not necessarily aligned with the project's stated mission.

a. Direct Token Governance

Direct token governance is the simplest implementation of token-weighted voting. Token holders vote directly on governance proposals, without intermediaries, and with influence proportional to the number of tokens they hold. Major protocols like Uniswap (UNI),[486] Aave (AAVE),[487] and Compound (COMP),[488] employ this model (where each token equals one vote), for protocol upgrades, parameter adjustments, and treasury allocations.

The actual degree of decentralization depends on multiple interrelated factors beyond the basic voting mechanism.[489] Token distribution patterns can significantly concentrate power, e.g. when protocols launch with 30-50% of tokens allocated to teams and investors. The scope of decisions that can be voted on also matters: Some protocols limit governance to minor parameter tweaks, while core development remains centralized.[490] Implementation details create another axis of decentralization: Proposals might trigger on-chain execution or merely signal preferences to multisig-controlled smart contracts.

The one-token, one-vote model embodies a form of plutocracy, assuming that wealth concentration produces optimal outcomes, as large token holders are the most aligned with the interests of the protocol. Yet, it disregards the risk that such an approach —without proper constitutional constraints— may undermine minority interests. If venture funds were to control a majority of tokens, they could potentially use that position to extract value through favorable market conditions, leaving smaller holders with limited recourse.

---

483 *Investments*, The LAO, https://docs.thelao.io/investments.html (last visited Jan. 15, 2026).

484 *See* Gerry Tsoukalas & Brett Hemenway Falk, *Token-Weighted Crowdsourcing*, 66 Mgmt. Sci. 3843, 3843-45 (2019), https://faculty.wharton.upenn.edu/wp-content/uploads/2018/06/token-weighted-crowdsourcing.pdf.

485 *See* Vitalik Buterin, *Moving Beyond Coin Voting Governance*, Vitalik Buterin's Website (Aug. 16, 2021), https://vitalik.eth.limo/general/2021/08/16/voting3.html (noting the claim on the profits is less direct as it only represents "some kind of economic interest in the protocol's revenue").

486 *Governance - Overview*, Uniswap Labs, https://docs.uniswap.org/concepts/governance/overview (last visited Jan. 15, 2026).

487 *Governance*, Aave, https://aave.com/docs/developers/governance (last visited Jan. 15, 2026).

488 *Compound Governance Explained: How COMP Token Voting Works*, Levex, https://levex.com/en/blog/compound-governance-comp-token-voting-explained (last visited Jan. 15, 2026).

489 Int'l Org. of Sec. Comm'ns, Policy Recommendations for Decentralized Finance (DeFi) 24, 76-78 (Sept. 2023) [hereinafter IOSCO Sept. 2023 Report], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

490 *Id.* at 78. Token-holder power often falls on a spectrum: Governance voting rights do not necessarily include authority for maintaining or updating the protocol or for managing other aspects of the project, such as determining access permissions. These may rest only with core developers. *Id.* at 70. In some models, votes are purely advisory. In other cases, votes may be more ratificatory in nature, formally approving actions already suggested or recommended by a project's stewards. *See, e.g.*, kyle, *Gitcoin DAO Governance Process v3*, Gitcoin (Apr. 2022), https://gov.gitcoin.co/t/gitcoin-dao-governance-process-v3/10358 (section "Voting").

FIGURE 25.

The problem of plutarchy

Evidence suggests that voting by tokens is extremely concentrated in just a few hands, with less than one percent of token holders controlling 90% of voting power in ten major DAOs.[491] This is the problem of "plutarchy," or rule by the wealthy.[492] In blockchain systems, this occurs when governance power becomes concentrated in the hands of individuals or entities —often referred to as "whales"— holding large quantities of tokens.[493]

In practice, whales have a disproportionate influence on the system[494] and may prioritize short-term increases in token value over the long-term sustainability and health of the broader ecosystem.[495] Moreover, they can make decisions with little or no consideration for the interests of minority participants or non-token stakeholders. This may raise concerns regarding the protection of minority interests and the distributional consequences of governance decisions, particularly in the absence of countervailing mechanisms.[496] Overall, a system based purely on majority voting lacks checks and balances, which operate to chasten power in political and corporate institutions.[497]

Blockchain protocols might thus attempt to mitigate the drawbacks of token-weighted voting through various mechanisms, each with their own complications. These include:

- **Quorum requirements** (frequently set between one to five percent of the total token supply) aim to ensure legitimate community support but often create gridlock. Many proposals might die because of apathy rather than opposition, and wealthy actors can block proposals by simply not participating.
- **Multi-signature ("multisig") controls** reintroduce human discretion as a safety mechanism to protect against malicious proposals.[498] A core team retains ultimate control via a multi-signature wallet (multisig),[499] or a designated group can overrule a passed proposal to protect the protocol from malicious actions.[500] This also creates central points of failure, as the controllers become the new power brokers.
- **Quadratic voting** *(See Appendix 12)* attempts to democratize influence by making voting power proportional to the square root of the tokens held by each individual, thereby reducing whale dominance. However, this mechanism does not protect against

491 Chainalysis Team, *Exploring DAOs: Uncovering Web3 Ownership Realities*, Chainalysis (June 27, 2022), https://blog.chainalysis.com/reports/web3-daos-2022; *See also*: Robin Fritsch, Marino Müller & Roger Wattenhofer, *Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?*, 5 Blockchain: rsch. & Applications 100208 (2024), https://doi.org/10.1016/j.bcra.2024.100208.

492 Larry Wall, *Blockchain Challenges and Governance*, Fed. Rsrv. Bank of Atlanta 1, 2 (July 30, 2018), https://business.cch.com/bfld/FederalReserveBankofAtlanta.pdf.

493 *See* Andrew Hall, *Governance FAQs*, a16z Crypto (July 20, 2023), https://a16zcrypto.com/posts/article/governance-faq/.

494 Yannis Bakos & Hanna Halaburda, *Will Blockchains Disintermediate Platforms? The Problem of Credible Decentralization in Daos* (Mar. 15, 2023) (manuscript at 18), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4221512.

495 De Filippi et al. *Report on Blockchain Governance Dynamics*, *supra* note 406, at 32-33.

496 *Cf.* Tom W. Bell, *Blockchain and Authoritarianism: The Evolution of Decentralized Autonomous Organizations*, *in* Blockchain and Public Law 102-04 (Oreste Pollicino & Giovanni De Gregorio eds., 2021) https://www.pbookshop.com/blockchain-and-public-law-global-challenges-in-the-era-of-decentralisation.html; Morshed Mannan, *Technocratic Despotism in the Network State*, *in* Decoding Digital Authoritarianism 73 (Global Affairs Canada 2023) https://posada.website/publication/platform-authority-and-data-quality/Digital-Authoritarnism.pdf.

497 Camiel Vermeulen & Willem-Jan Smits, *Blockchain Governance: What Is It, What Types Are There and How Does It Work in Practice?*, WatsonLaw (Oct. 24, 2018), https://watsonlaw.nl/en/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/.

498 Some DAOs allow proposals to be directly executed, even where there is a multisig, through oSnap or Zodiac reality.eth module. *See e.g.*, *oSnap*, UMA, https://uma.xyz/osnap (last visited Jan. 15, 2026) (allows community participation in governance transactions through off-chain governance voting).

499 *See What is Multi-Signature (Multi-Sig)?*, CoinBase, https://www.coinbase.com/learn/wallet/what-is-a-multi-signature-multi-sig-wallet (last visited Jan. 15, 2026); *see, e.g.*, alextnetto.eth, *[EP5.7] [Social] Security Council*, ENS Docs, https://docs.ens.domains/dao/proposals/5.7/ (last visited Jan. 15, 2026).

500 *See, e.g.*, alextnetto, blockful, *security-council-ens*, GitHub, https://github.com/blockful/security-council-ens (last visited Jan. 15, 2026).

"Sybil attacks,"[501] where large holders split holdings across multiple addresses to maximize influence.

- **Time-weight voting** rewards long-term alignment by increasing voting power based on lock-up duration. The drawback is that this creates illiquid governance markets and entrenches early adopters who locked tokens when opportunity costs were lower.

b. Staked-Based Governance

Staking refers to the process of locking cryptocurrency or tokens in a blockchain protocol to perform specific network functions, e.g. to validate transactions in proof-of-stake networks. When users stake tokens, they commit them for a specified period, during which the tokens cannot be freely traded or transferred. In return, stakers typically earn rewards (proportional to their stake) and/or acquire specific privileges, such as the right to validate blocks, participate in consensus, or participate in governance decisions. The specific rights and responsibilities associated with staking vary significantly across protocols.

Staking serves different functions across blockchain networks and is not inherently tied to governance rights. The most prominent example is Ethereum —the largest proof-of-stake network— where staking ETH provides economic security for the network but grants no governance privileges.[502] Ethereum validators earn rewards for securing the chain, but protocol decisions remain entirely off-chain through the EIP process.

When staking is linked to governance, it requires participants to lock tokens within a protocol to gain voting rights —along with some form of economic yield— thereby creating an economic mechanism that generates token demand, while distributing rewards and governance power to participants. This mechanism attempts to filter out speculators and short-term actors by requiring voters to bear opportunity costs, theoretically aligning governance with those genuinely invested in the protocol's long-term success. The basic premise is that staking demonstrates commitment beyond mere ownership. When token holders lock assets, they cannot sell during downturns or exploit temporary voting power for short-term gains. The reward mechanisms further strengthen the alignment between voting power and sustained engagement with the protocol.

However, the rise of liquid staking fundamentally challenges this "commitment" narrative often used to justify staking requirements. Over one-third of staked ETH exists as liquid staking derivatives (like stETH or rETH). This allows holders to maintain liquidity while they earn staking rewards. Users receive transferable tokens representing their staked position and enjoy staking yields without sacrificing capital efficiency. This feature reveals that staking's primary function might be economic rather than signaling long-term alignment.

Some protocols explicitly incorporate time-weighted voting into staked-based governance to enforce commitment. For instance, Curve Finance's vote-escrowed CRV (veCRV) requires locking tokens for longer periods (up to four years) to maximize voting power and protocol revenues.[503] Yet, even here, protocols like Convex[504] aggregate these locked positions, creating liquid markets

501 Named after a well-known book and film about a woman named Sybil with multiple personalities (*Sybil* is a 1973 book by Flora Rheta Schreiber that chronicles the treatment of Sybil Dorsett for dissociative identity disorder), a Sybil attack occurs when a single individual creates numerous identities or wallet addresses to manipulate the voting process by falsely appearing as multiple participants. This tactic of creating multiple identities to gain disproportionate voting power can distort perceptions of community consensus, mislead other token holders and enable the attacker to exert disproportionate influence over governance outcomes.

502 Matthieu Saint Olive & Simran Jagdev, *Understanding Slashing in Ethereum Staking: Its Importance and Consequences*, CONSENSYS (Feb. 7, 2024), https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences.

503 *See Overview - Locked CRV (veCRV)*, Curve Resources, https://resources.curve.finance/vecrv/overview/#boosting-crv-rewards (last visited Jan. 15, 2026); *Getting ATOM and Staking It*, Cosmos Acad., https://tutorials.cosmos.network/academy/1-what-is-cosmos/4-atom-staking.html (last visited Jan. 15, 2026).

504 *Convex Finance - Profile*, Messari, https://messari.io/project/convex-finance-2/profile (last visited Jan. 15, 2026).

for governance power and ultimately defeating the original purpose.

Despite its benefits, where staking and governance intersect, the requirements create barriers favoring specific actors over others. Professional validators accumulate delegated voting power from passive stakers, liquid staking providers control massive influence across chains, and early adopters who locked their tokens at low prices maintain permanent advantages.[505] Rather than democratizing participation, staked governance often concentrates power among those best positioned to exploit the rules of the system.

c. Delegate-Based Governance (Proxy Voting)

Delegate-based governance addresses a fundamental problem in token voting: Most holders lack the time, expertise, or interest to participate meaningfully in governance.[506] By enabling token holders to delegate voting power to third parties (while retaining ownership of tokens), these systems attempt to increase participation rates and decision quality. Those who are delegated to vote for others are often better informed or possess a deeper understanding of the specific rights and scope of authority associated with the governance process.[507] By delegating their votes to proxies, token holders can help ensure their tokens contribute to reaching a quorum and having their view represented in the governance decisions. Those who *receive* delegated voting power cannot access the underlying tokens. The separation between token ownership and governance participation is intended to facilitate more informed decision making while protecting the interests of token holders, since the proxy delegation can be revoked at any time.

However, delegation of voting power creates new forms of power concentration. While participation metrics might improve, actual influence concentrates among a small number of "super delegates" (such as venture capital funds like a16z or Polychain) who control a large ratio of active voting power. For example, in Compound governance, ten addresses control over 50% of delegated COMP.[508] Power concentration can occur through several mechanisms. Professional delegated voters can invest significant amounts of resources to build their reputations —publishing detailed voting rationales and engaging in governance forums to encourage more users to delegate voting power to them. Sometimes, this can even attract large token holders who delegate to aligned parties to maintain influence without the appearance of excessive centralization. This concentration of delegated voting power also raises transparency and disclosure concerns, as the incentives, affiliations, or potential conflicts of major delegates are not always visible to token holders.

505 *See generally* Kelsi Nabben & Primavera De Filippi, *Accountability Protocols? On-chain Dynamics in Blockchain Governance*, 13 Internet Pol'y Rev. 1 (2024), https://policyreview.info/articles/analysis/chain-dynamics-blockchain-governance.

506 *See* Lukas Weidener, Fabio Laredo, Kishore Kumar & Karlin Compton, *Delegated Voting in Decentralized Autonomous Organizations: A Scoping Review*, 8 FRONTIERS IN BLOCKCHAIN 01, 04-06 (2025), https://doi.org/10.3389/fbloc.2025.1598283. *See generally* Jeff Strnad, *Delegation and Participation in Decentralized Governance: An Epistemic View*, arXiv (May 7, 2025), https://arxiv.org/abs/2505.04136.

507 Patrick Kiger, *Inside a Government Where People Are Paid to Vote*, Stan. Graduate Sch. of Bus. (Nov. 17, 2023), https://www.gsb.stanford.edu/insights/inside-government-where-people-are-paid-vote. *See also* Hall, *supra* note 493.

508 Robin Fritsch, Marino Müller & Roger Wattenhofer, *Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?*, 5 Blockchain: Rsch. & Applications 1, 6-7 (2024), https://doi.org/10.1016/j.bcra.2024.100208.

FIGURE 26.

Compound's proxy-voting implementation

Compound's proxy-voting implementation[509] illustrates the double-edged nature of delegating votes. In order to boost participation in governance, Compound uses a delegate system where COMP holders can delegate their voting rights to community members without transferring token ownership.[510] To submit a proposal to be voted on, the proponent must have or garner the support of one percent of the total COMP supply —a safeguard to prevent frivolous or spam proposals. Other safeguards include the obligation to submit executable code in proposals (for transparency), a three-day voting period, and a two-day timelock between the end of voting and implementation of the result. This delay provides an opportunity for users to reassess their positions or exit the protocol if they oppose the changes.

Yet, these mechanisms do not prevent vote concentration. Major delegates, such as the venture capital fund a16z, control many delegated COMP tokens,[511] enabling them to effectively determine the outcome on most proposal votes. The one percent threshold means that only these "super delegates" or their allies can submit changes. While any token holder can theoretically become a delegate, building sufficient reputation to attract meaningful delegations requires significant time and resources. Hence, despite the greater participation generated by delegation, actual voting power remains highly concentrated among professionalized governance actors.

2. Automated Execution via Code

The defining feature of on-chain governance is its automated execution. Once voting concludes, smart contracts implement decisions without human intervention. This automation promises to eliminate implementation risk. It also ensures faithful execution of community will and removes the political maneuvering that often occurs between decision and action in traditional systems. When MakerDAO votes to adjust stability fees or Compound approves a new lending market, the changes activate precisely as specified, with no opportunity for intermediaries to delay, modify, or selectively implement decisions.[512]

This deterministic execution provides powerful benefits. Governance outcomes become credibly neutral[513] — the code executes an approved proposal identically, regardless of who proposed or opposed a measure. Minorities gain protection from implementation discrimination, as smart contracts cannot selectively apply rules. The gap between policy and practice disappears, solving the longstanding political problem of ensuring that decisions are faithfully translated into action. For global communities operating across jurisdictions, automated execution eliminates reliance on any single legal system or enforcement mechanism.

However, the deterministic nature of smart contracts creates a significant degree of rigidity. While off-chain governance systems preserve human judgment as a final safeguard (i.e. boards can recognize extraordinary circumstances, courts can issue injunctions, and leaders can exercise emergency powers), on-chain systems

509 *See Governance*, COMPOUND, https://docs.compound.finance/v2/governance/ (last visited Jan. 15, 2026).

510 See *Compound*, TALLY, https://www.tally.xyz/gov/compound (last visited Jan. 15, 2026), for an example of how voting power is assessed and delegated in the Compound network.

511 *See Compound – Delegates*, TALLY, https://www.tally.xyz/gov/compound/delegates (last visited Jan. 15, 2026).

512 MakerDAO, *Pause-Detailed Documentation*, MAKER PROTOCOL TECH. DOCS, https://docs.makerdao.com/smart-contract-modules/governance-module/pause-detailed-documentation (last visited Jan. 15, 2026).

513 Mikolaj Barczentewicz, *Legally Credible Neutrality,* 26-27 (2024) (unpublished manuscript), https://ssrn.com/abstract=5029148.

execute regardless of context, unable to distinguish between normal operations and exceptional situations.[514]

This rigidity extends beyond technical execution to social coordination. When circumstances change between the approval of a proposal and its implementation, on-chain systems cannot adapt. A parameter change appropriate during market stability might become destructive during volatility, but automated execution proceeds regardless. The 2022 Terra collapse *(See below Figure 27)*. demonstrated how governance decisions made under normal conditions can accelerate death spirals when contexts shift rapidly.[515] Off-chain governance might have recognized the extraordinary circumstances Terra faced and suspended normal procedures; on-chain automation ultimately amplified the crisis.[516]

514 *See generally* Wessel Reijers et al., *Now the Code Runs Itself: On-chain and Off-chain Governance of Blockchain Technologies*, 37(17) Topoi 821 (2021), http://dx.doi.org/10.2139/ssrn.3340056

515 *See generally* Jiaying Liu, Igor Makarov & Antoinette Schoar, *Anatomy of a Run: The Terra Luna Crash* (Nat'l Bureau of Econ. Rsch., Working Paper No. w31160, 2023), http://dx.doi.org/10.2139/ssrn.4416677.

516 Jiahua Cho, *A Token Economics Explanation for the De-pegging of the Algorithmic Stablecoin: Analysis of the Case of Terra*, 8 Ledger J. 27, 27-36 (2023), https://doi.org/10.5195/ledger.2023.283.

FIGURE 27.

The Terra collapse (2022)

In May 2022, TerraUSD ("UST") and its sister token Luna ("LUNA") collapsed over the course of just a few days, wiping out roughly $40 billion of value in the crypto ecosystem. The collapse was made possible by critical weaknesses in the underlying blockchain architecture.[517]

TerraUSD was an algorithmic stablecoin designed to maintain a $1 peg through a "burn-and-mint" mechanism involving LUNA, the native token of the Terra blockchain. Users could mint UST by burning LUNA and mint LUNA by burning UST, with the expectation that arbitrageurs would exploit price discrepancies to restore parity. This structure adjusted the supply of both tokens to maintain the exchange rate. The system, however, depended on continuous arbitrage activity, deep liquidity, and sustained market confidence.

UST's principal use case was within decentralized finance (DeFi) lending platforms, most notably Anchor, which attracted deposits by offering yields of up to 20% annually. Anchor's liabilities consistently exceeded its income from loans, rendering Terra's broader economic model unsustainable.[518] Once confidence eroded, depositors began rapidly withdrawing UST from Anchor, and traders started converting massive quantities of UST back into LUNA. This dramatically expanded LUNA's supply, driving its price toward zero, which in turn undermined the peg even further —a classic "death spiral."[519]

During the collapse, several governance proposals were introduced, including changes to minting caps and the deployment of reserve funds. Yet the governance process —requiring proposal submission, community deliberation, and voting— proved far too slow to address the speed of the unfolding crisis. This mismatch between the rapid dynamics of financial markets and the procedural pace of on-chain governance underscored the inability of decentralized governance mechanisms to provide effective crisis management. Moreover, despite the formal existence of participatory governance, decision making was heavily concentrated in Terraform Labs and its founder, Do Kwon, raising questions about the legitimacy and resilience of the system's governance architecture.[520]

In the aftermath, the U.S. Securities and Exchange Commission charged Terraform Labs and Do Kwon for securities fraud, describing the scheme as "breathtaking." Following a unanimous jury verdict finding them liable, Terraform and Kwon agreed to pay more than $4.5 billion — one of the largest civil securities fraud recoveries on record.[521] Separately, Do Kwon was sentenced to 15 years in prison in a parallel criminal prosecution.[522]

---

517 Antonio Briola et al., *Anatomy of a Stablecoin's failure: The Terra-Luna case*, 51 Finance Res. Letters 103358 (Jan. 2023), https://www.sciencedirect.com/science/article/abs/pii/S1544612322005359.

518 Financial Stability Board, Consultative Report: Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements 3-6 (2022), https://www.fsb.org/uploads/P111022-4.pdf. Financial Stability Board, Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements (July 2023), https://www.fsb.org/uploads/P170723-3.pdf.

519 *See* Liu, Makarov & Schoar, *supra* note 515.

520 *Id.*; *see* Marco Quiroz-Gutierrez, *Luna Founder Do Kwon Faces Criticism from Influential Voters About How the Terra Blockchain 'Rebirth' Was Carried Out*, Fortune (May 25, 2022), https://fortune.com/crypto/2022/05/25/terraform-labs-luna-crypto-do-kwon-vote-new-blockchain/.

521 Press Release, Sec. & Exch. Comm'n, Terraform and Kwon to Pay $4.5 Billion Following Fraud Verdict (June 13, 2024), https://www.sec.gov/newsroom/press-releases/2024-73.

522 Press Release, U.S. Att'y's Off., S.D.N.Y., Crypto-Enabled Fraudster Sentenced For Orchestrating $40 Billion Fraud (Dec. 11, 2025), https://www.justice.gov/usao-sdny/pr/crypto-enabled-fraudster-sentenced-orchestrating-40-billion-fraud. *See also* Superseding Indictment, United States v. Do Kwon, S1 23 Cr. 151 (JPC) (Jan. 2, 2025), https://www.justice.gov/d9/2025-01/do_kwon_superseding_indictment.pdf.

3.2.2.B. Case Studies

On-chain governance is widely implemented in Layer 1 (base-layer) blockchains, where governance powers are embedded in the native cryptocurrency, as well as in many decentralized applications (dApps) that introduced dedicated governance tokens to facilitate user participation in decision-making processes.

1. Tezos

Tezos pioneered self-amending ledgers where protocol upgrades occur entirely on-chain.[523] It offers a model where on-chain voting outcomes for protocol amendments are automatically enforced and integrated into the code. Its multi-stage process includes proposal periods, exploration voting, testing, and promotion voting, with automatic implementation of approved changes.[524] This eliminates hard forks but creates complex coordination challenges, with proposals sometimes failing due to voter apathy.[525]

2. Polkadot

Polkadot's governance system, OpenGov,[526] represents one of the most sophisticated implementations of on-chain governance, featuring multiple parallel tracks for different proposal types, adaptive quorums based on turnout, and a Technical Fellowship that provides expert guidance.[527] Despite its benefits, this complexity creates barriers to participation, as most DOT holders cannot navigate the intricate system, thus defaulting power to a small group of active participants.[528]

3. Cosmos

Cosmos standardized governance across its ecosystem through a governance module that all chains can implement.[529] Holders of staked ATOMs (Cosmos' tokens) vote on proposals ranging from parameter changes to software upgrades.[530] A unique "No with Veto" option allows one-third of voters to kill proposals entirely, thus providing minority protection but also enabling obstructionism.[531]

4. Uniswap

Uniswap is a decentralized finance (DeFi) protocol operating on Ethereum. Like many decentralized applications and scaling solutions built on Ethereum, it relies on explicit on-chain governance mechanisms.[532] Holders of the UNI governance tokens participate in collective decision making by voting on protocol parameters, the allocation of treasury funds, and upgrade proposals.[533] While this model enhances transparency and formalizes accountability, it also exhibits structural limitations. Voter participation is typically very low —often below one percent of the circulating UNI supply— and governance outcomes frequently reflect the preferences of large token holders, including venture capital funds, rather than the broader user community.

---

523 *See generally* L.M. Goodman, *Tezos – A Self-Amending Crypto-Ledger White Paper,* (Sept. 2, 2014), https://tezos.com/whitepaper.pdf.

524 De Filippi et al, *Report on Blockchain Governance Dynamics*, *supra* note 406, at 55-56.

525 Carthage was the first proposal to be rejected during the Proposal Period, which requires a minimum of 5% approval to move to the Exploration Period, and Carthage only obtained 3.5%. *Amendment History*, TEZOS DOCS, https://docs.tezos.com/architecture/governance/amendment-history (last visited Jan. 15, 2026).

526 *Polkadot OpenGov*, Polkadot Wiki, https://wiki.polkadot.network/learn/learn-polkadot-opengov/ (last visited Jan. 15, 2026).

527 De Filippi et al, *Report on Blockchain Governance Dynamics*, *supra* note 406, at 60.

528 *How to Implement Governance Proposals on Polkadot*, DEV Community (Aug. 5, 2024), https://dev.to/chainparser/how-to-implement-governance-proposals-on-polkadot-10hb.

529 *See Cosmos Whitepaper*, Cosmos Network, https://cosmos.network/whitepaper/ (last visited Jan. 15, 2026).

530 *See Governance Overview*, Cosmos Network, https://hub.cosmos.network/main/governance (last visited Jan. 15, 2026).

531 Notional Ventures, *A Beginner's Guide to Cosmos Governance*, Cosmos Ecosys. Blog (May 29, 2023), https://blog.cosmos.network/a-beginners-guide-to-cosmos-governance-26c5d767633a (last visited Jan. 15, 2026).

532 *See* Christine Kim, *The Ethereum Government*, Galaxy (June 3, 2024), https://www.galaxy.com/insights/research/ethereum-governance.

533 Fair Tokenomics Team, *The Tokenomics of Uniswap (UNI)*, FinDaS, https://www.findas.org/tokenomics-review/coins/the-tokenomics-of-uniswap-uni/r/581DwifCMJFX7eLsofUR56 (last visited Jan. 15, 2026).

FIGURE 28.

Uniswap

The Uniswap protocol allows holders of its native governance tokens, UNIs, to vote on protocol changes.[534] Any UNI holder with enough tokens can submit a proposal. Initially, proposals are reviewed off-chain or through community discussion to assess feasibility and impact. On-chain, proposals must pass a minimum threshold of UNI tokens to be given a formal vote. Votes are typically weighted by token holdings, allowing larger stakeholders to have proportionally greater influence. Delegation allows smaller holders to participate indirectly by assigning their voting power to trusted delegates. Certain technical or risk-sensitive proposals may undergo additional review by experienced developers to mitigate protocol risk.[535]

The fact that the Ethereum ecosystem has developed Layer 2 solutions and DAOs that often employ on-chain governance mechanisms results in a hybrid model. On the protocol layer, governance is off-chain, based on informal coordination among developers, researchers, validators, and community members. On the application layer, governance is on-chain, where token holders vote on upgrades, parameters, or resource allocation. Meanwhile, this creates a hybrid landscape where protocol-level decisions remain off-chain, while many applications built on Ethereum use on-chain governance.

3.2.2.C. Challenges of On-Chain Governance

One of the primary advantages of blockchain-based governance is its global accessibility. Because it is not constrained by geographic boundaries, anyone with internet access can participate in governance processes, potentially fostering more diverse and inclusive decision making. Moreover, the use of smart contracts enables automated and programmable execution of governance decisions, minimizing the risk of human error and ensuring that outcomes are implemented exactly as approved, without reliance on intermediaries.

Transparency is another key benefit: Every proposal, vote, and execution is permanently recorded on an immutable ledger, creating a complete audit trail of governance decisions. This visibility enables public scrutiny that is impossible in traditional systems[536] —researchers can analyze voting patterns, journalists can track fund allocations, and community members can verify that approved proposals are implemented exactly as specified. However, private or anonymous voting mechanisms can be implemented in blockchain-based systems, enabling ballots to remain confidential including through techniques such as zero-knowledge proofs.[537] These approaches allow individual votes to remain confidential, while preserving the public verifiability of the overall outcome. Such approaches remain technically complex and have not yet been widely adopted in practice. As a result, most existing DAO governance systems continue to rely on fully transparent voting. In this context, transparency may introduce unintended consequences that can undermine governance integrity.

1. Vote Buying

Vote buying, once difficult to verify in secret ballot systems, becomes explicitly verifiable on-chain, enabling explicit

534 *See Governance Reference*, Uniswap Docs, https://docs.uniswap.org/contracts/v2/reference/Governance/governance-reference (last visited Jan. 15, 2026); *Process*, Uniswap Docs, https://docs.uniswap.org/concepts/governance/process (last visited Jan. 15, 2026).

535 RevoGames, *The Creation of the Uniswap Risk DAO*, Uniswap (Dec. 2022), https://gov.uniswap.org/t/the-creation-of-the-uniswap-risk-dao/19586 (a risk assessment mechanism that applies, among other things, to governance proposals).

536 Naresh Kshetri, *Blockchain Technology for Improving Transparency and Citizen's Trust*, *in* Advances in Information and Communication 716-735 (Kohei Arai ed., 2021), https://www.scirp.org/reference/referencespapers?referenceid=3413790.

537 Kamilla Nazirkhanova, Vrushank Gunjur, X. Pilli, Cruz de Jesus and Dan Boneh, *Kite: How to Delegate Voting Power Privately*, ArXiv (2025) https://arxiv.org/abs/2501.05626; Felix Maduakor, Thi Van Thao Doan & Joerg Mitzlaff, *opn.vote: A Publicly Verifiable Blockchain-Based eVoting System* (2025) https://www.opn.vote/wp-content/uploads/2025/04/Voting_25-short-paper-opn.vote-A-Publicly-Verifiable-Blockchain-Based-eVoting-System.pdf.

bribery markets. Protocols like Curve *(See below Figure 29)* have seen the emergence of sophisticated bribery markets where millions are spent on vote incentives. Governance is transformed from deliberation into auction. The DeFi protocol Votium built its entire business around aggregating and selling voting power, creating liquid markets for political influence.[538] While buying votes and bribing voters can lead to bad collective or social outcomes,[539] such mechanisms may also be understood as allowing participants to express the intensity of their preferences, potentially improving the allocative efficiency of governance decisions.

FIGURE 29.

Curve

"Bribing" token holders is a key feature of a popular DeFi protocol, Curve.[540] With Curve, token holders with the largest number of tokens can pay (the community uses "bribe" as a term of art, even though it refers to a legitimate incentive) other token holders to provide liquidity to favored Curve liquidity pools. The chosen Curve liquidity pools in turn receive greater "emissions" (issuances) of new Curve governance tokens. Paying token holders for their votes simply allows holders to actively monetize their voting rights and should increase the allocative efficiency of the votes.[541] Overtly and publicly paying other token holders is referred to – non-pejoratively– as "incentivized governance."[542]

2. Majority Governance Attacks

Most on-chain governance systems lack safeguards against "majority governance attacks." These are attacks in which the token-weight majority of actors consolidate voting power to unilaterally influence governance decisions. This means that wealthy actors or coordinated groups could potentially accumulate enough tokens to push through self-serving proposals, effectively hijacking the protocol's future direction. Without mechanisms like timelocks, veto powers for minority stakeholders, and caps on voting influence, these systems remain susceptible to plutocratic capture where governance becomes dominated by the largest token holders rather than reflecting the broader community's interests.

Two notable majority governance attacks were made against the DeFi protocols "Build Finance" and "Beanstalk Finance." In the attack on Build Finance, the attacker obtained enough governance tokens to vote through a proposal that gave the attacker full control of the DAO treasury.[543] In the attack on Beanstalk, the attacker used a flash loan to temporarily acquire a majority of governance voting power, approved a malicious proposal, and immediately executed it—draining approximately $182 million from the protocol and realizing a net profit of about $77 million after repaying the loan.[544]

538 Darcy W. E. Allen & Kelsie Nabben, *Democratic Governance and Blockchain Governance: Is Reconciliation Possible?* 9 (Dec. 17, 2024) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5008643.

539 *See* Vitalik Buterin, *Moving Beyond Coin Voting Governance*, Vitalik Buterin's Website (Aug. 16, 2021), https://vitalik.eth.limo/general/2021/08/16/voting3.html. *See also* Vitalik Buterin, *On Collusion*, Vitalik Buterin's Website (Apr. 3, 2019), https://vitalik.eth.limo/general/2019/04/03/collusion.html; Lucas Tcheyan, *Governance in DeFi*, GALAXY (Nov. 4, 2022), https://www.galaxy.com/insights/research/governance-in-defi/.

540 *There's Now an App for Bribing Curve Token Holders*, THE DEFIANT (Aug. 12, 2021), https://thedefiant.io/news/defi/andre-cronje-curve-bribe-tool.

541 *What Are Bribes in Cryptocurrency and Decentralized Finance?*, CHAINDEBRIEF (May 18, 2023), https://chaindebrief.com/what-are-bribes-in-cryptocurrency-and-decentralized-finance/.

542 Aragon, *Incentivized Governance or Institutional Bribery in Web3?*, The Aragon Network (May 14, 2022), https://blog.aragon.org/incentivized-governance-or-institutional-bribery-in-web3/.

543 Tim Copeland, *Build Finance DAO suffers 'hostile governance takeover,' loses $470,000*, THE BLOCK (Feb. 14, 2022), https://www.theblock.co/post/134180/build-finance-dao-suffers-hostile-governance-takeover-loses-470000.

544 Rob Behnke, *Explained: The Beanstalk Hack (April 2022)*, HALBORN BLOG (Apr. 25, 2022), https://www.halborn.com/blog/post/explained-the-beanstalk-hack-april-2022.

FIGURE 30.

The Steem governance takeover[545]

The Steem platform (steemit.com) is a blockchain-based social media network that employs its native token to incentivize content creation and curation *(See below 4.6.2.B.)*. Steem operates through a delegated proof-of-stake governance system in which token holders vote to elect "Witnesses," who serve as block producers and validators responsible for maintaining the network in a role broadly analogous to miners or validators in other blockchain architectures. At the project's inception, the founders publicly stated that a large founder-controlled stake created at the network's launch would not be used to influence governance. At the same time, substantial quantities of Steem tokens were held in custodial accounts by centralized cryptocurrency exchanges on behalf of their users.

In 2020, Justin Sun acquired Steemit Inc., the private company behind the Steem platform that held a large allocation of STEEM tokens, thereby obtaining control over those tokens. He then persuaded several major exchanges to use the tokens held in custody to support his voting block: these exchanges used Steem tokens deposited by their customers to vote in witness elections supporting Sun's preferred governance slate. Through the combined use of these custodial tokens and the newly acquired stake, this coalition temporarily secured sufficient voting power to influence the composition of Steem's governing witnesses. Many community members characterized this episode as a de facto "hostile takeover" of the blockchain's governance. In response, many token holders coordinated to elect an alternative set of witnesses and subsequently implemented a hard fork that created a new blockchain, Hive, which excluded the contested stake from its governance structure. The exchanges that had initially supported Sun later withdrew their votes following significant public backlash.

This episode can be understood as a blockchain analogue of what corporate governance scholars describe as "empty voting"[546], a situation in which voting rights are exercised by actors whose economic interests do not fully correspond to those of the underlying asset holders. In the Steem case, exchanges used tokens held in custody for their customers to influence governance outcomes, even though the economic interests in those tokens belonged to the customers rather than to the exchanges themselves. By contrast, many forms of empty voting in corporate governance are far more subtle and often remain difficult to detect.[547]

Some protocols retain the ability to act unilaterally in a crisis by granting emergency powers to founding teams or other knowledgeable affiliates and insiders.[548] However, emergency governance mechanisms designed to prevent such attacks —like multisig overrides[549] or guardian roles[550]— can create the opposite problem by concentrating power in the hands of a small group of trusted actors who can bypass normal governance processes. This creates a fundamental tension between protecting against malicious takeovers and maintaining true decentralization, because the cure for majority attacks often involves creating new centralization risks.

545 Werbach et al., *supra* note 430.

546 Henry T.C. Hu & Bernard Black, *The New Vote Buying: Empty Voting and Hidden Ownership*, 79 S. Cal. L. Rev. 811 (2006), https://southerncalifornialawreview.com/wp-content/uploads/2018/01/79_811.pdf.

547 *Id.*; see *also* Jeff Strnad, *Economic DAO Governance: A Contestable Control Approach*, ARXIV, at 7-9 (2024), https://arxiv.org/abs/2403.16980.

548 Carolyn Wilkins, *Governance of "Decentralised" Finance: Get up, Stand up!*, BANK OF ENGLAND (Oct. 19, 2022), https://www.bankofengland.co.uk/speech/2022/october/carolyn-wilkins-speech-at-ucl-centre-for-blockchain-technologies.

549 A multisig override allows a small group of members to bypass the voting process and make changes to a network in case of an emergency, such as an active hacking.. The Investopedia Team, *Multi-Signature Wallets: Definition and Use Cases*, INVESTOPEDIA, https://www.investopedia.com/multi-signature-wallets-definition-5271193 (last visited Jan. 15, 2026).

550 A designated member or group of members (guardians) can initiate an emergency protocol and bypass ordinary governance mechanisms, if needed. *See, e.g.*, *Governance*, AAVE, https://aave.com/docs/developers/governance (last visited Jan. 15, 2026).

FIGURE 31.

Solend

The DeFi protocol Solend encountered a potential solvency crisis in 2022, related to its lending operations. In response, the founding team advanced a governance proposal on an expedited timeline, despite the fact that the protocol's established governance procedures did not permit such acceleration.[551] The proposal sought to grant the team immediate and unilateral authority to take control of a large user account that was at risk of triggering a margin call.[552] The team argued that a sudden liquidation of this account could destabilize the protocol by sharply depressing asset prices. Intervention was necessary, said the team, to conduct an orderly liquidation. Although the proposed measure may have been driven by prudential concerns, it provoked a strong backlash from the Solend community. Facing significant opposition, the team ultimately withdrew the proposal and abandoned its claim to emergency powers.[553]

Some protocols have introduced "rage-quit" mechanisms that allow dissenting token holders to exit with their proportional share of treasury assets before controversial proposals take effect, creating indirect social pressure on majority voters to consider minority interests. This exit option acts as a check on governance power, as proposals that trigger mass exits would diminish the value and utility of the remaining network, incentivizing more inclusive decision making.

FIGURE 32.

Rage-quit mechanisms

A rage-quit mechanism is a governance feature in decentralized autonomous organizations (DAOs) that enables members who disagree with a community decision to withdraw from the organization and claim a proportional share of its treasury.[554] This mechanism serves as a safeguard against the tyranny of the majority by providing dissenting members with a formal exit option. Upon initiating a rage quit, a member relinquishes their governance tokens and voting rights, receives their share of the DAO's assets, and severs their affiliation with the organization. This affords a level of minority protection, though early results with this protection have been mixed.[555] MolochDAO[556] was the first to implement the rage-quit mechanism, which has since been adopted by other DAOs, such as DAOhaus and MetaCartel.[557]

551 Oliver Knight, Danny Nelson & Coindesk, *Solana DeFi Platform Votes to Reverse 'Emergency Powers' to Take over Whale Account Facing Massive Margin Call*, Fortune Crypto (June 20, 2022), https://fortune.com/crypto/2022/06/20/solana-defi-platform-solend-votes-to-reverse-emergency-powers-to-take-over-whale-account. *See also* Danny Nelson, *Solend's Whale Liquidation Crisis Prompts Second Vote to Reverse 'Emergency Powers'*, Yahoo Fin. (June 20, 2022), https://finance.yahoo.com/news/solend-whale-liquidation-crisis-prompts-042015827.html.

552 Scott Chipolina, *Cryptocurrency Fallout Delivers Sharp Kick to Decentralised Finance Dreams*, THE FIN. TIMES (June 22, 2022), https://www.ft.com/content/3d1a2409-4030-4a26-be27-dbcb25f6fd75.

553 Nelson, *supra* note 551.

554 Gail Weinstein, Steven Lofchie & Jason Schwartz, *A Primer on DAOs*, Harvard L. Sch. F. on Corp. Governance (Sept. 17, 2022), https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/.

555 Jack Kubinec, *3 DAO Governance Trends to Watch in 2024*, Blockworks (Dec. 22, 2023), https://blockworks.co/news/dao-governance-experiments-2024.

556 *What is Rage Quitting in Crypto and DAOs?*, COINARY, https://coinary.com/learn/meaning-ragequit-in-crypto-daos/ (last visited Jan. 15, 2026).

557 Moloch DAO, COINMARKETCAP ACAD., https://coinmarketcap.com/academy/glossary/moloch-dao (last visited Jan. 15, 2026).

3. Social Pressures and Informal Negotiations

Another issue specific to on-chain governance is that the public nature of voting enables social pressures that can compromise independent decision making.[558] Large token holders can monitor and potentially retaliate against those who vote against their interests, creating implicit coercion. This visibility generates herding effects, too, where early votes disproportionately influence outcomes as voters observe trending decisions and align with perceived winners rather than exercising independent judgment.[559]

Furthermore, while blockchain can record all formal governance actions, it cannot capture the informal negotiations, side deals, and social dynamics that shape these decisions. While smart contracts automate vote counting and execution, they cannot automate the human processes of deliberation, compromise, and consensus building. Critical governance work still occurs off-chain —in Discord channels, forum posts, and private negotiations. Empirical research shows whales often coordinate their voting strategies through private communication channels,[560] and participants report reputation concerns affecting their voting behavior.[561] On-chain mechanisms merely ratify decisions shaped by traditional social dynamics. The transparency is thus selective, showing final votes while obscuring the process that produced them. This creates an accountability gap where visible on-chain actions may merely ratify invisible off-chain agreements, providing transparency theater rather than genuine openness. The immutability that ensures accountability also means that governance mistakes, hasty decisions, or compromised votes become permanent records that cannot be corrected or contextualized.

558 Jun Huang et al., *The Application of the Blockchain Technology in Voting Systems: A Review*, 54 ACM COMPUTING SURVEYS 1, 7-8 (Apr. 2021) https://dl.acm.org/doi/10.1145/3439725.

559 *See generally* Johannes Sedlmeir, Jonathan Lautenschläger, Gilbert Fridgen, and Nils Urbach, *The Transparency Challenge of Blockchain in Organizations*, 32 ELEC. MKTS. 1779 (March 17, 2022), https://doi.org/10.1007/s12525-022-00536-0.

560 Tanusree Sharma et al., *Unpacking How Decentralized Autonomous Organizations (DAOs) Work in Practice* 5 ARXIV (Apr. 17, 2023), https://arxiv.org/pdf/2304.09822. The study identified several contextual factors contributing to coordinated voting patterns among large token holders (whales), including that many whales belong to managerial teams and "some of their communication happen through private channels like private discord, DMs or telegrams."

561 *Id*. The study also documented reputation concerns affecting voting behavior, with one participant noting reluctance to vote against certain proposals because "my reputation would be on the line."

FIGURE 33.

MakerDAO's on-chain governance system

MakerDAO provides a useful illustration of the evolving dynamics of governance in decentralized protocols, including the tensions between progressive decentralization, persistent concentrations of power, and subsequent efforts to restructure governance arrangements. The governance of the Maker protocol originally combined the Maker Foundation, which played a central role in the protocol's early development, with on-chain governance exercised through MKR token holders.

MakerDAO governs the issuance and stability of DAI, one of the most widely used decentralized stablecoins.[562] Holders of MakerDAO's governance token (MKR) may vote on a broad range of proposals, including adjustments to risk parameters (such as collateral types, stability fees, and debt ceilings), protocol upgrades, and strategic initiatives.[563] Governance proposals are typically discussed in public forums and calls before being encoded in smart contracts and submitted for on-chain, token-weighted voting. Once the required voting thresholds are met, approved changes are executed directly on the blockchain.

Because voting power is proportional to the amount of MKR held, governance outcomes are heavily influenced by large token holders, including early investors and venture capital firms.[564] Governance analyses have shown that a relatively small number of MKR addresses consistently exercise significant influence over outcomes, raising concerns about concentration of power in a system nominally designed to be decentralized.[565] This concentration illustrates a broader governance pattern observed in many DAO-based systems: While decision-making is formally decentralized, effective influence may remain concentrated among a relatively small set of actors. Those with significant holdings can steer outcomes in ways that may privilege their interests, which do not always align with those of DAI users or the broader DeFi ecosystem. For instance, token holders may favor strategies that generate short-term fee revenue while shifting risks to stablecoin holders.

To mitigate these dynamics, MakerDAO experimented with a range of governance mechanisms aimed at broadening participation and improving decision quality. These included governance facilitators, delegated voting, and specialized expert teams. The governance facilitators were neutral actors tasked with managing governance processes, ensuring procedural fairness, and lowering barriers to entry for community members.[566]

Continued

562 *MKR Governance 101*, MakerDao, https://makerdao.com/en/governance/ (last visited Jan. 15, 2026); Sun, Stasinakis & Sermpinis, *supra* note 482 at 1, 2,

563 Sun, Stasinakis & Sermpinis, *supra* note 482 at 4; *see also* Jordan Cole, *Understanding the MakerDAO Governance Process for Stablecoins: Insights and Mechanisms*, BlockApps (Dec. 26, 2024), https://blockapps.net/blog/understanding-the-makerdao-governance-process-for-stablecoins-insights-and-mechanisms/.

564 *See generally* Sun, Stasinakis & Sermpinis, *supra* note 482;Venture capital firms have acquired substantial stakes: Andreessen Horowitz purchased 6% of MKR supply for $15 million in September 2018, while Dragonfly Capital Partners and Paradigm collectively purchased approximately 5.5% of total supply for $27.5 million in December 2019. *See* Shermin Voshmgir, Token Economy, (3d ed.), ch. 20, https://token.kitchen/token-economy/third-edition/ch20-use-case-2-makerdao;.

565 Sun, Stasinakis & Sermpinis, *supra* note 482 at 1, 13.

566 MIP3, *Governance Cycle*, MakerDao (defining Governance Facilitator responsibilities), https://mips.makerdao.com/mips/details/MIP3 (last visited Jan. 15, 2026).

FIGURE 33. (continued)

MakerDAO's on-chain governance system (continued)

Delegated voting[567] through the MakerDAO Delegates Program allowed MKR holders to delegate their voting power to publicly accountable representatives. And specialized expert teams,[568] were funded operational teams responsible for functions such as collateral risk analysis, protocol engineering, governance coordination, and treasury management, providing analysis and structured recommendations. The expert teams' role was to ensure that governance decisions were informed by technical and financial expertise.

Following the progressive transfer of governance responsibilities from the Maker Foundation to MKR token holders, the Foundation formally dissolved in 2021, after which governance of the protocol was conducted through on-chain voting by MKR holders. Contemporaneous communications by the Foundation and industry media described this transition as rendering MakerDAO "fully" or "completely" decentralized.[569]

Beginning in 2024, MakerDAO implemented a major governance restructuring known as the *Endgame Plan*, accompanied by a rebranding of the ecosystem as "Sky." This restructuring argued that the previous "Core Unit" model had become too bureaucratic and complex for token holders to manage effectively.[570] The Endgame Plan replaces direct management of human teams with a constitutional ruleset (The "Atlas") and splits the ecosystem into semi-autonomous entities often described as "SubDAOs" or "Stars," each with its own governance structure, treasury, and economic incentives.[571] While presented as a means of improving scalability and resilience,[572] this restructuring has also been interpreted by some observers as reflecting a broader dynamic in DAO governance:[573] systems initially designed to decentralize decision-making may periodically reintroduce more structured coordination mechanisms in response to governance inefficiencies. In this sense, the evolution of MakerDAO illustrates how decentralized governance arrangements may evolve through successive phases of decentralization, concentration of influence, and institutional redesign.[574]

567 *See generally* Chuxuan Fan, Tao Shu & Fei Xie, *Is There Wisdom Among the DAO Crowd? Evidence from Vote Delegation* (Eur. Corp. Governance Inst., Finance Working Paper No. 1077/2025, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5066656; *see also MKR Holder's Guide to Delegation*, MakerDao Governance Manual, https://github.com/makerdao/governance-manual/blob/main/delegation/mkr-holder-guide.md (last visited Jan. 15, 2026).

568 *See* MIP39, *Core Units*, MakerDao Governance Manual, https://github.com/makerdao/governance-manual/blob/main/core-units/core-units.md (last visited Jan. 15, 2026); MIP41c4-SP2, *Risk Core Unit Facilitator Onboarding*, MakerDao (Feb. 3, 2021), https://github.com/makerdao/mips/blob/master/MIP41/MIP41c4-Subproposals/MIP41c4-SP2.md (last visited Jan. 15, 2026).

569 Brady Dale, *MakerDAO Moves to Full Decentralization; Maker Foundation to Close in Months*, Nasdaq (July 20, 2021), https://www.nasdaq.com/articles/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months-2021-07-20. *See also* Andrew Asmakov, *MakerDAO's Foundation to Dissolve as Protocol Completes Decentralization*, CoinDesk (July 20, 2021), https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months?utm.

570 Bessie Liu, *MakerDAO Makes First Steps Toward Endgame*, Blockworks (Mar. 27, 2023), https://blockworks.co/news/makerdao-makes-first-steps-toward-endgame.

571 LCX AG Liechtenstein, *MiCAR White Paper v 1.0*, 14 (Aug. 2025), https://www.lcx.com/wp-content/uploads/SKY-SKY-MiCA-Whitepaper-v1.0.pdf.

572 David Christopher, *Maker Gets Ready for Endgame*, Bankless (Mar. 19, 2024), https://www.bankless.com/maker-gets-ready-for-endgame.

573 Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L.J. 487 (2018), http://www.btlj.org/data/articles2018/vol33/33_2/Werbach_Web.pdf.

574 Jeff Strnad, *Economic DAO Governance: A Contestable Control Approach*, arXiv, at 27–28 & nn.105–06, 117–18, 129–30, 147–48, 153 (2024), https://arxiv.org/abs/2403.16980.

3.3. CONCLUSION

The distinction between on-chain and off-chain governance is central to understanding the challenges of blockchain governance. On-chain governance offers significant advantages, particularly in terms of confidence, transparency, and traceability. Yet it is also beset by limitations which reflect structural trade-offs inherent to collective decision-making systems: risks of plutocracy, vote buying, excessive determinism, and institutional rigidity. By contrast, off-chain governance is more flexible and adaptable but frequently operates through invisible channels of influence and remains vulnerable to human fallibility, including corruption or capture. Effective blockchain design, therefore, requires acknowledging both modalities and striking an appropriate balance, so that systems can benefit from the predictability of on-chain mechanisms while retaining the adaptability of off-chain processes.

This on-chain/off-chain divide is also related to another key divide: minimalist governance (exemplified by Bitcoin) and maximalist governance (illustrated by MakerDAO). Proponents of *minimalist governance* argue that a protocol's core code should remain fixed, with changes introduced only rarely and under exceptional circumstances.[575] Making protocol changes exceedingly difficult[576] is intended to safeguard decentralization, strengthen the credibility of the protocol, and preserve its resistance to censorship.[577] Yet excessive rigidity can undermine the system's ability to adapt to new challenges, since blockchain protocols, like other complex systems, require mechanisms for evolution.[578] By contrast, *maximalist governance* permits frequent and wide-ranging adjustments to system parameters. Governance-token systems, for example, may extend decision-making authority beyond technical matters to encompass user rights, content moderation, and broader economic policies.

Ultimately, governance-minimization strategies cannot eliminate the need for protocol modification: Rules can always be altered —most notably through forks— which may override or nullify on-chain guarantees. Within this framework, off-chain governance consistently takes precedence over on-chain mechanisms. Recognizing this dynamic, certain blockchains, such as Tezos and Polkadot, have introduced formal on-chain processes for protocol change to combine stability with adaptability. These experiments underscore a broader lesson: Blockchain governance cannot be reduced to code alone but must be understood as an interplay between technological constraints and political authority.

More broadly, while blockchain networks often succeed in achieving *technical* decentralization, *political* decentralization remains far more elusive. *Technical decentralization* relates to the architecture of the blockchain protocol and network: how many nodes validate transactions, whether consensus is permissionless, whether there are bottlenecks or single points of failure. Yet these features do not necessarily produce a genuine dispersion of power. *Political decentralization*, by contrast, concerns governance and

575 Fred Ehrsam & Dan Robinson, *Governance Minimization*, Fred Ehrsam (Nov. 28, 2020), https://www.fehrsam.xyz/blog/governance-minimization ("Governance minimization means reducing the power and reliance on governance wherever possible. Governance minimization is important because it supports the primary value proposition of protocols: credible neutrality. Minimizing governance tends to make protocols more credibly neutral.")

576 *See generally* Jakob Svennevik Notland, Mariusz Nowostawski & Jingyue Li, *An Empirical Study on Governance in Bitcoin's Consensus Evolution*, arXiv (Feb. 14, 2024), https://arxiv.org/pdf/2305.04079, for a discussion about coming to a consensus on the Bitcoin network.

577 *Id.*; see *also* Miles Jennings, *Machiavelli for DAOs: Principles for Fixing Decentralized Governance (Part 1)*, a16z Crypto (Sept. 21, 2023), https://a16zcrypto.com/posts/article/machiavelli-principles-dao-decentralized-governance/.

578 Eric Alston, Wilson Law, Ilia Murtazashvili & Martin B.H. Weiss, *Blockchain Networks as Constitutional and Polycentric Orders*, 18 J. Institutional Econ. 707, 711-13 (2022), https://www.researchgate.net/publication/357716553_Blockchain_networks_as_constitutional_and_competitive_polycentric_orders.

the distribution of authority: who decides on protocol upgrades, who can alter rules, and whether influence is concentrated among a limited set of actors.

In practice, decision-making power is frequently monopolized by a narrow elite of core developers, miners, token holders, or corporate entities, thereby reproducing the very hierarchies blockchain was intended to displace. This structural asymmetry —with systems technically decentralized (many nodes, open consensus) yet politically centralized (a small group dictates upgrades or controls development)— reveals that technical architecture alone cannot guarantee political pluralism and instead risks entrenching new forms of oligarchic control under the guise of decentralization. One form of power asymmetry arises when authority is concentrated in the hands of large token holders: a de facto plutocracy. Another occurs when decision-making authority is concentrated among technical experts and core developers, whose deep knowledge of the system's architecture and vulnerabilities gives them disproportionate influence.[579]

Although the value of technical expertise in governance is undeniable,[580] such technocratic dominance —sometimes described as a "developer oligarchy"[581]— may, under certain conditions, reduce responsiveness to the broader user community. However, the influence of developers and the power of large token holders should not be understood in exclusively negative terms. In some instances, these features may enhance, rather than undermine, the system's capacity to respond to external signals and adapt over time. In particular, they may contribute to more effective coordination and decision making, especially where widely dispersed participants lack the incentives or expertise to engage meaningfully in governance. Moreover, the concentration of voting power in large token holders may align governance authority with economic exposure and mitigate certain collective action or agency problems.[582] In practice, governance tokens are frequently traded on secondary markets, creating continuous feedback mechanisms between governance decisions and market valuation. This market discipline may, in turn, exert pressure on both large token holders and core developers to act in ways that sustain user confidence and long-term value.

Finally, consensus mechanisms themselves may exhibit centralization tendencies.[583] In PoW (proof of work) systems, miners frequently aggregate their computational resources into mining pools, resulting in a concentration of hash power among a small number of dominant actors. In Bitcoin, for example, pools such as AntPool[584] and ViaBTC,[585] have at times collectively controlled a substantial share of the network's computational power.[586] Such developments raise concerns about the risk that dominant actors could selectively exclude or delay certain transactions from being processed.[587]

579 Fred Ehrsam, *Blockchain Governance: Programming Our Future*, Medium (Nov. 27, 2017), https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74 (arguing that a blockchain's long-term success depends on its governance model's ability to adapt and align stakeholder incentives through on-chain coordination); Ehrsam & Robinson, *supra* note 575 (proposing that the most successful protocols will minimize active governance to become more credibly neutral and dependable, thereby fostering wider adoption).

580 *The Future of Digital Assets: Providing Clarity for the Digital Asset Ecosystem: Hearing Before the H. Comm. on Fin. Servs.*, 118th Cong. 4 (2023) (statement of Dr. Emin Gün Sirer, Founder & CEO, Ava Labs, Inc.), https://www.congress.gov/event/118th-congress/house-event/116085/text.

581 *See* Bodó & Giannopoulou, *supra* note 435, at 121.

582 Strnad, *Delegation and Participation in Decentralized Governance*, supra note 506, at 58.

583 Halaburda, *supra* note 399.

584 *AntPool - World Leading BTC Mining Pool*, AntPool, https://www.antpool.com/home?lang=en (last visited Jan. 15, 2026).

585 *ViaBTC - Your All-in-one Crypto Mining Pool*, ViaBTC, https://www.viabtc.com/en/ (last visited Jan. 15, 2026).

586 Matteo Romiti et al., *A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares*, arXiv 12 (May 15, 2019), https://arxiv.org/abs/1905.05999.

587 Malik et al. showed that when large miners dominate PoW mining, they increase transaction fees and generate deadweight loss. *See generally* Nikhil Malik et al., *Why Bitcoin Will Fail to Scale?*, 68 Mgmt. Sci. 7065 (2022), http://dx.doi.org/10.2139/ssrn.3323529.

Centralization risks are not eliminated in proof-of-stake (PoS) systems. Since Ethereum's transition from PoW to PoS, validator concentration has increasingly taken the form of staking intermediaries. Liquid staking protocols, such as Lido,[588] aggregate staking power on behalf of users[589] (on Lido DAO, *see below section 6.4.2.B.)*. Similarly, centralized exchanges such as Coinbase and Binance also operate large validator sets. Although these actors do not exercise unilateral control over the protocol, their scale grants them disproportionate influence over transaction validation and, indirectly, over the network's governance dynamics.[590] These concerns are even more pronounced in more permissioned PoS-based systems. For instance, the Binance Smart Chain operates with a relatively small and curated validator set, many of whom are selected or closely associated with Binance itself, calling into question the network's effective level of decentralization.[591] This trend raises concerns that consensus power may become concentrated in the hands of a limited number of large validators, undermining the decentralization objectives that such mechanisms are intended to serve.

Overall, it is important that designers and developers get more acquainted with blockchain governance, because the success of a blockchain project depends first and foremost on the technical viability of the project, as well as its successful governance. Failures in governance can lead to a complete failure of a project, either because of conflict or paralysis, or the inability to adapt to the changing environment.

---

588 *See* Arijit Sarkar, *Lido's Ethereum Staking Market Share Dips Below 30%*, CoinTelegraph (Apr. 4, 2024), https://cointelegraph.com/news/lido-ethereum-staking-market-share-below-30. As of November 2025, Lido remains one of the largest Ethereum staking platforms by market share, controlling between 24% and 28% of all ETH staked; See *Dan Mitchell, What is Lido (LDO)? Everything you need to know about the DAO cryptocurrency*, Capital (Nov. 13, 2025), https://capital.com/en-eu/analysis/what-is-lido-your-ultimate-guide.

589 hildobby, *Ethereum ETH Staking*, Dune Analytics, https://dune.com/hildobby/eth2-staking (last visited Jan. 15, 2026).

590 *See* Sam Kessler, *Lido DAO Democratized ETH Staking, then Dominated It*, CoinDesk (Mar. 8, 2024), https://www.coindesk.com/consensus-magazine/2023/12/04/lido-dao-democratized-eth-staking-then-dominated-it; Aleksandar Gilbert, *Lido Co-Founder Sees Coinbase and Other Centralized Stakers as a Threat*, The Defiant (Oct. 14, 2022), https://thedefiant.io/news/defi/lido-coinbase-threat. *See also* Dominic Grandjean, Lioba Heimbach & Roger Wattenhofer, *Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization*, arXiv (June 19, 2023), https://arxiv.org/abs/2306.10777.

591 Micah Casella, *State of BNB Chain Q3 2023*, Messari (Oct. 30, 2023),https://messari.io/report/state-of-bnb-chain-q3-2023

KEY TAKEAWAYS

■ Blockchain systems are designed to operate without central authorities, yet they inevitably require governance to function and evolve. **Blockchain governance** refers to the processes through which such systems are maintained, updated, and adapted. It encompasses decisions about who can propose changes, how such proposals are evaluated, and how they are ultimately adopted. In practice, governance involves complex interactions among developers, users, and other stakeholders. It also spans multiple layers including the protocol, application-layer organizations, such as decentralized autonomous organizations (DAOs), and the broader ecosystem.

■ The expression "blockchain governance" designates both governance ***of* the infrastructure** (i.e., how protocols are maintained and updated) and governance ***by* the infrastructure** (i.e., the use of blockchain technology to govern activities beyond the protocol itself). In practice, most debates focus on governance of the infrastructure. These encompass decisions relating to consensus mechanisms, monetary policy, protocol upgrades, treasury allocation, interoperability, and cybersecurity. Because such updates and modifications may generate disagreement among stakeholders, governance processes must be perceived as legitimate by the community to be effective.

■ A central question is who has the authority to change the code. In practice, **decision-making power** is neither fully decentralized nor fully transparent. Core developers, miners or validators, token holders, exchanges, and user communities exert varying degrees of influence depending on the issue at stake. Informal practices often dominate, creating tensions between decentralization ideals and actual power dynamics. This has led to the emergence of "blockchain constitutionalism," in which both formal rules (on-chain protocols) and a material constitution (off-chain norms and social consensus) interact to shape outcomes. Governance thus emerges as a dynamic and polycentric process in which authority is continuously negotiated among stakeholders.

■ Blockchain governance operates along a spectrum defined by the locus of authority: ***On-chain* mechanisms** embed decision making directly in code, using smart contracts, token-based voting, or automated protocols. ***Off-chain* mechanisms** rely on social coordination, informal debate, and human judgment outside the blockchain. Most networks employ a hybrid model, combining both approaches, revealing that even highly automated systems depend on human coordination to function effectively.

■ In **off-chain governance,** key actors —including foundations, core developers, and market participants— exert **substantial influence** despite blockchain's decentralized ethos. Foundations manage treasury funds, hire developers, fund research, and coordinate ecosystem development. Core developers hold technical authority, translating proposals into executable code and interpreting community consensus, often giving them effective veto power over protocol changes.

■ **On-chain governance** leverages blockchain technology to embed decision-making processes directly within protocols, promising automated, transparent, and verifiable execution of governance actions. Token-weighted voting, stake-based governance, and delegate-based mechanisms constitute the core methods through which stakeholders participate, with decisions executed automatically by smart contracts once thresholds are met.

■ Despite the benefits of automation and transparency, on-chain governance faces persistent challenges, since it creates **new avenues for power concentration**. Large stakeholders, or "whales," can dominate token-based voting; liquid staking and delegation systems tend to reinforce the advantages of early adopters or professional participants; and complex governance structures often impose technical barriers that prevent broader, effective participation. The deterministic execution of smart contracts introduces rigidity, limiting adaptability in the face of rapidly changing circumstances and crises. Transparency can also generate social pressures, herding effects, and incentivized voting behaviors, such as vote buying or governance bribery, that distort decision making. Emergency powers, rage-quit mechanisms, and veto rights provide partial safeguards but create trade-offs between decentralization and protocol security. As a result, on-chain governance does not fully eliminate the influence of off-chain human actors.

■ Case studies of major blockchains illustrate these tensions. **Bitcoin** demonstrates the tension between open participation and the concentration of power among a small number of maintainers. **Ethereum** balances formalized processes, such as Ethereum Improvement Proposals (EIPs), with informal developer influence and technical expertise often translating into disproportionate control. Other networks reveal patterns of initial centralization via foundations or corporate entities. Across all networks, governance is **polycentric**, contested, and constantly negotiated, highlighting the persistent tension between decentralization ideals and operational realities.

■ Overall, decentralization in blockchain systems is often more advanced at the technical level than at the political level. ***Technical decentralization*** refers to distributed network architectures, characterized by multiple nodes, permissionless or open consensus mechanisms, and resilience to single points of failure. ***Political decentralization***, by contrast, concerns who exercises authority over protocol evolution, including decisions about upgrades, rule changes, and governance processes. In practice, decision-making power is frequently concentrated among a relatively small set of actors, such as core developers, validators or miners, and large token holders. As a result, systems that are technically decentralized may nonetheless exhibit significant degrees of political centralization.

■ Overall, blockchains are only imperfectly decentralized and risk replicating **oligarchic structures** under the guise of openness. Yet concentration of power may also facilitate coordination, align incentives, and improve responsiveness, particularly in contexts where participation is uneven or expertise is limited. Market dynamics—especially the trading of governance tokens—can further discipline key actors by linking governance decisions to market valuation and user confidence.

CHAPTER 4

Use Cases

CHAPTER 4 TABLE OF CONTENTS

CHAPTER 4. USE CASES **127**
4.1. Payments and Remittances 129
4.2. Tokenization and DeFi 130
4.2.1. The Emergence of Coin and Token-Based Fundraising 130
4.2.2. Tokenization 133
4.2.3. Decentralized Finance (DeFi) 134
4.3. Recordkeeping 135
4.3.1. Government and Public Record 136
4.3.2. Land Registries 137
4.4. Data Sharing 138
4.5. Blockchain-Based Identities 140
4.5.1. Key Features of Blockchain-Based Identity 141
4.5.1.A. Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) 141
4.5.1.B. Technical Characteristics of Blockchain-Based Identities 142
4.5.1.C. Advantages and Disadvantages 142
1. Advantages 142
2. Disadvantages 143
4.5.2. Case Studies 144
4.5.2.A. Human Passport 144
4.5.2.B. World Network 145
4.5.2.C. Identity Overlay Network (ION) 147
4.5.2.D. Other Examples 148
4.6. Blockchain-Based Social Media 149
4.6.1. Alternative Social Media Architectures 149
4.6.1.A. Decentralized and Distributed Social Networks 149
1. Decentralized Social Networks 149
2. Distributed Social Networks 151
4.6.1.B. Key Features of Blockchain-Based Social Media 151
1. Controlling the Social Graph 151
2. Leveraging Blockchain Features 152
3. Advantages and Disadvantages 153
4.6.2. Examples 154
4.6.2.A. Lens Protocol 154
4.6.2.B. Steem 155
4.6.2.C. Farcaster 155
4.6.2.D. Decentralized Social Networking Protocol (DSNP) 157
1. Identity 158
2. Social Graph 158
3. Messaging 158
4.7. Blockchain-Based Dispute-Resolution (BDR) Mechanisms 159
4.8. Supply Chain 162
4.9. Decentralized AI 163
4.10. Network States 165
KEY TAKEAWAYS 168

CHAPTER 4
Use Cases

Blockchain technology is associated primarily with cryptocurrencies and speculative digital assets. Yet it has generated interest across diverse sectors seeking to address collective action challenges, reduce reliance on trusted intermediaries, and establish verifiable records in environments where traditional institutional mechanisms are costly, inaccessible, or inadequate.

This chapter surveys the principal and potential applications of blockchain beyond the buying and selling of cryptocurrencies. It examines other ways blockchain technology is being used today and the structural constraints on its uses. These applications include both end-users use cases and infrastructural layers that enable broader digital ecosystems. They span diverse domains — from payments and decentralized finance to government recordkeeping, identity verification systems, data sharing, social media, dispute resolution, supply-chain management, and emerging applications in artificial intelligence.

4.1. PAYMENTS AND REMITTANCES

One of the earliest and most widespread applications of blockchain technology is enabling the use of crypto-assets for buying and selling globally. Coins —digital assets native to a blockchain *(See above, 2.4.1.A.)*— were precisely designed to function as peer-to-peer payment instruments. Tokens can also be used for payments, but they typically represent various assets or utilities beyond simple currencies *(See above, 2.4.1.B.)*.

Since the launch of Bitcoin in 2009 amid a global financial crisis, blockchain systems have promised to enable peer-to-peer payments without the intermediation of banks and other middlemen. This aspiration has fueled the development of thousands of new cryptocurrencies intended to operate as an alternative to fiat currencies and other traditional media of exchange. Early examples include Litecoin and Bitcoin Cash, both "forks" of Bitcoin's codebase,[592] as well as Ether, the native currency of the Ethereum blockchain. Payment systems built on blockchain technology emphasize disintermediation. At the protocol level, users can transfer value directly across the network without relying on clearinghouses, correspondent banks, or financial messaging networks, such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT), even though practical use of cryptocurrencies often involves intermediaries, such as exchanges or payment processors. However, disintermediation at one layer may produce re-intermediation at another: In practice, most users access cryptocurrencies through exchanges, custodial wallet providers, payment processors, and stablecoin issuers. While blockchain reduces intermediation at the settlement layer, it does not eliminate intermediaries altogether.

592 See Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain chs. 1, 10 (2d ed. 2017) (detailing Bitcoin's launch in response to the 2008 banking crisis and the subsequent proliferation of alternative cryptocurrencies). https://archive.org/details/masteringbitcoin0000anto/page/n5/mode/2up.

Proponents also point to blockchain technology's global reach. The current global payments infrastructure is fragmented by country, language, and regulations. The high cost of global remittances is frequently cited as a compelling justification for blockchain as a better alternative.[593] Cryptocurrencies work across borders. And thanks to this capacity to make payments anywhere in the world, blockchain appears as a radically new form of payment infrastructure. With little more than a smartphone and an internet connection, individuals who have lacked access to banking services may find blockchain-based payments to be faster, simpler, and more accessible than traditional financial channels.[594] Today, cross borders payments do not rely on volatile cryptocurrencies, such as Bitcoin, but on stablecoins — blockchain-based tokens pegged to fiat currencies *(See section 2.4.1.C.)*. Stablecoins reintroduce reliance on centralized issuers, custodians of reserve assets, and regulatory compliance frameworks.

Cryptocurrencies have also attracted interest in countries facing severe macroeconomic instability. In contexts of hyperinflation, they may serve —at least in theory— as a partial hedge against currency depreciation.[595] In environments marked by authoritarian repression, some dissidents have turned to crypto-based payments as providing an alternative financial channel resistant to direct state control.[596] Yet public blockchains are transparent by design, and on- and off-ramps remain subject to regulation, surveillance, and control.

Overall, blockchain-based payment systems add the most value where participants require censorship resistance, cross-border interoperability, or programmable settlement —but their effectiveness depends heavily on surrounding regulatory, custodial, and liquidity infrastructures.

4.2. TOKENIZATION AND DEFI

Tokens have emerged as a foundational building block for new economic models. What began as a tool for project fundraising evolved into a broader reconfiguration of how assets are issued, represented, governed, and traded. This section traces that evolution —from Initial Coin Offerings (ICOs) and Security Token Offerings (STOs) to real-world asset tokenization and the growth of decentralized finance (DeFi).

4.2.1. The Emergence of Coin and Token-Based Fundraising

Token-based fundraising emerged in the mid-2010s as an innovative means of financing early-stage ventures, offering an alternative to traditional channels, such as venture capital or angel investment.[597] In an Initial Coin Offering (ICO), a project issues blockchain-based, cryptographically secured digital tokens to raise capital, rather than traditional equity or debt. The market expanded at extraordinary speed. In 2017 alone,

593 Friederike Rühmann et al., *Can Blockchain Technology Reduce the Cost of Remittances?* OECD Dev. Co-Operation Working Paper No. 73 (Apr. 21, 2020), https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/04/can-blockchain-technology-reduce-the-cost-of-remittances_2722776e/d4d6ac8f-en.pdf.

594 U.S. Dep't of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* 20, 42-43, (Sept. 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

595 *See generally* Usman W. Chohan, *Cryptocurrencies and Hyperinflation*, Critical Blockchain Research Initiative (CBRI) Working Papers (Mar. 21, 2021), https://ssrn.com/abstract=3320702.

596 Crypto payments are sometimes described as offering an "escape hatch from tyranny." Alex Gladstein, *Bitcoin is Protecting Human Rights Around the World,* Reason (Feb. 5, 2021), https://reason.com/video/2021/02/05/bitcoin-is-protecting-human-rights-around-the-world/.

597 Sabrina T. Howell, Marina Niessner & David Yermack, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, 2–3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 24774, 2018), https://www.nber.org/system/files/working_papers/w24774/w24774.pdf (subsequently published in 33 Rev. Fin. Stud. 3925 (2020)); *see also*: John M. Griffin & Amin Shams, *Coin-Operated Capitalism*, 75 J. Fin. 1937 2-3, 10 (2020) https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2019/02/Coin-operated-Capitalism.pdf.

blockchain startups and companies raised $4.6 billion.[598] Between January 2016 and August 2019, ICOs raised more than $31 billion, with over twenty individual offerings, each surpassing the $100 million mark.[599]

When well designed, ICOs offered the prospect of greater security, liquidity, and transparency than conventional forms of early-stage finance. This addressed, in part, the familiar problems of asymmetric information and agency costs that typically discourage retail participation in young ventures.[600] Tokens issued through ICOs were often tradable almost immediately on cryptocurrency exchanges, and participation was open to virtually anyone with an internet connection, regardless of geography. This broad accessibility effectively loosened the traditional dominance of venture capital firms and other financial intermediaries in early-stage funding. Moreover, the emergence of platforms such as Ethereum significantly simplified token creation and distribution. Launching an offering often required little more than deploying a smart contract and publishing a white paper, without the complex legal or administrative procedures associated with traditional fundraising.

ICOs loosened the traditional gatekeeping function of venture capital and investment banks and attracted both entrepreneurs and speculators seeking rapid capital formation and the possibility of high returns.[601] Yet this democratization of access occurred in a regulatory grey zone, where investor protections were weak and governance rights were often ambiguous. In many jurisdictions, ICOs were subject to limited or uncertain oversight. In this context, the success of ICOs was accompanied by significant controversy, as the ICO ecosystem quickly became associated with speculative excess, low-quality projects, and outright fraud.[602]

A substantial proportion of cryptocurrency offerings failed to deliver on their promises: Many devolved into scams, consisted of projects that never progressed beyond the white paper stage, or collapsed as underdeveloped ventures. The largely unregulated and decentralized structure of ICOs exposed investors to heightened risks of fraud, money laundering, and other systemic vulnerabilities —particularly where tokens functioned, in substance, as unregistered securities.[603] The lack of clear legal and corporate-governance frameworks further undermined accountability: Token holders often had uncertain rights, limited avenues for recourse, and few mechanisms to ensure responsible project management. These concerns led many legal and financial practitioners to view ICOs not merely as novel fundraising mechanisms but as a complex regulatory challenge.[604]

In response, more regulated models emerged. In 2018-2019, Security Token Offerings (STOs) —the issuance

598 PwC Strategy& & Crypto Valley Ass'n ., *Initial Coin Offerings: A Strategic Perspective: Global; and Switzerland* 1 (Dec. 21, 2017), https://cryptovalley.swiss/wp-content/uploads/20171221_PwC-S-CVA-ICO-Report_December_final.pdf.

599 *See* PwC Strategy& & Crypto Valley Ass'n., *6th ICO / STO Report: A Strategic Perspective*, STRATEGY& 3 (Spring 2020), https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

600 Sabrina T. Howell et al., *supra* note 597 at 26.

601 Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, 60 HARV. INT'L L.J. 267, 268-271 (2019), https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/3_ICO_60.2.pdf; *see also* Pablo de Andrés et al., *Regulatory and Market Challenges of Initial Coin Offerings*, (Eur. Corp. Governance Inst., Law Working Paper No. 461, 2019), https://www.ecgi.global/sites/default/files/working_papers/documents/final2andresarroyocorreiarezola_1.pdf.

602 Stéphane Blemus & Dominique Guégan, *Initial Crypto-asset Offerings (ICOs), Tokenization and Corporate Governance* (Eur. Corp. Gov.e Inst. Law Working Paper No. 455/2019, 2019), https://arxiv.org/abs/1905.03340.

603 Banque de France, *The Emergence of Bitcoin and Other Crypto-Assets: Challenges, Risks and Outlook*, Focus No. 16 3-5 (Mar. 5, 2018), https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_en.pdf.

604 Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism* 119 COLUM. L. REV. 591, 593–95 (2019), https://ssrn.com/abstract=3215345.

of tokens structured as investment contracts under existing securities laws[605]— emerged as a more regulated alternative to ICOs. STOs introduced more formal investor protections —typically including Know Your Customer (KYC) procedures and compliance with securities regulations. Around the same time, exchanges launched Initial Exchange Offerings (IEOs), in which token sales were conducted directly through platforms such as Binance Launchpad and Huobi Prime.[606] These exchanges provided vetting services and immediate trading liquidity.[607] Blockchain-based fundraising continued to evolve throughout 2019. Notable examples included Bitfinex's LEO tokens, which raised $1 billion,[608] and Blockstack, which secured $23 million through the first U.S. Securities and Exchange Commission-qualified token offering.[609] These fundraising mechanisms attracted both retail and institutional investors seeking exposure to blockchain-driven innovation.

By late 2020, the popularity of token-based fundraising had declined sharply as returns diminished, regulatory scrutiny intensified *(See section 7.2.2.)*, and market confidence waned.[610] In this context, new categories of tokens emerged, shifting focus from pure fundraising to governance and utility within decentralized finance protocols.[611] Projects such as Compound, Aave, and Uniswap distributed tokens that provided governance rights and fee-sharing mechanisms, rather than acting as purely speculative assets.[612] At the same time, Decentralized Autonomous Organizations (DAOs) emerged as alternative funding structures: Projects raised capital through DAO treasuries and governance token distributions, while attempting to decentralize key operations to mitigate regulatory exposure.[613]

Token-based fundraising volumes surged again during the 2021 bull market, exceeding $25 billion (including venture capital, NFT sales, token launches),[614] but then contracted sharply during the 2022 downturn.[615] By 2023–2024, activity had shifted toward more mature models, emphasizing regulatory compliance and tokens that performed concrete operational or governance functions within blockchain protocols.[616]

---

605 *See* Thomas Lambert, Daniel Liebau & Peter Roosenboom, *Security Token Offerings*, 59 Small Bus. Econ. 299, 300 (2022), https://doi.org/10.1007/s11187-021-00539-9; Dafan Zhang, *Security Tokens: Complying with Security Laws and Regulations Provides More than Token Rewards*, 88 UMKC L. Rev. 10 (2019), https://umkclawreview.org/wp-content/uploads/2019/03/zhang-2019-1.pdf.

606 *See What is an IEO?* CoinMarketCap Academy, https://coinmarketcap.com/academy/article/what-is-an-ieo (last visited Jan. 15, 2026); Guneet Kaur, *IEO 101: A Beginner's Guide to an Exchange Administered Fundraising Event*, Superex (Jan. 16, 2024) https://x.Superex.com/Academys/Beginner/2717/.

607 *What is an IEO?,* see *supra* note 606.

608 Yogita Khatri, *Bitfinex's Private Token Sale Raised $1 Billion in 10 Days, Exec Says*, CoinDesk (Sept. 13, 2021), https://www.coindesk.com/markets/2019/05/13/bitfinexs-private-token-sale-raised-1-billion-in-10-days-exec-says/.

609 Nikhilesh De, *Blockstack's Regulated Token Offerings Raise $ 23 Million*, CoinDesk (Sept. 13, 2021), https://www.coindesk.com/markets/2019/09/10/blockstacks-regulated-token-offerings-raise-23-million.

610 *See* Anja van Oosterhout, *ICOs 'Will Disappear in 2020' As Data Shows 95% Funding Decline*, Bitcoinist, https://bitcoinist.com/icos-will-disappear-in-2020-as-data-shows-95-funding-decline/, (last visited Jan. 15, 2026).

611*What Are Governance Tokens?*, Binance Academy, (Sept. 29, 2022) https://academy.binance.com/en/articles/what-are-governance-tokens*; See generally* Campbell R. Harvey, Ashwin Ramachandran & Joey Santoro, DeFi and The Future of Finance (2021); *See* also Yunji Sun & Sung-Byung Yang, *Are ICOs the Best? A Comparison of Different Fundraising Models in Blockchain-Based Fundraising,* 73 J. Fin. Stability 101288 (2024), https://doi.org/10.1016/j.jfs.2024.101288.

612 *Id.*

613 *See* Saqib Sheikh et al., *Built to Last, Not to Scale: The Long Run of Decentralised Autonomous Organisations*, 2, 8, 17, 18 (Jan. 22, 2023), ssrn.com/abstract=4335053; 9 J. Innovation & Knowledge 100513 (2024) https://doi.org/10.1016/j.jik.2024.100513.

614 *See* Brayden Lindrea, *Crypto Fundraising Hits $30.3B in H1, Outpacing All of 2021: Report*, CoinTelegraph (Aug. 5, 2022), https://cointelegraph.com/news/crypto-fundraising-already-outpacing-all-of-2021-report.

615 *See* Arjun Kharpal et al., *This 'crypto Winter' Is Unlike Any Downturn in the History of Digital Currencies. Here's Why*, CNBC (July 14, 2002), https://www.cnbc.com/2022/07/14/why-the-2022-crypto-winter-is-unlike-previous-bear-markets.html.

616 *See* Lana Schwartzman, *Embracing Evolution: Crypto Compliance in Review and a Vision for 2024*, NotaBene (Jan. 4, 2024), https://notabene.id/post/embracing-evolution-crypto-compliance-in-review-and-a-vision-for-2024#:~:text=Regulatory%20Maturity%20and%20Global%20Alignment,to%20support%20various%20use%20cases; *see also* Barry Elad, *Cryptocurrency Regulations Impact Statistics 2025: Regulatory Changes and Economic Impacts*, Coin Law (Mar. 30, 2025), https://coinlaw.io/cryptocurrency-regulations-impact-statistics/?utm_source.

4.2.2. Tokenization

"Tokenization" refers to the process of creating a blockchain-based digital token that represents ownership or other rights associated with an underlying asset.[617] The asset may be tangible (such as real estate, commodities, or works of art) or intangible (such as intellectual property, carbon credits, or governance rights).[618]

By representing these rights on a distributed ledger, tokenization enables their storage, transfer, and management in a secure and interoperable digital environment. It also allows these rights to be divided into smaller units, thereby improving the accessibility and liquidity of assets that are typically difficult to divide or trade. Through smart contracts, certain rules, rights, and functional features can be embedded directly into the token, allowing for varying degrees of automated execution and compliance. Overall, this architecture enhances transparency and auditability in ownership and transactions.

While the term "tokenization" is widely used, it encompasses two distinct paradigms that rely on different technical and governance assumptions.

- **Public chain tokenization.** On public blockchains, tokenization refers to the representation of rights or assets on permissionless blockchains, where tokens function as natively digital bearer instruments, and smart contracts embed rules governing transfer, use, and ownership.[619]
- **Institutional or permissioned tokenization**. Financial institutions and market infrastructures employ "tokenization" to describe the digital representation of traditional assets within permissioned distributed-ledger environments.[620] In these systems, the token functions as an institutional record, rather than a standalone on-chain asset, and automation is limited to processes permitted within established regulatory frameworks.

The rise of token-based fundraising in 2016–2017 marked the first mainstream wave of tokenization. Over time, attention has moved away from utility tokens —digital tokens that grant users access to a service or functionality within a blockchain platform— toward the tokenization of real-world assets (RWAs), including real estate, art, securities, commodities, and financial instruments. This trend accelerated with the emergence of decentralized finance (DeFi) protocols, which applied tokenization to financial services and introduced liquidity models that did not rely exclusively on traditional intermediaries.

By mid-2025, major financial institutions, such as BlackRock, JPMorgan, and Goldman Sachs, launched tokenization initiatives for assets including U.S. Treasury Bills and money market funds (MMFs), signaling the technology's growing integration into traditional finance.[621] The market now includes money market

617 Mary C. Lacity & Horst Treiblmaier, eds., Blockchains and the Token Economy: Theory and Practice 45 (2022); Anutosh Banerjee et al., *From Ripples to Waves: The Transformational Power of Tokenizing Assets*, McKinsey & Co. (June 20, 2024), https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets; Piero Cipollone, *Tokenisation and the Future of Finance: The Role of Central Bank Money*, slides at the Cent. Bank of Ir.'s Fin. Sys. Conference 2 (Nov. 25, 2025), https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp251125~754585ec10.en.pdf

618 World Econ. Forum, *Asset Tokenization in Financial Markets: The Next Generation of Value Exchange* (May 2025), https://reports.weforum.org/docs/WEF_Asset_Tokenization_in_Financial_Markets_2025.pdf; OECD, *Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets: Potential Impediments to Market Development and Policy Implications*, OECD Bus. & Fin. Pol'y Papers No. 75 (Jan. 2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_be149012/40e7f217-en.pdf.

619 *See* McKinsey & Co, *What Is Tokenization?* McKinsey Explainers (July 25, 2024), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization

620 Eur. Cent. Bank, *Tokenisation in Money Markets* 2 (Money Mkt. Contact Grp., Item 3, Sept. 18, 2024), https://www.ecb.europa.eu/paym/groups/pdf/mmcg/20240918/20240918_MMCG_Item3_Tokenisation_in_money_markets.pdf

621 Nicholas Barbaroux, Claire Brousse & Déborah Zribi, *Tokenised money market funds: what are the implications for financial stability?*, Banque de France (July 1, 2025), https://www.banque-france.fr/en/news/tokenised-money-market-funds-what-are-implications-financial-stability; *see also* Francesca Carapella et al., *Tokenization: Overview and Financial Stability Implications* 17-18 (Fin. & Econ. Discussion Series 2023-060r1 (Bd. of Governors of the Fed. Rsrv. Sys., Sept. 2023), , https://doi.org/10.17016/FEDS.2023.060r1.

funds, private credit, and repurchase agreements.[622] Institutions are increasingly embedding tokenization into legacy infrastructure to unlock liquidity, enhance interoperability across on-chain systems, and streamline settlement workflows.[623] The growth of collateralized MMFs in DeFi illustrates how tokenization is contributing to new liquidity mechanisms and the packaging of familiar financial instruments in on-chain formats.[624] Notably, many of these initiatives rely on public blockchains such as Ethereum and Solana. Examples include BlackRock's tokenized Money Market Fund BUIDL and Etherfuse's tokenized CETES.[625]

In particular, the tokenization of real-world assets introduces new pathways to generate liquidity independent of centralized moneymakers, especially in DeFi, by reducing some of the costs and frictions associated with traditional intermediaries, even though many functions remain performed by centralized actors.[626] Analysts at McKinsey & Co. forecast a "base case" of $2 trillion and "bullish scenario" of $4 trillion in tokenized digital securities could be issued by 2030, reflecting a broader shift from simple digital representations of value to the on-chain issuance and management of complex real-world assets.[627] Tokenization nonetheless faces a number of technological, legal, and regulatory hurdles, as well as financial-stability concerns that may constrain its evolution.[628]

4.2.3. Decentralized Finance (DeFi)

Decentralized Finance (DeFi) refers to a financial ecosystem built on blockchain technology in which key financial services are provided through smart contracts rather than through traditional intermediaries, such as banks, brokers, dealers, custodians, transfer agents, or clearinghouses. DeFi protocols replicate and extend functions such as lending, borrowing, trading, hedging, and asset management by replacing institutional infrastructure with open, programmable, and publicly verifiable code.[629] The core appeal lies in having a universal ledger that natively integrates payments, tokenized assets, and interoperable financial applications— such as exchanges and lending markets— allowing new services to emerge without centralized coordination. In essence, DeFi offers a shift from a closed, intermediary-based financial system to one where access is open, transactions are executed automatically by code, and financial services can be designed to interact and be used together across different applications.[630]

The main characteristics of DeFi include:

Permissionless access: DeFi is fundamentally open and permissionless, with users having self-custody of their own assets and transacting directly with counterparties, instead of operating through government-regulated intermediaries. Anyone with an internet connection and a cryptocurrency wallet can access DeFi services without needing approval from a central authority.

622 Anutosh Banerjee, *supra* note 617.

623 *Id.*

624 *Ethena Launches USDtb Stablecoin Backed by BlackRock's $500M BUIDL Fund To Reduce USDe Risks,* CoinMarketCap (June 27, 2025), https://coinmarketcap.com/academy/article/ethena-launches-usdtb-stablecoin-backed-by-blackrocks-dollar500m-buidl-fund-to-reduce-usde-risks.

625 Francisco Rodrigues & Krisztian Sandor, *BlackRock, Securitize Expand $1.7B Tokenized Money Market Fund BUIDL to Solana,* CoinDesk (Mar. 25, 2025), https://www.coindesk.com/markets/2025/03/25/blackrock-securitize-expand-usd1-7b-tokenized-money-market-fund-buidl-to-solana.

626 *Real-World Assets (RWAs) Explained*, Chainlink, https://chain.link/education-hub/real-world-assets-rwas-explained (last visited Jan. 15, 2026).

627 *From Ripples to Waves: The Transformational Power of Tokenizing Assets*, McKinsey (June 19, 2024), https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets.

628 Francesca Carapella et al., *supra* note 621, at 7-9.

629 Int'l Org. of Sec. Comm'ns (IOSCO), Final report with Policy Recommendations for Decentralized Finance (DeFi) 1, 6 (Dec. 2023), https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf.

630 Fabiar Schär, *DeFi's Promise and Pitfalls,* IMF (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/Defi-promise-and-pitfalls-Fabian-Schar.

Transparency: All transactions, balances, and smart contract code are publicly visible and auditable on the blockchain.

Interoperability: DeFi applications are designed to interact with one another, enabling modular or "building-block" financial services that can be combined or extended across protocols.

Self-custody: Users maintain direct control over their digital assets through private keys, eliminating the need to entrust assets to custodians or other third parties.

Each feature introduces corresponding trade-offs. Permissionless access complicates AML/KYC compliance. Transparency enhances auditability but exposes transaction data. Interoperability accelerates innovation but creates contagion risks across tightly coupled protocols. Self-custody reduces custodial risk but shifts responsibility and loss risk to users.

DeFi applications allow users to trade cryptocurrencies without intermediaries (e.g., Uniswap, Curve);[631] provide lending and borrowing platforms where users can supply assets to earn interest or take out over-collateralized loans (e.g., Aave, Compound);[632] enable synthetic asset protocols that issue on-chain instruments designed to track the value of real-world assets such as equities, commodities, or fiat currencies (e.g., Synthetix, MakerDAO's DAI mechanism);[633] and include risk-mitigation or insurance protocols that provide coverage against smart contract exploits or operational failures (e.g., Nexus Mutual).[634] Among the most common DeFi applications are decentralized exchanges (DEXs). Unlike centralized exchanges (CEXs), which hold customer funds in custody and operate as regulated intermediaries, DEXs execute trades directly between users through smart contracts, without taking custody of assets.

Despite its benefits —such as increased financial inclusion, reduced barriers to entry, and continuous innovation— DeFi also entails significant risks. Smart-contract vulnerabilities and operational failures can lead to substantial losses *(See section 6.2.)*, and the extreme volatility of crypto-asset prices *(See section 5.1.1.A.)* can undermine the stability of lending markets and collateralized positions. In addition, the legal and regulatory statuses of many DeFi activities remain uncertain, raising challenges for investor protection and market integrity. Finally, the permissionless nature of DeFi, while facilitating openness and accessibility, also heightens concerns related to AML/KYC compliance[635] and the potential for systemic risks arising from interlinked protocols, liquidity shocks, or oracle failures.

4.3. RECORDKEEPING

Recordkeeping is a fundamental component of information governance in both the public and private sectors. Traditional systems often rely on centralized databases, which can be vulnerable to manipulation, single points of failure, or administrative errors. Blockchain technology offers a decentralized approach that can enhance the integrity, authenticity, and auditability of records by providing tamper-evident logs, verifiable timestamps, and transparent provenance trails.

631 Angelo Aspris, Sean Foley, Jiri Svec & Leqi Wang, *Decentralized Exchanges: The "Wild West" of Cryptocurrency Trading*, 77 Int'l Rev. Fin. Analysis 1, 1 (2021), https://www.sciencedirect.com/science/article/pii/S1057521921001782.

632 *See* Rakesh Sharma, *Understanding Decentralized Finance (DeFi): Basics and Functionality* , Investopedia (Aug. 31, 2025), https://www.investopedia.com/decentralized-finance-defi-5113835.

633 *What is a Synthetic Asset? Digital Assets That Mirror Real-World Value*, CoinTracker, https://www.cointracker.io/learn/synthetic-asset (last visited Jan. 15, 2026).

634 *What is DeFi?*, CoinBase, https://www.coinbase.com/public-policy/advocacy/documents/what-is-defi (last visited Jan. 15, 2026).

635 AML/KYC compliance refers to legal obligations requiring financial institutions to verify customer identities (Know-Your-Customer, or KYC) and monitor transactions to prevent money laundering and terrorist financing (Anti-Money-Laundering, or AML).

While public-sector interest is strong, most initiatives remain at the pilot stage, and large-scale adoption raises legal, technical, and cost-related challenges.

4.3.1. Government and Public Record

In the United States, various states have been early adopters. In 2019, for instance, Illinois enacted the Blockchain Technology Act,[636] which grants legal validity to blockchain-based records and smart contracts, although it does not mandate their use across state agencies. To date, pilot projects under the Illinois law have shown technical feasibility, but vital records such as birth certificates have not yet been migrated onto blockchain systems. California has moved further in operationalizing blockchain for vehicle-title management. In mid-2024, the California Department of Motor Vehicles partnered with Oxhead Alpha and Ava Labs to tokenize vehicle titles using the Avalanche blockchain.[637] While public announcements refer to the digitization of "42 million" titles, this figure reflects the migration of the DMV's title database to a blockchain-enabled infrastructure rather than the minting of millions of individual tokenized titles at once.[638] The initiative provides a blockchain-anchored record of ownership and enables residents to manage title transfers and related transactions through a mobile application. The program aims to create a transparent and tamper-evident record of ownership, reduce lien fraud, improve traceability, and simplify title issuance and transfer processes.[639]

Brazil has integrated blockchain into its notarial system through e-Notariado, a digital platform developed by the Notarial College of Brazil–Federal Council (CNB-CF). The system allows notarial offices to issue and manage digital acts while ensuring the authenticity and integrity of documents through a permissioned blockchain infrastructure.[640] Applicants no longer need to schedule in-person visits to register, notarize, or validate legal documents, as these procedures can be carried out remotely on the platform. Each notarial act is recorded by generating a unique hash stored on the blockchain, creating a tamper-evident proof of the document's existence and content at the time of issuance.[641] The extrajudicial documents produced through e-Notariado have been formally recognized by Brazil's National Council of Justice as legally equivalent to those generated through traditional manual procedures.[642]

In Europe, Malta adopted a blockchain-based academic credentialing system in 2017. This system enables educational institutions to issue tamper-evident credentials and allows employers or other institutions to verify them without relying on paper documents or centralized databases.[643]

636 Illinois Blockchain Technology Act, 205 Ill. Comp. Stat. Ann. 730/1–730/20 (West 2020).

637 *California DMV Makes History, Digitizes 42 Million Car Titles on Avalanche Blockchain*, Avalanche Blog (July 30, 2024), https://www.avax.network/about/blog/california-dmv-makes-history-digitizes-42-million-car-titles-on-avalanche-blockchain?utm_source=tldrcrypto

638 *California DMV Puts 42M Car Titles on the Avalanche Network in Digitization Push*, CoinDesk (July 30, 2024), https://www.coindesk.com/business/2024/07/30/california-dmv-puts-42m-car-titles-on-the-avalanche-network-in-digitization-push/.

639 Akash Sriram, *California DMV puts 42 million car titles on blockchain to fight fraud*, Reuters, https://www.reuters.com/technology/california-dmv-puts-42-million-car-titles-blockchain-fight-fraud-2024-07-30/ (last visited Jan. 15, 2026)

640 Cassio Gusson, *Brazil already has more than 8,000 Living Wills registered on the Hyperledger blockchain*, CoinTelegraph, https://br.cointelegraph.com/news/brazil-already-has-more-than-8-thousand-living-wills-registered-on-blockchain-on-hyperledger (last visited Jan. 15, 2026)

641 *See* Provimento No. 100, de 26 de Maio de 2020, Conselho Nacional de Justiça [C.N.J.] (Braz.) (establishing the «e-Notariado» system and verifying the authenticity of digital notarial acts via the Notarchain permissioned ledger); Giovanna Fantinato, *Brazil has already authenticated 156,000 documents with blockchain,* Tecmundo, https://www.tecmundo.com.br/internet/214841-blockchain-156-mil-documentos-autenticados-tecnologia.htm (last visited Jan. 15, 2026)

642 Bruno Andrioli, *Blockchain and its applicability in the legal universe*, Migalhas https://www.migalhas.com.br/depeso/379019/blockchain-e-sua-aplicabilidade-no-universo-juridico (last visited Jan. 15, 2026)

643 David Allessie, Maciej Sobolewski & Lorenzino Vaccari, *Blockchain for digital government*, Eur. Comm'n, https://interoperable-europe.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (last visited Jan. 15, 2026).

4.3.2. Land Registries

Several jurisdictions have experimented with, or implemented, blockchain-based systems for securing land and property records. These initiatives generally aim to reduce fraud and enable more reliable verification of ownership records by providing tamper-evident logs of transactions. While most projects remain at the pilot stage, a few have progressed toward operational deployment.

The Republic of Georgia is among the most prominent examples. Since 2016, its National Agency of Public Registry (NAPR) has operated a blockchain-enabled system developed in partnership with the Bitfury Group and the Blockchain Trust Accelerator.[644] The user-facing land registry did not change, but every new land transaction or ownership record now produces a cryptographic "fingerprint" that is stored on a blockchain. Georgia uses a private (permissioned) Exonum-based ledger[645] for fast and secure recordkeeping and periodically anchors a hash of this ledger onto the public Bitcoin blockchain to create an immutable timestamp. This hybrid model combines the speed and privacy of a private ledger with the auditability of a public blockchain. Citizens can verify, through NAPR's web or mobile portal, that the hash of their title extract corresponds to the hash stored on the blockchain, thereby ensuring that the underlying record has not been altered. Over time, the system has expanded beyond land titles to cover property transfers, demolitions, mortgage registrations, rental agreements, and certain notarial services.[646]

Dubai represents another significant initiative. As part of the "Dubai Blockchain Strategy," the Dubai Land Department (DLD) operates a blockchain built on a permissioned ledger which records property-ownership data, leasing contracts, and selected real-estate transactions.[647] Although it is not decentralized in the sense of a public blockchain, the system uses blockchain features to authenticate documents, streamline the verification of property information, and enable secure data-sharing among government entities and approved private-sector partners. The system is operational and reflects a broader strategy to digitize real-estate services and reduce administrative friction.

Sweden has explored blockchain for real-estate transactions. In 2016, the Swedish mapping and land registry authority (Lantmäteriet) conducted a pilot project with private partners to test blockchain-based "immutable storage" for digitizing the workflow of real-estate sales.[648] The pilot demonstrated technical feasibility but faced legal barriers —particularly the prohibition of digital signatures for completing property transfers under Swedish law[649]— as well as interoperability challenges for IT systems of government bodies and resistance from brokers.[650] As a result, the project did not progress beyond the proof-of-concept phase.[651]

644 Bitfury Group, *The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project*, Bitfury Press Release (Feb. 7, 2016), https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf; see *also*: Mitchell Weiss & Elena Corsi, *Bitfury: Blockchain for Government*, Harv. Bus. Sch. Case 818-031 (2017).

645 Exonum is a permissioned blockchain framework developed by Bitfury that allows governments and institutions to run fast, private ledgers while anchoring cryptographic hashes to a public blockchain (e.g., Bitcoin) for external auditability. Bitfury Group, *Bitfury Group Announces Launch of Exonum: Exclusive Open Source Enterprise-Grade Blockchain Framework*, Bitfury Press Release (July 17, 2017), https://bitfury.com/content/downloads/7_17_17_bitfury_announces_exonum.pdf.

646 Weiss & Corsi, *supra* note 644.

647 *See DLD Launches Innovative Property Token Ownership Certificate*, Finance World Mag. (May 30, 2025), https://thefinanceworld.com/dld-launches-innovative-property-token-ownership-certificate/.

648 Lantmäteriet et al., *The Land Registry in the Blockchain*, 5 (Project Report, 2016), https://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf (concluding that while the blockchain solution was secure, widespread adoption required legislative changes to accept digital signatures for real estate conveyance);

649 *Id.*; *see also* Molly Jane Zuckerman, *Swedish Government Land Registry Soon to Conduct First Blockchain Property Transaction*, Cointelegraph (Mar. 7, 2018), https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction

650 Anastasiia Proskurovska & Sabine Dörry, *The Blockchain Challenge for Sweden's Housing and Mortgage Markets*, 54 Env't & Plan. A: Econ. & Space 1569-85 (2022), https://ideas.repec.org/a/sae/envira/v54y2022i8p1569-1585.html.

651 Anetta Proskurovska, *Re-inventing housing finance with blockchain, The case of Sweden*, 147 Geoforum (preprint version 2023), https://www.sciencedirect.com/science/article/abs/pii/S0016718523002105.

India's National Blockchain Framework includes a permissioned chain dedicated to land registration which has currently piloted in the states of Telangana, Goa, and Maharashtra, with the objective of producing tamper-resistant title records capable of reducing fraudulent conveyances and evidentiary disputes in property transactions *(See Appendix 21)*.

4.4. DATA SHARING

Data sharing refers to the practice of making data accessible for use by individuals, organizations, or technological systems across different domains. Data sharing is critical to innovation because it enables the combination, comparison, and large-scale analysis of datasets across institutions. In so doing, it improves model development, accelerates discovery, and supports the creation of new products, services, and scientific insights. In this context, organizations are increasingly motivated to dismantle data silos[652] and improve interoperability to generate greater analytical value, improve operational processes, and exploit the economic value of data through commercialization and other forms of valorization.

Yet data sharing raises complex coordination and governance challenges, particularly in relation to privacy risks and cybersecurity threats. The protection of user privacy has become a central concern, given the unprecedented volume of personal information now being generated and exchanged, ranging from sensitive medical records to detailed financial transactions. In the absence of robust security measures, data transfers and storage systems expose individuals and organizations to the risk of large-scale breaches with severe consequences. Once such a breach occurs, personal information —including identity credentials and authentication data— may be compromised.[653] The increasing automation of data collection, storage, and dissemination further intensifies these risks, underscoring the need for clearly defined access rights, robust technical safeguards, and continuous monitoring of system vulnerabilities.

Traditional data-sharing models typically rely on centralized repositories, third-party data centers, standardized exchange protocols, or replicated databases.[654] While these approaches enable interoperability, they often leave data owners or controllers with limited visibility into downstream use. Control over how long data are retained, how they are reused, or whether they are modified may be fragmented or opaque.[655] In multi-party environments, reconciliation across institutions can be costly and error-prone.

Blockchain-based architectures offer an alternative design. Rather than storing raw data directly on a distributed ledger, most systems separate storage from verification. The data is kept in an off-chain storage system in encrypted form, while the blockchain records only cryptographic hashes or metadata that attest to the data's integrity and provenance.[656] This design allows

652 A common barrier to effective data sharing is the persistence of data silos, which occur when information is stored in isolated systems controlled by different entities. Such silos may result from (1) technical incompatibilities, including outdated IT infrastructures or paper-based records requiring manual processing, (2) regulatory requirements that restrict access to specific categories of data, or (3) economic disincentives, such as the unwillingness of competitors to share commercially valuable information. See OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, 92-98 (Nov. 26, 2019), https://doi.org/10.1787/276aaca8-en; Noman Yaqub et al., *Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records*, 11 PeerJ Computer Sci. art. e2647 (Jan. 23, 2025), https://doi.org/10.7717/peerj-cs.2647; Hongmin Gao et al., *Blockchain-enabled supervised secure data sharing and delegation scheme in Web3.0.*, 13(21) J. Cloud Computing 21 (Jan. 22, 2024), https://doi.org/10.1186/s13677-023-00575-8.

653 Noman Yaqub et al., *Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records*, 11 PeerJ Computer Sci. art. e2647 6-7 (Jan. 23, 2025), https://doi.org/10.7717/peerj-cs.2647

654 Shuai Wang & Jia Liu, *Blockchain based Secure Data Sharing Model*, 2021 IEEE 24th Int'l Conf. on Computer Supported Coop. Work in Design (2021), 464-469, https://ieeexplore.ieee.org/document/9437751.

655 Sandra Kumi, Richard Lomotey & Ralph Deters, *A Blockchain-Based Platform for Data Management and Sharing*, 203 Procedia Computer Sci. 95-102 (2022), https://doi.org/10.1016/j.procs.2022.07.014..

656 Wang & Liu, *supra* note 654 at 467.

participants to verify that data have not been altered without exposing the underlying content. By design, blockchain can support mechanisms that enhance user-centric data governance, ensure data portability, and enable the development of open architectures that protect individual privacy by anchoring verification on a shared, tamper-evident ledger.[657]

Smart contracts can encode data-sharing rules directly into programmable logic and automatically enforce the agreed rules of access. Access is typically granted according to permissions that the user has predefined or approved, rather than through repeated explicit consent for every request. Users retain the ability to authorize or deny access to their data using private cryptographic keys. They may hold these encryption keys directly or have them managed through user-approved intermediaries, depending on the design. This model ensures transparency, preserves data integrity, and provides users with effective control over how, when, and by whom their data is used, while generating auditable records of access events.[658]

Blockchain-based data-sharing systems provide several concrete advantages, including the streamlining of information exchange, the reduction of reconciliation errors, and potentially lowering operational costs. Smart contracts automate fine-grained access control,[659] minimizing administrative burdens and improving the efficiency of data sharing. Token mechanisms can incentivize participants to share and update data.[660] The immutability of blockchain ensures data integrity, while time-stamped records create an auditable history of provenance and data-access events. Cryptographic techniques protect user privacy and enable secure management of data access rights.[661]

However, blockchain does not eliminate all data-sharing risks. It cannot guarantee the accuracy of data at the point of entry, nor can it resolve disputes regarding ownership, liability, or regulatory compliance. The so-called "oracle problem"[662] — the difficulty of verifying off-chain inputs — remains central in blockchain-based data-sharing systems. Legal frameworks — including sector-specific rules and instruments such as the EU Data Act *(See section 7.3.3.A.)* — remain decisive in determining who may access, modify, or commercialize shared information. Blockchain can enhance transparency and integrity, but it cannot substitute for clear governance structures or enforceable legal rights.

In practice, blockchain-based data-sharing systems are most compelling where multiple partially trusted actors require a shared, tamper-evident record of data access and provenance. Current examples include the sharing of health data *(See Appendix 7)*, insurance claim settlement, and IP management. However, most of these examples are not truly decentralized and instead operate within permissioned or consortium-based governance structures. Moreover, where a single trusted authority already exists and performs these functions efficiently, conventional database architectures may suffice.

657 Yaqub et al., *supra* note 653, at 6, 24 (arguing that traditional centralized systems provide patients with "limited control" and proposing a decentralized blockchain architecture that "empower[s] stakeholders like patients with more control," specifically by utilizing smart contracts that allow users to dynamically grant, revoke, or audit access to their sensitive records in real-time).

658 For a discussion on Policy-Based Access Control (PBAC) and how smart contracts can be utilized to dynamically enforce these user defined access permissions, see Yaqub *supra* note 654 at 8.

659 Yaqub et al., *supra* note 653, at 14-23.

660 Thanh Linh Nguyen et al., *Blockchain-Empowered Trustworthy Data Sharing: Fundamentals, Applications, and Challenges* (Mar. 12, 2023) (unpublished manuscript) 1 ARXIV, https://arxiv.org/abs/2303.06546.

661 Umair Ullah Tariq et al., *Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review*, 13 IEEE ACCESS 45415, 45421 (2025), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10909514.

662 *Can Artificial Intelligence Solve the Blockchain Oracle Problem?*, 3 Frontiers in Blockchain (2025), https://www.frontiersin.org/articles/10.3389/fbloc.2025.1682623

4.5. BLOCKCHAIN-BASED IDENTITIES

The state has traditionally served as the guarantor of identity by verifying personal details, such as name, gender, date of birth, and residence, and issuing official documents, such as passports, birth certificates, and driver's licenses. By contrast, digital environments have relied on their own distinct mechanisms of verification. From the outset, devices connected to the internet have incorporated technical markers, such as IP addresses, that allow for a limited form of user identification.

As online transactions have expanded, service providers have developed more sophisticated and centralized systems of digital identity management. They assigned "identifiers" to users —whether tied to their legal identity or to a pseudonym— and linked these identifiers to personal data. To complete an online purchase, for example, users typically register on a platform and provide information such as their name, address, contact details, financial data, or even biometric information for facial recognition. These systems typically involve several layers: identity proofing, credential issuance, and authentication through passwords, verification codes, or biometric checks.

Digital identity systems generally depend on trusted third parties to establish identification procedures, issue identifiers, and authenticate users through credentials such as passwords or verification codes. Major technology companies such as Apple, Google, and Facebook have assumed this role by offering single sign-on (SSO) services that allow individuals to access multiple platforms with a single set of credentials. This reliance on intermediaries generates significant risks: Users may become dependent on dominant platforms which control their accounts and can use identity management as a means to collect personal data and monitor online activity.[663] Vast quantities of sensitive information are, therefore, concentrated in private hands, and the security of this sensitive data is not guaranteed, as data breaches and identity theft remain persistent concerns.[664]

At its core, digital identity raises various questions: How can individuals prove who they are, or demonstrate specific attributes (such as age, qualifications, or authorization), across multiple services without repeatedly disclosing significant personal data and without relying on a single dominant intermediary? Blockchain-based identity initiatives seek to address this problem by enabling verifiable claims to circulate across networks while limiting data concentration and platform dependency. While "self-sovereign identity" (SSI) does not inherently require blockchain, many SSI initiatives use blockchain infrastructures to anchor identifiers (such as decentralized identifiers, or DIDs), manage credential schemas, or record revocation registries.[665] These blockchain-based approaches seek to reduce reliance on centralized intermediaries, enhance security, and give users greater control over how their credentials are stored and shared.[666]

663 Christopher Allen, *The Path to Self Sovereign Identity*, Life with Alacrity (Apr. 16, 2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

664 Alexandra Giannopoulou, *Data Protection Compliance Challenges for Self-Sovereign Identity*, in J. Prieto et al. eds., Blockchain 2020, AISC 1238, 2 (2021), https://ssrn.com/abstract=3671523.

665 Bilgesu Sümer, *Can Self-Sovereign Identity (SSI) Provide You with Control Over Your Digital Identity? A Techno-Legal Analysis of Opportunities and Challenges*, KU Leuven Ctr. for IT & IP Law (Nov. 2, 2022), https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-provide-you-with-control-over-your-digital-identity-a-techno-legal-analysis-of-opportunities-and-challenges/.

666 *See generally* Anhtuan Le, Gregory Epiphaniou & Carsten Maple, *A Comparative Cyber Risk Analysis between Federated and Self-Sovereign Identity Management Systems,* 5 Data & Pol'y e38 (2023), https://doi.org/10.1017/dap.2023.41; Xinjie Zhu et al., *An Efficient Decentralized Identity Management System Based on Range Proof for Social Networks*, 4 IEEE Open J. Computer Soc. 84-96 (2023), https://ieeexplore.ieee.org/document/10073618; Lukas Stockburger et al., *Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation*, 2(2) Blockchain Rsch. & Applications (2021), https://doi.org/10.1016/j.bcra.2021.100014; Gabriella Laatikainen, Taijia Kolehmainen & Pekka Abrahamsson, *Self-Sovereign Identity Ecosystems: Benefits and Challenges*, 12th Scandinavian Conf. on Info. Sys. (2021), https://aisel.aisnet.org/scis2021/10; /; Gabriella Laatikainen et al., *Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems*, in PACIS 2021 Proceedings, art. 19 (2021), https://arxiv.org/abs/2105.15131; Greg McMullen, Primavera De Filippi & Constance Choi, *Blockchain Identity Services: Technical Benchmark of Existing Blockchain Based Identity Systems*, Blockchain Research Institute and Coalition of Automated Legal Applications 12 (2019).

4.5.1. Key Features of Blockchain-Based Identity

4.5.1.A. Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs)

"Self-sovereign identity" (SSI) refers to a model of digital identity in which individuals exercise control over their identifiers and credentials, without relying on a centralized authority to manage or store their data.[667] Under the SSI model, a trusted entity (for example, a university, employer, or government body) gives an individual "verifiable credentials," which are digitally signed attestations that confirm specific attributes or qualifications of the individual. Credentials are not stored in centralized databases held by platforms or identity providers; they are instead stored under the user's control —typically in a digital wallet that manages the keys needed to hold and present them. When someone needs to verify the individual's credentials, they do so by using cryptographic proofs, not by pulling the data from the database of the trusted entity that issued the credentials.

At its foundation, SSI builds on decentralized identifier (DID) systems.[668] A DID is a globally unique, cryptographically verifiable identifier associated with a DID Document that sets out public keys and service endpoints. These elements allow verifiers to authenticate the holder's control of the identifier through cryptographic signature checks. DID systems provide the technical infrastructure that enables individuals to independently generate and manage their identifiers, store verifiable credentials in digital wallets under their control, and present these credentials across different services.[669] Unlike traditional identity systems, which rely on centralized databases, SSI keeps credentials in the custody of the user. Using cryptographic proofs, credentials can be verified without contacting the original issuer —for example, confirming a diploma without reaching out to the university that delivered it.

While SSI and DIDs are frequently associated with blockchain systems, they are not inherently dependent on them. Blockchain is often used as an implementation layer because it can provide decentralized consensus, tamper resistance, and public verifiability for components such as DID method registries or credential revocation lists in environments lacking a trusted central administrator.[670] However, the core principles of SSI —user autonomy, privacy, and decentralization— can also be implemented through other distributed infrastructures,[671] including peer-to-peer networks or content-addressed storage systems, such as the IPFS.[672] This architectural flexibility is particularly relevant in light of data protection regimes (e.g., GDPR), which may require the modification or effective erasure of personal data references *(See section 6.7.1)*. Blockchain remains one of the most mature technical substrates for certain SSI implementations, but it constitutes only one possible design choice rather than a technological prerequisite.

667 Aarti Amod Agarkar, et al., *Blockchain aware decentralized identity management and access control system,* 31 Measurement: Sensors art. 101032 (2024), https://doi.org/10.1016/j.measen.2024.101032; Alexandra Giannopoulou & Fennie Wang, *Self-sovereign identity*, 10(2) Internet Pol'y Rev. abstract (Apr. 10, 2021), https://policyreview.info/open-abstracts/self-sovereign-identity.

668 Alexandra Giannopoulou, *Digital Identity Infrastructures: A critical approach of self-sovereign identity*, 2(18) Digital Society 1-2 (2023), https://doi.org/10.1007/s44206-023-00049-z; Giannopoulou & Wang, *supra* note 667.

669 Galia Kondova & Jörn Erbguth, *Self-sovereign identity on public blockchains and the GDPR*, Proceedings of the 35th Annual ACM Symposium on Applied Computing 342 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3515213

670 Giannopoulou & Wang, supra note 667 at 7.

671 *See* W3C, *Decentralized Identifiers (DIDs) v1.0,* §1, §1.4 and §6, (July 19, 2022), https://www.w3.org/TR/did-1.0/.

672 Nikos Papatheodorou, George Hatzivasilis & Nikos Papadakis, *The YouGovern Secure Blockchain-Based Self-Sovereign Identity (SSI) Management and Access Control*, 15 Applied Sci. 6437 (2025), https://www.mdpi.com/2076-3417/15/12/6437 (demonstrating IPFS integration as a decentralized storage layer in a W3C-compliant SSI system, and noting that while IPFS enables content-addressed decentralized storage, it does not inherently ensure long-term data persistence).

4.5.1.B. Technical Characteristics of Blockchain-Based Identities

On blockchain-based systems, users are represented through cryptographic key pairs: a *public key* visible to network participants and a *private key* that enables the user to authenticate and control their accounts and associated digital assets *(See section 5.5.3.)*. The creation of a decentralized identity typically begins with a digital wallet application, which creates one or more Decentralized Identifiers (DIDs), rather than having identifiers "assigned" by any central authority.[673] A DID is expressed as a Uniform Resource Identifier (URI),[674] which might look like this: `did:example:123456`. Each DID connects to a DID Document which contains the metadata necessary for secure interactions, such as public keys, authentication methods, and service endpoints. DID Documents are not necessarily stored on-chain; instead, they are retrieved through the resolution process defined by the DID method. They may be updated only by the DID's controller, who proves control through the corresponding private key.

Personal information itself is not stored in the DID Document. Instead, identity-related attributes are conveyed through *Verifiable Credentials* (VCs) —cryptographically signed attestations issued by trusted issuers, such as governments (identity credentials), universities (diplomas), or insurance companies (coverage certificates).[675] To verify a VC, the verifier checks the issuer's digital signature using the public key listed in the issuer's DID Document.[676]

Once a digital identity wallet is established, its holder can accumulate VCs from multiple issuers and exercise granular control over their disclosure. Wallets may also link to encrypted off-chain data —such as medical or financial records— stored in external databases or cloud systems. These links preserve user privacy because access to the data can be authorized or denied solely by the wallet holder.

4.5.1.C. Advantages and Disadvantages

1. Advantages

Decentralized identifier (DID) systems offer several advantages. They make it possible to manage official credentials —such as birth or marriage certificates, passports, residence permits, diplomas, or social security documents— in digital form and in contexts where authorities choose to issue them as verifiable credentials. Through digital identity wallets, users can generate and control multiple identifiers, allowing them to authenticate or interact online while disclosing only the information strictly required for a given purpose. This selective presentation of credentials helps avoid exposing a broader digital footprint and reduces the amount of personal data collected, thereby strengthening privacy and user autonomy.[677] For example, a user can prove that they are above a minimum age without revealing their exact age or full date of birth.[678] By limiting unnecessary data disclosure, DID systems support compliance with personal data protection frameworks, such as the GDPR, especially regarding data minimization and user control.[679]

673 *Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2025*, Dock Labs (Dec. 2, 2025), https://www.dock.io/post/decentralized-identifiers.

674 A Uniform Resource Identifier (URI) is a standardized string of characters used to uniquely identify a resource. It includes both Uniform Resource Locators (URLs) which locate resources (e.g., https://www.stanford.edu) and Uniform Resource Names (URNs), which name resources (e.g., urn:isbn:0451450523). A DID is a specific type of URI designed for decentralized identity. For user convenience, a DID can also be encoded into alternative representations, such as QR codes, but these are not part of the identifier itself; *see* McMullen, De Filippi & Choi, *supra* note 667 at 20.

675 McMullen, De Filippi & Choi, *supra* note 666 at 20.

676 *Id.* at 21.

677 *Id*. at 12.

678 McMullen, Filippi & Choi, *supra* note 666 at 9 (explaining how zero-knowledge proofs allow users to prove an attribute without revealing the underlying data); *see also id*. at 3 (listing birth certificates, diplomas, and licenses as credentials managed in a user-controlled identity "black box"). .

679 Galia Kondova & Jörn Erbguth, *Self-sovereign identity on public blockchains and the GDPR*, Proceedings of the 35th Annual ACM Symposium on Applied Computing 342 (2020), https://ssrn.com/abstract=3515213; Christopher Allen, The Path to Self Sovereign Identity Life with Alacrity (2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

A further advantage lies in the security properties associated with decentralized architectures. Because identifiers and related verification data are not concentrated in a single, central database, the risk of large-scale breaches is reduced. Depending on the implementation, DID systems may operate entirely off-chain or make use of blockchain infrastructures. In the latter case, users retain direct control over their identifiers and associated private keys, which can lower the likelihood of identity theft or credential fraud, though it does not eliminate security risks entirely.

2. Disadvantages

Despite their advantages, decentralized identifier systems involve significant risks and trade-offs. The most immediate concern is the shift in responsibility from centralized authorities to individuals. In DID systems, the user becomes solely responsible for safeguarding their private keys and managing their digital identity.[680] If a private key or identity wallet is lost, recovery is generally impossible unless specific backup or recovery mechanisms are built into the system ex ante, which undermines the promise of full user control.[681] This places disproportionate burdens on users with limited digital literacy. Proposed solutions —such as secure intermediaries, social recovery, or key custodians— can reduce this risk, but they reintroduce elements of centralization that contradict the initial rationale of self-sovereign identity.[682]

Interoperability constitutes another major challenge. DID ecosystems remain highly fragmented: A significant number of DID methods coexist, each with different resolution processes, trust models, and technical assumptions,[683] and various competing formats for verifiable credentials are still used in parallel. This lack of convergence creates barriers to cross-platform and cross-jurisdictional use and complicates the integration of DIDs into public or private identity systems.[684] Without greater standardization and compatibility, DID systems are unlikely to achieve wide adoption or practical utility beyond pilot projects.

Significant legal and governance challenges also remain. SSI architectures do not eliminate the need for authoritative issuers: Credentials must still be generated by trusted entities,[685] often public authorities, whose legal recognition determines their validity. In practice, SSI redistributes trust rather than removes it. Users must trust issuers of credentials, the security of their wallet software, the governance of DID registries, and, where applicable, the blockchain infrastructure anchoring revocation lists or identifiers. Certain jurisdictions — most notably the European Union through eIDAS 2.0[686] *(See below section 7.3.3.B.)* — have begun to regulate digital identity wallets and verifiable credentials that overlap with SSI architectures. However, questions of liability, enforceability, and compliance with identity-

680 McMullen, De Filippi & Choi, *supra* note 666 at 7.

681 *Id*. at 16; *see also* Satoru Hori, *Self-sovereign identity: the future of personal data ownership?* World Economic Forum (Aug. 12, 2021), https://www.weforum.org/stories/2021/08/self-sovereign-identity-future-personal-data-ownership/?utm_source; "a lost private key is impossible to restore [...] blocking the consumer permanently from accessing their data.", Marco Hünseler & Elena Pöll, *Promises and Problems in the Adoption of Self-Sovereign Identity Management from a Consumer Perspective*, *in* Privacy and Identity Management: Privacy and Identity 2022, IFIP Advances in Info. & Commc'n Tech, vol. 671, 85, 93 (Felix Bieker et al. eds., 2023), https://philarchive.org/archive/HNSPAP

682 McMullen, De Filippi & Choi, *supra* note 666 at 41.

683 Ralph Swick, *Director's Decision on DID 1.0 Proposed Recommendation Formal* Objections, W3C (June 30, 2022), https://www.w3.org/2022/06/DIDRecommendationDecision.html; Hünseler & Pöll, *supra* note 681 at 93; McMullen, De Filippi & Choi, *supra* note 666 at 17.

684 McMullen, De Filippi & Choi, *supra* note 666 at 17-18.

685 McMullen, De Filippi & Choi, *supra* note 666 at 15; Giannopoulou & Wang, *supra* note 667 at 2.

686 Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework, 2024 O.J. (L) 1183, https://eur-lex.europa.eu/eli/reg/2024/1183/oj [hereinafter eIDAS 2.0 Regulation]. eIDAS 2.0 regulates digital identity wallets, electronic attestations, and trust services that overlap significantly with SSI architectures (see section 7.3.3.B.), but it does not regulate SSI or decentralized identifiers (DIDs) as such. The European Digital Identity Wallet (EUDI Wallet) is nevertheless explicitly built around verifiable credentials, qualified electronic attestations of attributes, and user-controlled wallets, elements that closely parallel SSI and VC ecosystems.

management laws and AML/KYC obligations remain insufficiently settled, especially outside the EU. Moreover, user behavior presents an additional obstacle: Individuals accustomed to the convenience of passwords or federated login systems may resist adopting identity tools that require greater operational responsibility, even when these tools offer stronger privacy protections.

Real-world experiments underscore these concerns. China's RealDID system,[687] while using decentralized identifiers, links them directly to state-issued identities and enables extensive government monitoring, illustrating that decentralized technologies are not inherently decentralizing and can be repurposed for centralized control.[688] Similarly, initiatives such as WorldID *(See section 4.5.2.B.)* raise concerns about the centralization of biometric data collection and governance, suggesting that blockchain-based identity solutions can replicate, rather than eliminate, risks of surveillance and concentration of power.[689]

4.5.2. Case Studies

A few examples illustrate the development of blockchain-based digital identities.

4.5.2.A. Human Passport

Human Passport (originally launched as Gitcoin Passport in 2022) was created as a privacy-preserving Proof-of-Humanity protocol.[690] Its purpose is to protect systems from bot-driven attacks by verifying that each user is a real and unique human being.[691] The system recognizes a user as human by collecting "stamps" —identity-related attestations. These can include such things as logging into Google or LinkedIn, verifying a phone number, or, in some cases, submitting passport or biometric data. These stamps can be, but are not necessarily, verifiable credentials; many rely instead on Application Programming Interfaces-based attestations provided by third-party services. Each stamp carries a predefined weight, and these weights are aggregated into a "Unique Humanity Score."[692] When the score reaches a threshold of 20, the protocol designates the user as a verified human. This assures partner applications that they are interacting with a human user, rather than a bot.

Human Passport seeks to preserve user privacy by storing only cryptographic proofs, rather than personally identifiable information. It relies on privacy-enhancing techniques, including zero-knowledge proofs, to demonstrate humanity without revealing sensitive data.[693] Stamps are verified off-chain by Passport's servers, but proofs derived from these stamps may be minted on-chain, creating a tamper-resistant record that decentralized applications can query without accessing underlying personal data.[694] According to the Holonym

687 Xinmei Shen and Matt Haldane, *Blockchain-managed IDs arrive in China with new government-backed scheme aiming to reduce data leaks*, South China Morning Post, (Dec. 14, 2023), https://www.scmp.com/tech/policy/article/3245028/blockchain-managed-ids-arrive-china-new-government-backed-scheme-aiming-reduce-data-leaks

688 Andrey Sergeenkov, *China Bets On Massive Blockchain Infrastructure,* Forbes (2024), https://www.forbes.com/sites/digital-assets/2024/10/08/china-bets-on-massive-blockchain-infrastructure/.

689 *See Scrutiny of Iris-Scanning Crypto Project Worldcoin Grows*, Reuters (Mar. 26, 2024), https://www.reuters.com/technology/scrutiny-iris-scanning-crypto-project-worldcoin-grows-2023-09-01/; see *also* Liza Savenko, *What is the World's Orb, and How Does It Protect Your Personal Data?*, CoinTelegraph (Oct. 30, 2024), https://cointelegraph.com/explained/what-is-worldcoin-and-how-does-it-help-preserve-world-id.

690 Chainwire, *Holonym Foundation Acquires Gitcoin Passport to Onboard Its 2M Users to Create World's Largest Proof of Humanity Solution*, THE DEFIANT (Feb. 10, 2025), https://thedefiant.io/news/press-releases/holonym-foundation-acquires-gitcoin-passport-to-onboard-its-2m-users-to-create-worlds-largest-proof-of-humanity-solution?utm_source

691 Shrey Jain et al., *AI and Democracy's Digital Identity Crisis*, 7(1) Stan. J. Blockchain L. & Pol'y 56-75 (2024), https://stanford-jblp.pubpub.org/pub/ai-democracy-digital-identity/release/1.

692 *What is Human Passport?*, Human Passport Knowledge Base, https://support.passport.xyz/passport-knowledge-base (last visited Jan. 15, 2026).

693 *Why your privacy matters to us*, Human Passport, https://passport.human.tech/privacy (last visited Jan. 15, 2026).

694 Human Passport, *supra* note 693.

Foundation, which operates Human Passport, the system currently has more than two million users with over 35 million recorded attestations.[695]

Despite these advantages, several challenges remain. Usability is a major concern: The multi-step process for collecting and validating stamps is neither intuitive nor easily accessible for a broad internet audience.[696] The Human Passport scoring system —while transparent— is not entirely seamless for new users during onboarding.[697] Liability questions also persist, as the Terms of Use place full responsibility on users for managing their wallets, securing their keys, and addressing any complications or losses that may occur.[698]

4.5.2.B. World Network

World Network —formerly Worldcoin— is a digital identity project launched publicly by Tools for Humanity, a company co-founded by Sam Altman, Max Novendstern, and Alex Blania.[699] The project comprises two main components: World ID, a proof-of-personhood protocol, and the Worldcoin (WLD) cryptocurrency. In 2023, World ID launched out of beta, and WLD tokens became freely tradable on several cryptocurrency exchanges, though not initially in the United States.[700] Worldcoin was rebranded as World Network in October 2024.[701] In April 2025, the company announced that WLD tokens would become available in most of the United States, including through exchanges such as Coinbase, and it formally launched U.S. operations on May 1, 2025.[702] As of January 2026, World reported approximately 38 million World App users, of whom approximately 17 million were verified with World ID.[703]

World ID is presented as an open and privacy-preserving identity protocol designed to verify that a user is a human being without revealing their real-world identity.[704] Verification occurs through an iris-scanning device known as the Orb,[705] which generates a cryptographically irreversible iris hash, rather than storing actual biometric images.[706] The system uses hashing techniques and zero-knowledge proofs to allow users to authenticate across web, mobile, and blockchain-based applications without revealing personal data.[707] Upon successful verification, users may receive an allocation of WLD tokens (the "Genesis Grant"), although token rewards vary by jurisdiction and are unavailable in some countries —including the United States— due to regulatory constraints. The project was conceived with the ambition

695 *Passport Update*, GITCOIN, (Feb. 10, 2025), https://gov.gitcoin.co/t/passport-update/19966?utm_source.

696 Ayae Ide & Tanusree Sharma, *Personhood Credentials: Human-Centered Design Recommendation Balancing Security, Usability, and Trust*, arXiv (Feb. 22, 2025), https://doi.org/10.48550/arXiv.2502.16375.

697 Credential Map and Weights, Human Passport Developer Docs, https://docs.passport.xyz/building-with-passport/stamps/major-concepts/credential-map-and-weights (last visited Jan. 15, 2026).

698 *Terms of Use*, Human Passport, https://passport.human.tech/terms?utm_source (last visited Jan. 15, 2026).

699 *GPS 2025: Sam Altman, Alex Blania Discuss Tools for Humanity's Biometric Technology*, Int'l Ass'n of Priv. Pros. (Jan. 23, 2025), https://iapp.org/news/a/gps-2025-sam-altman-alex-blania-discuss-tools-for-humanity-s-biometric-technology

700 Anna Tong, *Sam Altman's Worldcoin Launches Token*, Reuters (July 24, 2023), https://www.reuters.com/technology/sam-altmans-worldcoin-launches-token-2023-07-24

701 MK Manoylov, *Sam Altman-Backed Worldcoin Project Launches Mainnet Blockchain Following a Rebrand*, The Block (Oct. 17, 2024), https://www.theblock.co/post/321792/sam-altman-backed-worldcoin-project-launches-mainnet-blockchain-following-a-rebrand.

702 *World Launches San Francisco Flagship in Iconic Union Square*, World (May 6, 2025), https://world.org/blog/announcements/world-launches-san-francisco-flagship-in-iconic-union-square; *see also* MK Manoylov, *World Raises $135 Million via WLD Token Sale to Expand Across the US*, The Block (May 21, 2025), https://www.theblock.co/post/355263/world-raises-135-million-via-wld-token-sale-to-expand-across-the-us.

703 World, https://world.org/ (last visited Jan. 15, 2026).

704 World ID FAQs, For every human (April 4, 2024), https://worldcoin.org/blog/worldcoin/world-id-faqs (last visited Jan. 15, 2026).

705 Introducing World ID 2.0: A Human Passport for the Internet, Introducing World ID 2.0 (December 13, 2023), https://worldcoin.org/blog/announcements/introducing-world-id-2.0 (last visited Jan. 15, 2026); Worldcoin Whitepaper, Worldcoin Whitepaper, https://whitepaper.worldcoin.org/ (last visited Jan. 15, 2026).

706 World ID FAQs, World (2024), https://worldcoin.org/blog/worldcoin/world-id-faqs (last visited Jan. 15, 2026).

707 *Introducing World ID 2.0: A human passport for the internet*, World (Dec. 13, 2023), https://worldcoin.org/blog/announcements/introducing-world-id-2.0.

of providing a form of universal basic income (UBI) by distributing tokens to verified individuals.[708]

The project has attracted sustained criticism, particularly in relation to privacy and data protection.[709] Although the company states that biometric data is hashed,[710] meaning no images of iris scans are stored, its terms and conditions provide that users can 'opt-in' to share iris images to help Worldcoin improve its system.[711] In May 2024, World migrated all stored iris codes to a secure multi-party computation (SMPC) system in an effort to enhance privacy. According to the company, legacy iris codes were deleted after the migration.[712] Yet critics also note that, because enrollment can occur only through Orb devices controlled by Tools for Humanity and its partners, the verification process introduces a significant point of centralization and potential single point of failure.[713]

Independent audits have reinforced these concerns. In 2023, the security firm CertiK disclosed a vulnerability in the operator-onboarding process that could have enabled unauthorized individuals to register as Orb operators, potentially compromising the integrity of identity issuance.[714] Although the flaw was promptly fixed, it raised further doubts about the project's security model. Ethical concerns have also emerged, especially regarding early deployments in developing countries where participants received monetary incentives for verification. Observers warn that individuals in vulnerable communities may not fully understand the risks associated with providing biometric data, raising concerns about exploitation.[715]

Regulators in several jurisdictions have expressed concern over the processing of sensitive biometric data. Germany's Bavarian data protection authorities investigated Worldcoin's iris-scanning practices and found that iris codes had been stored in centralized databases without adequate safeguards during earlier stages of the project. The authorities, in December 2024, ordered the company to implement stricter data protection measures.[716] World subsequently paused its iris-scanning operations in Germany while updating its Orb stations and appealing the regulatory orders.[717] In November 2025, Thailand's Personal Data Protection Committee ordered World to suspend biometric enrollment operations, citing inadequate transparency and failure to obtain valid consent for processing sensitive biometric data collected

708 Casey Tonkin, *Worldcoin Wants To Provide UBI Through Crypto*, InformationAge (July 26, 2023), https://ia.acs.org.au/article/2023/worldcoin-wants-to-provide-ubi-through-crypto.html.

709 Daniel Ramirez-Escudero, *Worldcoin Faces Bans Worldwide Amid Increasing Privacy Fears*, CoinTelegraph (May 27, 2024), https://cointelegraph.com/news/worldcoin-ban-privacy-regulation-ai (last visited Jan. 15, 2026) (quoting Rory Mir, Associate Director of Community Organizing, Electronic Frontier Foundation, and Christoph Schmon, International Policy Director, Electronic Frontier Foundation).

710 *See Scrutiny of Iris-Scanning Crypto Project Worldcoin Grows*, Reuters (Mar. 26, 2024), https://www.reuters.com/technology/scrutiny-iris-scanning-crypto-project-worldcoin-grows-2023-09-01/; *see also* Tobias Vilkenson, *What is the World's Orb, and How Does It Protect Your Personal Data?* CoinTelegraph (Oct. 30, 2024), https://cointelegraph.com/explained/what-is-worldcoin-and-how-does-it-help-preserve-world-id.

711 Oluwapelumi Adejumo, *Hong Kong Bans Worldcoin's Data Collection Over Alleged Privacy Violations*, CryptoSlate (May 23, 2024), https://cryptoslate.com/hong-kong-bans-worldcoins-data-collection-over-alleged-privacy-violations/.

712 Assad Jafri, *Worldcoin Open-Sources Revamped Biometric Data System*, CryptoSlate (May 15, 2024), https://cryptoslate.com/worldcoin-open-sources-revamped-biometric-data-system/

713 Amin Haqshanas, Is *World's biometric ID model a threat to self-sovereignty?,* COINTELEGRAPH, (May 25, 2025), https://cointelegraph.com/news/world-biometric-id-decentralization-criticism.

714 *See* Derek Andersen, *Worldcoin's Orb Had Serious Security Vulnerability in Operator Onboarding: CertiK*, CoinTelegraph (Aug. 4, 2023), https://cointelegraph.com/news/worldcoin-orb-had-serious-security-vulnerability-in-operator-onboarding-certik.*See also* Tobias Vilkenson, *What is the World's Orb, and How Does It Protect Your Personal Data?* CoinTelegraph (Oct. 30, 2024), https://cointelegraph.com/explained/what-is-worldcoin-and-how-does-it-help-preserve-world-id.

715 *See* Eileen Guo et al., *Deception, Exploited Workers, and Cash Handouts: How World Recruited Its First Half a Million Test Users*, MIT Tech. Rev. (Apr. 6, 2022), https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3/.

716 *German Watchdog Orders Worldcoin to Delete Non-Compliant Dat*a, COINTELEGRAPH (Dec. 19, 2024), https://cointelegraph.com/news/german-watchdog-order-worldcoin-delete-data.

717 *Worldcoin Pauses Iris Scanning in Germany Amid Station Upgrades and Regulatory Review*, ID TECH (July 10, 2025), https://idtechwire.com/worldcoin-pauses-iris-scanning-in-germany-amid-station-upgrades-and-regulatory-review/.

from over 1.2 million Thai residents.[718] Kenya's Office of the Data Protection Commissioner suspended Worldcoin operations in 2023 due to concerns over data collection and consent[719] and, in May 2025, Kenya's High Court ordered the permanent deletion of all biometric data collected in the country after finding that cryptocurrency incentives had undermined the validity of user consent.[720] Additional investigations or regulatory actions have been taken in Spain, Portugal, France, Hong Kong, Indonesia, Argentina, Brazil, South Korea, and China.[721] Despite these enforcement actions, World has secured governmental support in other markets. In 2024, the company established partnerships with Taiwan and Malaysia to support national digital-identity verification initiatives.[722]

4.5.2.C. Identity Overlay Network (ION)

The Identity Overlay Network (ION) is a decentralized identifier (DID) network developed by Microsoft in collaboration with the Decentralized Identity Foundation (DIF), active since 2019 and launched in 2021.[723] It provides a scalable, open infrastructure for managing digital identifiers without relying on centralized authorities or special-purpose tokens. Unlike many blockchain-based identity systems, ION does not introduce a native cryptocurrency. Instead, it implements the Sidetree protocol in a Layer-2 architecture on top of the Bitcoin blockchain, using Bitcoin solely as an immutable anchoring layer, while performing the majority of DID operations off-chain.[724]

ION provides an infrastructure for creating, updating, and resolving decentralized identifiers (DIDs). The network is designed for high throughput —capable of handling thousands of DID operations per second— by batching many operations and anchoring them periodically to the Bitcoin blockchain.[725] It enables users to control their identifiers through cryptographic keys.[726] ION makes no claim that a DID corresponds to a real or unique individual, but simply guarantees that whoever controls the corresponding private keys controls the DID.

The system is fully open source, and development occurs within the Decentralized Identity Foundation (DIF) ecosystem.[727] The codebase is publicly available on GitHub, enabling anyone to review, contribute, or run an ION node.[728] Participation is permissionless, and no single entity has administrative control over the

718 *Thailand Orders Worldcoin to Halt Iris Scans and Delete Biometric Data*, ID TECH (Nov. 26, 2025), https://idtechwire.com/thailand-orders-worldcoin-to-halt-iris-scans-and-delete-biometric-data/

719 Carlos Mureithi, *Five Things to Learn from Kenya's Inquiry into Worldcoin's Activities in the Country*, TECH POLICY PRESS (Apr. 24, 2024), https://www.techpolicy.press/five-things-to-learn-from-kenyas-inquiry-into-worldcoins-activities-in-the-country/

720 Steve Kaaru, *Kenya Orders Worldcoin to Cease Biometric Data Collection*, COINGEEK (Aug. 2, 2023), https://coingeek.com/kenya-orders-worldcoin-to-cease-biometric-data-collection/

721 Helen Partz, WORLDCOIN SAYS IT'S LEGAL IN ALL COUNTRIES IT OPERATES IN DESPITE SPANISH BAN COINTELEGRAPH (2024), https://cointelegraph.com/news/worldcoin-legal-all-operated-countries-ban-spain (last visited Jan. 15, 2026); Tanpat Kraiwanit et al., *Adoption of Worldcoin Digital Wallet in Thailand*, 7 RESEARCH IN GLOBALIZATION 1–5 (2023) https://www.researchgate.net/publication/375906390_Adoption_of_Worldcoin_Digital_Wallet_in_Thailand; see *Argentina: AAIP Initiates Investigation into Handling of Personal Data by Worldcoin Foundation*, DATAGUIDANCE (Aug. 9, 2023), https://www.dataguidance.com/news/argentina-aaip-initiates-investigation-handling; *Worldcoin in the Spotlight Again as China Warns of Biometric Data Threats*, BITCOINIST (Aug. 7, 2025), https://bitcoinist.com/worldcoin-in-spotlight-again-china-warns-biometric/

722 *See Malaysia Partners with Worldcoin for Advanced Digital ID Verification*, Identity Week (Aug. 19, 2024), https://identityweek.net/malaysia-partners-with-worldcoin-for-advanced-digital-id-verification/ (detailing the MoU with the Malaysian government); *see also World Proof of Human Now Available in Taiwan*, WORLD (May 28, 2025), https://world.org/blog/announcements/world-launches-in-taiwan (announcing the official launch in Taiwan to support the country's digital economy initiatives).

723 Colin Harper, *Microsoft's ION Digital ID Network Is Live on Bitcoin*, NASDAQ (Mar. 25, 2021), https://www.nasdaq.com/articles/microsofts-ion-digital-id-network-is-live-on-bitcoin-2021-03-25.

724 *Toward Scalable Decentralized Identifier Systems*, MICROSOFT CMTY. HUB (May 13, 2019), https://techcommunity.microsoft.com/blog/microsoft-entra-blog/toward-scalable-decentralized-identifier-systems/560168

725 *Id*.

726 Harper, *supra* note 723.

727 Pamela Dingle, *ION – We Have Liftoff!*, MICROSOFT CMTY. HUB (Mar. 25, 2021), https://techcommunity.microsoft.com/blog/microsoft-security-blog/ion-%E2%80%93-we-have-liftoff/1441555

728 *GitHub – Decentralized-Identity/ION*, GITHUB, https://github.com/decentralized-identity/ion (last visited Jan. 15, 2026).

network. Organizations can participate in the network by running public nodes that help process and validate DID operations across the system. In practice, some DID resolution currently relies on public nodes run by a limited number of organizations.[729]

4.5.2.D. Other Examples

Various identity solutions have been developed on public and permissionless blockchains. Veramo[730] (which evolved from the earlier uPort project[731]) provides an open-source framework for building decentralized-identity and verifiable-credential applications. Jolocom,[732] a German-based initiative, is also advancing SSI technologies and wallet applications. Sovrin,[733] which was built as a permissioned ledger on Hyperledger Indy, played a pioneering role in early SSI development, although its activity and ecosystem participation have diminished significantly in recent years.

Other identity solutions have been implemented which are not necessarily built on blockchain systems. KYC-Chain[734] functions as a compliance-oriented service that provides know-your-customer (KYC) and anti–money laundering (AML) verification tools for financial institutions. It may incorporate blockchain components within its workflows but is not itself a blockchain-based identity network. The ID2020 Alliance[735] is a multi-stakeholder initiative promoting ethical, privacy-preserving digital-identity standards in humanitarian and development contexts. It does not prescribe or rely on a specific technological architecture and is, therefore, not a blockchain identity system per se.

The Civic project[736] has introduced an identity-verification ecosystem aimed at decentralized applications. Its "Civic Pass" enables users to download an application, store encrypted credentials (such as government-issued identity numbers or other personal attributes), and authenticate across platforms without repeatedly disclosing their personal information. Civic itself does not retain users' personal data; instead, data remain encrypted on the user's device or in user-controlled storage, accessible only with consent. Biometric authentication mechanisms (e.g., fingerprint or facial recognition on the device) provide additional layers of security. Importantly, the application stores only credentials, not the underlying personal data, thereby reinforcing user control and privacy.

Another emerging example is the integration of DIDs with existing large-scale digital identity systems. In India, the National Blockchain Framework is exploring the issuance of verifiable credentials for education and healthcare that can be anchored to Aadhaar - the country's biometric digital identity system covering over a billion residents. The pilot enables self-sovereign verification of credentials without exposing the underlying identity data *(See Appendix 21)*.

While decentralized identifier systems enhance user autonomy, they do not eliminate the role of governments or other authoritative issuers in identity management. Legal identity remains grounded in state-recognized credentials, such as passports and birth certificates,

729 Pamela Dingle, *ION – We Have Liftoff!*, Microsoft Cmty. Hub (Mar. 25, 2021), https://techcommunity.microsoft.com/blog/microsoft-security-blog/ion-%E2%80%93-we-have-liftoff/1441555 (encouraging partner organizations to operate nodes to strengthen the network, acknowledging that early adoption relies on deployed infrastructure)

730 *Veramo*, https://veramo.io/ (last visited Jan. 15, 2026).

731 uPort, *Veramo: uPort's Open Source Evolution*, MEDIUM, https://medium.com/uport/veramo-uports-open-source-evolution-d85fa463db1f (last visited Jan. 15, 2026).

732 Jolocom, ALCHEMY, https://www.alchemy.com/dapps/jolocom (last visited Jan. 15, 2026).

733 Sovrin, Sovrin Found., https://sovrin.org/, (last visited Jan. 15, 2026).

734 KYC Chain, https://kyc-chain.com/, (last visited Jan. 15, 2026).

735 ID2020, https://www.id2020.org/, (last visited Jan. 15, 2026).

736 Civic Auth, https://www.civic.com/, (last visited Jan. 15, 2026).

and public authorities continue to determine which attestations carry legal effect. Blockchain-based identity systems, therefore, redistribute trust rather than replace it: They shift control over credential storage and presentation toward users, while preserving reliance on trusted issuers and regulatory frameworks. These architectures are most compelling where individuals must present verifiable attributes across multiple services without repeatedly disclosing excessive personal data or depending on a single dominant platform. In such contexts, blockchain can enhance portability, selective disclosure, and auditability —but it does not substitute for authoritative credential issuance, legal recognition, or coherent governance structures.

4.6. BLOCKCHAIN-BASED SOCIAL MEDIA

Over the past decade, the rise of influential social networks, dominated by a handful of powerful investor-owned companies,[737] has underscored the need for greater transparency, stronger user control over personal data, and more competition within the digital ecosystem. In response, scholars, developers, and civil-society advocates have increasingly called for alternatives to these centralized platforms, including decentralized and distributed social-network models.[738]

4.6.1. Alternative Social Media Architectures

4.6.1.A. Decentralized and Distributed Social Networks

While the terms *"decentralized social media"* and *"distributed social media"* are often used interchangeably, they are not synonymous. Both approaches seek to reduce reliance on centralized platform operators and to redistribute control over data, content, and governance to users;[739] but, they differ in their underlying technical architectures and governance implications. In practice, most real-world platforms combine elements of both, and the distinction is best understood as an analytical clarification rather than a strict classificatory grid.

1. Decentralized Social Networks

Decentralized social media refers to social networking platforms —such as Mastodon, Bluesky, or Diaspora— that operate without a single central authority controlling the entire network.[740] Rather than being hosted on infrastructure owned and governed by one entity, decentralized platforms are composed of independently operated servers or services that interoperate through shared protocols.[741] Data management, identity authentication, and moderation are, therefore, distributed across multiple operators rather than concentrated in a single organization.[742] This architecture limits single points of control or failure, even though individual nodes or services may themselves be centrally managed.

Decentralized social networks are often intended to give users greater control over their data and content, rather than having such data exclusively collected, stored, or

737 Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised social media*, 12 Internet Policy Review 7, 3 (2023), https://policyreview.info/pdf/policyreview-2023-1-1681.pdf.

738 Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, Knight First Amendment Inst. at Columbia Univ. (2019), https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech (last visited Jan. 15, 2026); *see also* Yaman Zhao, *Decentralized Social Networks and the Future of Free Speech Online*, 75 Computer L. & Sec. Rev. 106011 (2024), https://www.sciencedirect.com/science/article/pii/S0267364924001250 (last visited Jan. 15, 2026).

739 Yuanzhu Zhan, Yu Xiong & Xinjie Xing, *A conceptual model and case study of blockchain-enabled social media platform*, 119 Technovation 2 (2023), https://doi.org/10.1016/j.technovation.2022.102610.

740 Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised social media*, 12 Internet Policy Review 2 (2023), https://doi.org/10.14763/2023.1.1681; Mayank Jain et al., *Revamping social networking using blockchain: Conceptual Case-Study of Lens Protocol*, SSRN Electronic Journal 1–8 (2023), https://ssrn.com/abstract=4367051.

741 Alan Z. Rozenshtein, *Moderating the fediverse: Content moderation on distributed social media*, 3 Journal of Free Speech Law 2017 (2023), https://ssrn.com/abstract=4213674.

742 Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised social media*, 12 Internet Policy Review 2, 4 (2023), https://doi.org/10.14763/2023.1.1681.

monetized by a single platform operator. In practice, however, the degree of user control varies significantly depending on implementation choices. Some systems allow users to select their hosting provider or to migrate between providers, while others remain heavily reliant on default infrastructure. For example, the Bluesky network, which is based on the Authenticated Transfer (AT) Protocol, allows users, in principle, to choose their own personal data server (PDS). In practice, however, most users currently rely on the default PDS operated by Bluesky Public Benefit Corporation (PBC).[743]

These architectures frequently rely on open protocols and standards that enable interoperability across services. This can facilitate user mobility, allowing users to switch providers without entirely losing their identity or social connections. It also allows users to choose communities with moderation policies aligned with their preferences. While the absence of a single controlling authority makes system-wide censorship more difficult, it does not eliminate moderation or exclusion.[744] Content moderation typically occurs at the level of individual servers, client applications, or infrastructure providers and may still be shaped by app-store policies, hosting services, or dominant clients.

And not all decentralized social networks are blockchain-based. They include both blockchain-based systems and federated architectures built on open protocols, many of which do not rely on blockchains at all. A common feature of decentralized systems is federation: Independent servers interconnect and communicate, allowing users on different servers to interact. Users can choose which server (or "instance") to join, often based on community norms or moderation practices. Mastodon is a prominent example of a federated social network. It runs on open-source software and relies on the ActivityPub protocol to enable communication across independently operated instances.[745] Each instance is responsible for its own infrastructure, moderation rules, and governance decisions, including data storage, authentication, and identity management.[746] Users may, in principle, migrate between instances, but portability of social graphs and historical interactions remain partial. Connections are typically tied to the originating instance; and, if an instance ceases operation, users may lose access to parts of their network and content history.[747]

Bluesky represents a hybrid approach. The Authenticated Transfer Protocol is designed to support decentralization and portability,[748] while key infrastructure components —such as content indexing and discovery— have historically been operated by Bluesky PBC.[749] In response to concerns about infrastructural concentration, initiatives such as Project Liberty and Free Our Feeds have developed independent frameworks that aim to preserve the integrity of AT Protocol data while enabling public content to remain discoverable independent of Bluesky's services.[750] This has been achieved through integration with the Frequency blockchain, which supports independent data storage and indexing. These efforts seek to reduce reliance on corporate infrastructure

743 Martin Kleppmann et al., *Bluesky and the AT Protocol: Usable Decentralized Social Media*, arXiv (2024), https://arxiv.org/html/2402.03239v2.

744 Rozenshtein, *supra* note 741.

745 *ActivityPub*, Mastodon Documentation, https://docs.joinmastodon.org/spec/activitypub/ (last visited Jan. 15, 2026).

746 Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised social media*, 12 Internet Policy Review 4 (2023), https://policyreview.info/pdf/policyreview-2023-1-1681.pdf.

747 *Id.*

748 Martin Kleppmann et al., *Bluesky and the AT Protocol: Usable Decentralized Social Media*, arXiv (Oct. 16, 2024), https://arxiv.org/abs/2402.03239 (last visited Jan. 15, 2026).

749 Bluesky, https://bsky.social/about/faq (last visited Jan. 15, 2026).

750 Frequency, *Who Owns the Future of Social Media? A Giant Leap to Decentralize Core Components of Bluesky's AT Protocol Ecosystem*, PR Newswire (Feb. 27, 2025), https://www.prnewswire.com/news-releases/who-owns-the-future-of-social-media-a-giant-leap-to-decentralize-core-components-of-blueskys-at-protocol-ecosystem-302387397.html.

and mitigate the risk of unilateral control over public discourse, though they do not eliminate governance and power asymmetries altogether.

2- Distributed Social Networks

Distributed social networks refer to systems in which technical functions, such as data storage, message relay, and content delivery, are spread across multiple nodes, often including user devices. Distribution describes how infrastructure is organized, not who controls it. A system may be technically distributed while remaining institutionally centralized. For example, Facebook (Meta) operates a globally distributed infrastructure comprising thousands of servers across multiple jurisdictions, yet control over data, governance, and moderation remains fully centralized. By contrast, Mastodon is decentralized in governance, but most individual instances rely on conventional centralized servers. Its architecture is federated rather than fully peer-to-peer.

Some systems are both distributed and decentralized. Secure Scuttlebutt is a peer-to-peer social network in which messages are stored locally on user devices and shared directly between peers.[751] The network does not rely on central servers, and no single authority controls participation or content. Users can exchange messages even without continuous internet connectivity, synchronizing data opportunistically when devices come into contact. In such peer-to-peer systems, each participant's device functions as both client and server, and data is replicated across multiple nodes rather than stored in a central database. The blockchain-based platforms examined in the following section — Lens, Farcaster, and DSNP — each combine these dimensions differently: they are decentralized in their governance ambitions and identity architectures, while relying to varying degrees on distributed or partly centralized infrastructure for content storage and message relay.

4.6.1.B. Key Features of Blockchain-Based Social Media

Blockchain-based social media platforms combine decentralized governance aspirations with distributed technical architectures.[752] Their central objective is not merely technical decentralization, but the reallocation of control over identity, the social graph, and content monetization.[753] Instead of locking user identities and social connections inside proprietary databases, these systems use shared infrastructures to make identity and social graphs portable across applications.

1. Controlling the Social Graph

A core ambition of blockchain-based and protocol-based social media initiatives is to rethink control over the social graph. In social media systems, the social graph represents the network of relationships among users, including connections such as friendships, follows, and group affiliations.[754] Technically, it is modeled as a network of nodes connected by edges[755] (relationships), and it plays a central role in content distribution, recommendation, and influence.[756]

751 See *Scuttlebutt*, https://scuttlebutt.nz/ (last visited Jan. 15, 2026).

752 Mayank Jain et al., *Revamping social networking using blockchain: Conceptual Case-Study of Lens Protocol*, *in* Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022 (Feb. 22, 2023), https://ssrn.com/abstract=4367051; Bidita Sarkar Diba et al., *From Centralization to Decentralization: Blockchain's Role in Transforming Social Media Platforms*, 13 IEEE Access, (May 14, 2025), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10966494; Muhammad Hasnain, et al., *Cybersecurity challenges in blockchain-based social media networks: A comprehensive review,* 6(3) Blockchain: Rsch. & App. 100290, 2, 12, https://doi.org/10.1016/j.bcra.2025.100290.

753 Zhan, Xiong & Xing, *supra* note 739.

754 Jan H. Kietzmann et al., *Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media*, 54(3) Bus. Horizons 241, 244-245 (2011), https://doi.org/10.1016/j.bushor.2011.01.005

755 "Edge" refers to the connection/ relationship between nodes (individuals or objects) in social network analysis.

756 *Online Social Networks*, ScienceDirect Topics, https://www.sciencedirect.com/topics/computer-science/online-social-networks (last visited Jan. 15, 2026).

On centralized platforms, such as Facebook or X, the social graph is owned and controlled by the platform operator and constitutes one of its most valuable proprietary assets. Exclusive access to this data enables platforms to optimize engagement, personalize content, and extract economic value, while also creating strong barriers to user exit and interoperability. By contrast, blockchain-based social networks —and, more broadly, decentralized social network protocols— aim to make the social graph open, portable, and user-controlled. Identity and relationship data are recorded in shared, interoperable infrastructures rather than locked into proprietary databases. Users can, in principle, carry their identity and social relationships across applications that rely on the same protocol or blockchain-based data layer, as seen in ecosystems, such as Lens or Farcaster. Multiple applications can read from the same identity and social-graph layer, enabling interoperability and reducing dependence on any single platform or interface. While such systems do not eliminate power asymmetries, they shift control away from vertically integrated platform operators toward protocol-level governance and shared infrastructure.[757]

2. Leveraging Blockchain Features

In many blockchain-based social media systems, the blockchain functions as a tamper-evident and auditable public ledger that anchors identities, records social-graph operations, or secures pointers to off-chain content. Rather than relying on proprietary databases controlled by a single entity, these platforms rely on shared, verifiable infrastructures that constrain unilateral changes and increase transparency.

Governance arrangements vary across projects. Some systems rely on on-chain governance mechanisms, such as token-based voting for protocol changes, while others adopt hybrid models in which governance processes occur partly off-chain but remain publicly visible. In all cases, the blockchain layer reduces dependence on a single operator and limits the ability of any one actor to alter core rules without broader participation.

Blockchain immutability and auditability are often presented as trust-enhancing features, particularly for users concerned about opaque moderation or algorithmic curation on centralized platforms.[758] In practice, most blockchain-based social networks avoid storing full content directly on-chain. Instead, they record identity primitives, social-graph actions, or content hashes on the blockchain, while storing posts and media in off-chain decentralized storage systems such as IPFS[759] or Arweave.[760] This design preserves verifiability and tamper-evidence without overloading the blockchain or creating irreversible publication of sensitive content.[761]

Another hallmark of blockchain-based social media is a focus on interoperability and data portability. Users can control their identifiers and social connections and carry them across different applications built on the same protocol, reducing lock-in and dependence on any single service provider. Instead of user data residing in proprietary centralized databases, identity and relationship information is recorded in shared, open infrastructures, while content is stored in decentralized storage. User content can be accessed by any application that can read from the blockchain.

757 Zhan, Xiong & Xing, *supra* note 739.

758Rozenshtein, *supra* note 741.

759 *InterPlanetary File System*, IPFS, https://ipfs.tech/ (last visited Jan. 15, 2026).

760 *Arweave: A Community-Driven Ecosystem*, ARWEAVE, https://arweave.org/ (last visited Jan. 15, 2026).

761 Mayank Jain et al., *supra* note 752, at 2-3, 7.

3. Advantages and Disadvantages

Blockchain-based social media platforms reassign core platform functions —such as identity management, social-graph ownership, and value distribution— from centralized operators to users and protocol communities. Some projects introduce native tokens or tokenized assets that structure incentives within the network, rewarding activities such as posting, curation, or governance participation. These tokens may also confer governance rights or access to revenue-sharing mechanisms.

This model has given rise to *SocialFi* ("Social Finance"), which integrates social networking with decentralized finance.[762] With traditional social media, economic value is generated by user interactions and is largely captured by platform operators. SocialFi systems allow users to own, monetize, or transact around their data and content. Some platforms also integrate DeFi services, such as lending, trading, or micropayments, directly into social interactions. Examples include Steemit, which rewards engagement with tokens and applications built on the DeSo (decentralized social) blockchain. Other blockchain-based social networks, such as Lens or Farcaster, deliberately avoid engagement-for-reward mechanisms. Instead, they use blockchain primarily to enable portability and user control rather than financialized participation.

These architectures can reduce exposure to centralized data extraction and unilateral platform policies, but they also impose new responsibilities on users. Managing keys, backups, content discovery, and governance participation can be complex and burdensome. Moderation presents a particularly acute challenge.[763] Because on-chain data cannot be easily altered or removed, moderation typically shifts to the application layer, where individual clients apply their own filters, block lists, and content policies.[764] Users may be required to participate actively in moderation processes or to curate their own content environments.[765]

Various approaches have been proposed to address these challenges, including community-based voting systems and incentive mechanisms for moderation,[766] as well as automated moderation tools based on artificial intelligence. Each approach raises trade-offs related to scalability, accuracy, cost, and accountability.[767]

Finally, blockchain's resistance to censorship complicates the removal of harmful or unlawful content. Even when full content is stored off-chain, metadata or content references recorded on a blockchain may be permanent. A well-known example occurred in 2019, when Steemit banned a hacker group that demanded a bitcoin ransom in exchange for releasing documents related to the September 11 attacks.[768] While access was blocked through Steemit's interface, the underlying content remained visible through alternative interfaces accessing the Steem blockchain, illustrating the difficulty of suppressing information once it is anchored to an immutable ledger.[769]

---

762 Zhan, Xiong & Xing, *supra* note 739, at 2 -3.

763 *See generally* Ujun Jeong et al., *Navigating Decentralized Online Social Networks: An Overview of Technical and Societal Challenges in Architectural Choices*, arXiv (Mar. 31, 2025), https://arxiv.org/abs/2504.00071.

764 *Id*., at 11-14; Gian Marco Bovenzi, *Content Moderation in (Decentralized) Metaverses*, in Proceedings of the International Congress Towards a Responsible Development of the Metaverse, 11-13 (June 13–14, 2024), https://catedrametaverso.ua.es/wp-content/uploads/2024/07/Content-moderation-in-decentralised-metaverses-BOVENZI.pdf.

765 Wenrui Zuo et al., *Understanding and Improving Content Moderation in Web3 Platforms*, 18 Proc. Proc. Int'l AAAI Conf. on Web & Soc. Media 1859 (2024), https://doi.org/10.1609/icwsm.v18i1.31431.

766 Christian Teguh Prasetya Widjaja, Moeljono Widjaja, & Arya Wicaksana., *Community-Driven Moderation in Blockchain-Based Social Media*, *in* Proc. 6th Int'l Conf. on Computational Intel. & Intel. Sys., 181(2023), https://doi.org/10.1145/3638209.3638236.

767 Bovenzi, *supra* note 764, at 12.

768 Ramon Casadesus-Masanell et al., *Steemit: A New Social Media*, Harvard Bus. Sch. Case No. 720-034 (2019), https://www.hbs.edu/faculty/Pages/item.aspx?num=57393.

769 Hamid Khobzi, Ana Isabel Canhoto & Mohammad Sadegh Ramezani, *Content Creators at a Crossroads Between Decentralized and Centralized Social Media*, 68 Bus. Horizons 109, 114 (2025), https://doi.org/10.1016/j.bushor.2024.04.010

4.6.2. Examples

The blockchain-based platforms examined in this section —Lens, Farcaster, DSNP, and Steem— each combine decentralization and distribution differently, and the degree to which decentralization in governance design translates into decentralization in infrastructure and control in practice varies significantly across them.

4.6.2.A. Lens Protocol

Lens Protocol is a social-graph protocol originally deployed on the Polygon blockchain. Since 2024, the ecosystem has been migrating to Lens Chain, a dedicated Layer-2 network built using zero-knowledge technology and designed specifically to support decentralized social applications.[770] It enables decentralized control over user identity and provides flexible, distributed storage options. Lens describes itself as "a composable and decentralized social graph helping creators take ownership of their content wherever they go in the digital garden of the decentralized internet."[771] This protocol allows users to interact, publish content, and manage their social graph within a decentralized framework. Additionally, it enables users to transfer their connections (social graph) to any application built on Lens.[772]

Lens users create and publish unique profiles represented by non-fungible tokens (NFTs). One example is the *Profile NFT*, which serves as a unique, on-chain identifier for users and establishes ownership of a Lens profile.[773] For instance, through their Profile NFTs, users can build their social graph by following others and engaging with content shared across Lens applications.[774] Although the Profile NFT anchors identity, content itself (posts, comments, quotes) is stored off-chain with on-chain references. Users expand their social graph by following others: *Follow NFTs* are minted when a user follows another profile.[775] Follow NFTs can be used to implement governance mechanisms within specific Lens-based communities, but they do not inherently grant protocol-wide governance rights.

Lens NFTs serve multiple functions within the Lens ecosystem. Profile and Follow NFTs are ERC-721-compatible, enabling interoperability across decentralized applications that adhere to Ethereum standards.[776] This interoperability allows users to port their Lens identity across compatible applications while maintaining ownership of their social graph.[777]

Additionally, Lens users can assign specific permissions and tasks to other wallet addresses, known as delegated executors (or profile managers).[778] These delegated executors can act on behalf of the profile owner — for example, by publishing content, following other profiles, updating metadata, or performing other profile-management operations. This feature simplifies profile administration while preserving the user's ultimate control and ownership. Permissions granted to delegated executors can be revoked by the profile owner at any time.[779]

770 Lens Labs, *Migrating the Lens Ecosystem to Lens Chain*, Lens Protocol (Feb. 25, 2025), https://lens.xyz/news/migrating-the-lens-ecosystem-to-lens-chain.)

771 *Introduction: What is Lens Protocol?*, Lens Protocol, https://lens.xyz/docs (last visited Jan. 15, 2026). Following the transition to Mask Network in January 2026, parts of the Lens ecosystem are being reconfigured, temporarily making some links or interfaces inaccessible, particularly as third-party front ends are migrated or discontinued. Lens Labs, *Mask Network to Steward the Next Chapter of Lens*, Lens Protocol (Jan. 20, 2026), https://lens.xyz/news/mask-network-to-steward-the-next-chapter-of-lens.

772 *Lens Graph*, Lens Docs, https://lens.xyz/docs/protocol/concepts/graph (last visited Jan. 15, 2026) (explaining how the on-chain graph allows applications to build and manage audiences interoperably).

773 *Profile NFT*, Lens Protocol; *see also* Blockbytes, *Lens Protocol*, https://blockbytes.com/2022/12/09/lens-protocol/#profile-nfts (last visited Jan. 15, 2026).

774 *Social Primitives*, Lens Protocol (demonstrating how "Follow," "Collect," and "Mirror" actions construct the on-chain graph).

775 *Follow,* Lens Protocol.

776 *Social Primitives*, Lens Protocol.

777 *Lens Graph*, *supra* note 772.

778 *Profile Manager*, Lens Protocol. This refers to the ability of Lens users to specify Uniform Resource Identifiers (URIs), which point to additional metadata associated with their profiles that provides more context about the user or their profiles. Set profile metadata, Lens Protocol.

779 *Profile manager*, Lens Protocol.

4.6.2.B. Steem

Launched in 2016, Steem is a blockchain-based social media network that introduced the novel feature of rewarding users for creating and curating content. Its incentive model distributes native tokens to participants, thereby offering economic rewards and the possibility of influence in platform governance through token staking. Steem employs a Delegated Proof-of-Stake (DPoS) consensus mechanism, processing blocks every three seconds, ensuring scalability suitable for high-volume social interactions.[780]

The Steem blockchain underlies a range of applications with built-in reward systems,[781] including Steemit, its flagship blogging platform (comparable to Reddit or Medium);[782] DTube, a decentralized alternative to YouTube;[783] and Actifit, a fitness application that rewards physical activity. Users who create and curate content on any of these platforms or other platforms built on Steem blockchain are rewarded with tokens. These rewards include STEEM, the native cryptocurrency; STEEM Power, a staked form of STEEM used to increase voting influence; and Steem Dollars (SBD), a stablecoin-like asset pegged to the U.S. dollar. Smart Media Tokens (SMTs), originally envisioned as customizable tokens for Steem-based applications, were never fully launched and remained largely unrealized.[784]

The Steem blockchain is an open-source, permissionless, decentralized protocol governed through its Delegated Proof-of-Stake (DPoS) system. Holders of STEEM Power (staked STEEM tokens) elect witnesses (validators) who maintain the blockchain.[785] By contrast, Steemit Inc. was a private U.S. company that developed and operated Steemit.com, the flagship blogging platform built on the Steem blockchain. The company also held a large, privately pre-mined allocation of STEEM tokens, which gave it disproportionate influence over the blockchain's governance.[786]

In early 2020, Justin Sun, founder of TRON, acquired Steemit Inc. and, with it, Steemit's significant token holdings *(See above Figure 30)*. This acquisition was widely criticized as a de facto "hostile takeover," especially after Sun collaborated with major exchanges to use custodied customer tokens to seize governance control of the Steem blockchain.[787] In response, a large part of the Steem community forked the blockchain to create Hive, which sought to restore community-driven governance, free from corporate dominance.[788] Today, both Steem and Hive continue to operate as independent blockchain-based social media ecosystems.[789]

4.6.2.C. Farcaster

Farcaster is a decentralized social networking protocol[790] that leverages blockchain technology to provide users

780 Steemit, Inc., *Steem Bluepaper* 3 (2017), https://steem.com/steem-bluepaper.pdf [hereinafter Steem Bluepaper]; *see also Steem Whitepaper: An Incentivized, Blockchain-Based, Public Content Platform*, Steem, https://steem.com/steem-whitepaper.pdf (last visited Jan. 15, 2026);

781 Powering communities and opportunities, Steem, https://steem.com/ (last visited Jan. 15, 2026).

782 Steemit, https://steemit.com/ (last visited Jan. 15, 2026).

783 DTube, https://d.tube/ (last visited Jan. 15, 2026);

784 Steem Bluepaper, *supra* note 780, at 2–6; *What Is Steem (STEEM)*, CoinMarketCap, https://coinmarketcap.com/cmc-ai/steem/what-is/ (last visited Jan. 15, 2026).

785 Steem Bluepaper, *supra* note 780 at 3.

786 Shikhar Ghosh & Shweta Bagai, *Steem versus Hive: Testing Blockchain Governance*, Harvard Bus. Sch. Case No. 822-075, (Jan. 2022, rev. Apr. 2025), https://www.hbs.edu/faculty/Pages/item.aspx?num=61580.

787 *Id*.

788 *Id.; see also* Mike Dalton, *What are Steem and Hive? A Comparison of Both Decentralized Content Blockchains*, Crypto Briefing (Apr. 22, 2020), https://cryptobriefing.com/what-are-steem-hive-comparison-both-decentralized-content-blockchains/.

789 Mike Dalton, *supra* note 788.

790 Ilan Hazan & Benjamin White, *Farcaster Explained: The Blockchain-Powered Decentralized Social Media Protocol*, Decrypt (2024), https://decrypt.co/resources/farcaster-explained-the-blockchain-powered-decentralized-social-media-protocol (last visited Jan. 15, 2026).

with portable, decentralized identities.[791] Farcaster is developed on Optimism, an Ethereum Layer 2 network[792] and is described as a "sufficiently decentralized"[793] protocol that combines blockchain with off-chain infrastructure to balance decentralization and efficiency. The platform aims to create an experience similar to traditional social media while providing greater user ownership. Farcaster therefore adopts a hybrid architecture in which user identities are anchored on-chain through smart contracts on Optimism, while content and social interactions are handled off-chain. Historically, this off-chain layer has relied on a peer-to-peer network of nodes known as *Hubs*, which replicate user data and messages across the network. More recently, additional scaling components such as *Snapchain* have been introduced to provide higher throughput and improved coordination across the network.

Farcaster users own their identity through cryptographic keys, which can be used across different apps built on Farcaster.[794] Two broad categories of applications operate within the ecosystem:[795]

- Client apps, such as Warpcast,[796] a social media app similar to Twitter/X, that lets users post, follow, recast, and interact with others in the Farcaster network.
- Infrastructure components (e.g., Hubs, APIs), which relay and replicate messages and provide the technical backbone that allows the decentralized network to function and enables new applications to be built.[797]
- To Farcaster's founders, the real opportunity is in the infrastructure. Farcaster uses Warpcast, in part, as a product for convincing developers to build on its protocol and expand its network.[798]

Users own their accounts and social relationships with other users and can port their profiles across different apps developed through the protocol.[799] This enables Farcaster users to retain control over their profiles and continue interacting with their social graph regardless of attempts by the network or other third parties, such as other users, to prevent these interactions.[800]

To post content and communicate with other users on the network, users must register a unique numeric identifier known as a Farcaster ID (FID).[801] Farcaster users publish content on Farcaster applications through their FID,[802] which is controlled by an Ethereum custody address.

---

791 Farcaster Protocol, *Architecture Overview*, https://docs.farcaster.xyz/learn/architecture/overview (last visited Jan. 15, 2026).

792 FARCASTER, https://docs.farcaster.xyz/ (last visited Jan. 15, 2026).

793 Varun Srinivasan, *Sufficient Decentralization for Social Networks* (Jan. 11, 2022), https://www.varunsrinivasan.com/2022/01/11/sufficient-decentralization-for-social-networks (last visited Jan. 15, 2026).

794 Farcaster Protocol, *Protocol Overview Documentation*, https://github.com/farcasterxyz/protocol/blob/main/docs/OVERVIEW.md (last visited Jan. 15, 2026).

795 *Id*.

796 *Farcaster Created Crypto's Killer Social App: Warpcast*, PHANTOM, https://phantom.com/learn/crypto-101/farcaster-warpcast (last visited Jan. 15, 2026); *How To Use Farcaster and Warpcast*, ZERION (Jan. 19, 2024), https://zerion.io/blog/how-to-use-farcaster-and-warpcast-zerion-blog/ (last visited Jan. 15, 2026)

797 Coinbase, *What is the decentralized social media platform Farcaster?*, COINBASE https://www.coinbase.com/learn/crypto-basics/what-is-the-decentralized-social-media-platform-farcaster (last visited Jan. 15, 2026).

798 Gary Weinstein, *From Control to Community: Farcaster and the Future of Social Media*, FORBES, (Nov. 4, 2024) https://www.forbes.com/sites/digital-assets/2024/11/04/from-control-to-community-farcaster-and-the-future-of-social-media/.

799*Introduction,* FARCASTER, https://docs.farcaster.xyz/, (last visited Jan. 15, 2026).

800 Srinivasan, *supra* note 793.

801 Farcaster messages include the following types of content and actions: "casts," which are public messages published on Farcaster applications; "reactions" to casts made by Farcaster users; "links," which are connections between Farcaster accounts; profile data, which encompass Farcaster account metadata; and, verifications, which are proofs of ownership, FARCASTER, https://docs.farcaster.xyz/learn/what-is-farcaster/accounts (last visited Jan. 15, 2026).

802 *Accounts*, FARCASTER, https://docs.farcaster.xyz/learn/what-is-farcaster/accounts, (last visited Jan. 15, 2026).

Farcaster messages encompass user actions, such as likes, posts, and profile updates.[803] They are stored and replicated by Farcaster Hubs, off-chain servers that work somewhat similarly to Ethereum nodes[804] and support the operation of the Farcaster network.[805] Farcaster users delegate signer keys for each application, allowing apps to act on their behalf without exposing the Ethereum address that controls the FID.[806] Farcaster message authentication mechanisms rely on cryptographic signatures[807] that allow network nodes to verify that messages are validly signed, originate from the correct user, and have not been altered during propagation across the network.[808] Recent architectural developments, including the introduction of Snapchain, reflect ongoing efforts to balance decentralization with scalability and infrastructure coordination.[809]

4.6.2.D. Decentralized Social Networking Protocol (DSNP)

The Decentralized Social Networking Protocol (DSNP) is an open-source protocol released by nonprofit Project Liberty in 2021[810] and designed to support decentralized social networks. DSNP is built on open standards that allow developers to create interoperable applications without relying on proprietary platforms. The protocol relies on a consensus system —often implemented using blockchain technology— to record key protocol events and manage critical user information such as social graph data and cryptographic keys.

Although its reference implementation uses Ethereum, DSNP is technically ledger-agnostic and can operate on different blockchain-based or distributed ledgers.[811] It aims to create an open, shared social graph that does not depend on any specific application or centralized platform and gives users control over their identities and graph data.[812] DSNP works by recording protocol events —such as social graph updates and message "announcements"— on a consensus system, while the associated content is stored off-chain to improve scalability and efficiency.[813]

DSNP provides mechanisms to help ensure the integrity and authenticity of user data by anchoring cryptographically signed protocol events and content hashes on a public ledger, creating a transparent and auditable activity record.[814] Users keep cryptographic control over the information they share, and their data can move easily across different applications.[815] The protocol is designed to support interoperability among social networking clients.[816]

---

803 *Messages*, https://docs.farcaster.xyz/learn/what-is-farcaster/messages, Farcaster (last visited Jan. 15, 2026).

804 Lemniscap, *Breaking Down Walled Gardens: Farcaster and Decentralised Social Media*, PARAGRAPH, (Feb. 12, 2024), https://paragraph.com/%40lemniscap/breaking-down-walled-gardens-farcaster?utm_source (last visited Jan. 15, 2026).

805 *Id.*

806 *Accounts*, https://docs.farcaster.xyz/learn/what-is-farcaster/accounts, Farcaster (last visited Jan. 15, 2026).

807 Srinivasan, *supra* note 793.

808 Farcaster Protocol, *Protocol Overview Documentation*, https://github.com/farcasterxyz/protocol/blob/main/docs/OVERVIEW.md (last visited Jan. 15, 2026).

809 Farcaster Improvement Proposal: Snapchain, Farcaster (2024), https://github.com/farcasterxyz/protocol/discussions/207 (describing Snapchain as a new consensus and scaling architecture replacing the earlier hub-based coordination model to improve throughput and reliability).

810Project Liberty, *DSNP*, https://www.projectliberty.io/dsnp/ (last visited Jan. 15, 2026).

811 Project Liberty, Decentralized Social Networking Protocol (DSNP), 1, 3 (2024) https://dsnp.org/dsnp_whitepaper.pdf.

812 *Id*. at 2, 4.

813 *Id*. at 5, 14.

814 *Id*. at 15-16.

815 *Id*. at 4, 8-9.

816 *Id*. at 3.

DSNP is comprised of three core elements:[817]

1. **identity**, representing each user through a keypair and, in some implementations, user-controlled on-chain data or "individually owned smart contracts" representing a social identity;
2. **the social graph**, which records relationships between identities as protocol events anchored on the consensus system; and
3. **messaging**, which uses on-chain message announcements that link to off-chain content.

1. Identity

Unlike traditional social networks, where accounts are and data are controlled by the platform, DSNP identities are controlled directly by users through a cryptographic keypair typically managed through a digital wallet. Users may create multiple social identities, each attached to a distinct and "uncorrelated" control key or wallet address, thereby preserving privacy and enabling separate online personas.[818] This structure ensures that users retain control over their identity data without relying on a centralized account management system.

Users manage the cryptographic keypair associated with their identifier, and, if they so choose, may retire the identifier.[819] In some implementations, a user's identity may be represented through user-controlled data stored on-chain or through a smart contract that functions as the user's programmable identity. [820] Users may create, update or delete content associated with their identifier and may delegate specific permissions to third parties or applications to perform certain actions on their behalf without transferring ownership of the identity.

2. Social Graph

DSNP's social graph charts the relationships and connections among users of the protocol (i.e., social identities). These relationships are encoded as protocol events published to the consensus system and are primarily modeled as directed "follow" relationships, which can serve as the basis for more complex relationship types such as "friend" connections.[821] Users may choose to make their connections public or private. Public relationships are visible to all network participants, while private relationships are stored as encrypted events; the encrypted event is still posted on-chain, but only users possessing the decryption key can interpret it.[822]

Changes to the social graph —for example, the creation or removal of a connection— are represented as graph change events. These changes are released through operations associated with a user's social identity on the consensus system, thereby providing a verifiable chronological record of graph updates associated with that identity. While graph change events are publicly recorded, DSNP also supports private graph events: Although these appear on the ledger, their contents remain inaccessible to third parties without the decryption key.[823]

DSNP social graph data is portable. Users can share their social graphs with third parties by sending their symmetric keys via an encrypted direct channel.[824] This access is strictly read-only —third parties cannot alter graph data

817 *Id*. at 4.
818 *Id*. at 6.
819 *Id*. at 6-7.
820 *Id*. at 5-6.
821 *Id*. at 9.
822 *Id*. at 10.
823 *Id*. at 12.
824 *Id*. at 12. A symmetric key is a single key that is shared between a sender and a user for both encrypting and decrypting data.

or generate new DSNP events.[825] DSNP users can revoke access to new graph change events on their social graph by assigning a new value to the access symmetric key, ensuring that third parties cannot read newly added events.

3. Messaging

Decentralized Social Networking Protocol users can employ messages to communicate with each other. DSNP messages may also be used to link to off-chain content. Messages are represented as message announcements recorded on the consensus system and are published through operations associated with the user's social identity. The sender initiates the message by publishing a message announcement referencing the location of the message content.[826] The recipient then retrieves, authenticates, and interprets the message content. Message authenticity is ensured by matching the hash embedded in the on-chain announcement with the hash of the retrieved content.[827] The message body itself is never stored on-chain, which preserves scalability and reduces costs.[828]

While the DSNP protocol presents itself as an open technical standard for social networking infrastructure, similar to SMTP for email or HTTP,[829] it has been advanced primarily through initiatives associated with the Project Liberty ecosystem. For example, MeWe, a 20-million-member global social network, has integrated with DSNP through Frequency, a Polkadot-based blockchain infrastructure,[830] designed to support decentralized social networking systems inspired by DSNP.[831] In 2023, MeWe had transitioned almost a million of its users to controlling their own social identity using DSNP.

Overall, blockchain-based social media architectures face persistent challenges related to moderation, scalability, governance design, token concentration, infrastructure dependency, and regulatory compliance. As in other blockchain domains, decentralization tends to redistribute authority rather than eliminate it, and hybrid models — combining on-chain anchoring with off-chain content storage and application-layer governance— remain the dominant practical configuration.

4.7. BLOCKCHAIN-BASED DISPUTE-RESOLUTION (BDR) MECHANISMS

Parties to blockchain transactions increasingly explore blockchain-based dispute-resolution (BDR) mechanisms, particularly because cross-border activity, pseudonymity, and automation make traditional litigation slow or difficult to apply to smart-contract disputes *(See section 6.5.2.B.)*.[832] In addition, many blockchain-native users value decentralization and prefer mechanisms that reflect similar design principles, such as transparency, automation, and limited reliance on centralized intermediaries.[833] Blockchain-based mechanisms for resolving disputes are intended to address the specific challenges of blockchain environments: the cross-jurisdictional nature of transactions, the technical

825 *Id.* at 12-13.

826 *Id.* at 14-17.

827 *Id*. at 16.

828 *Id*. at 5, 21.

829 *Reimagining Social Media: The Promise of Distributed Social Networking Protocol (DSNP),* Social Media (June 17, 2025, https://www.sociaimedia.com/p/reimagining-social-media-the-promise.

830 *See* DSNP *MeWe and Social Media*, https://dsnp.org/about/MeWe-use-case.html (last visited Jan. 15, 2026).

831 MeWe, *MeWe and Frequency Enable World's Largest Migration to Decentralized Social*, PR Newswire (Nov. 14, 2023), https://www.prnewswire.com/news-releases/mewe-and-frequency-enable-worlds-largest-migration-to-decentralized-social-301987495.html.

832 Federico Ast & Bruno Deffains, *When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice*, Stanford J. Blockchain L. & Policy, 248 (2021), https://stanford-jblp.pubpub.org/pub/birth-of-decentralized-justice/release/1.

833 Ast & Deffains, *supra* note 832 at 242.

complexity of smart-contract execution, and the difficulty of identifying contracting parties.[834]

BDR mechanisms can be understood as a new branch of Online Dispute Resolution (ODR),[835] sharing with ODR the use of digital processes, while introducing distinct features made possible by blockchain.[836] These include blockchain-based arbitration, in which arbitrators with technical expertise resolve disputes according to legal standards and issue awards.[837] They also include "decentralized justice" systems,[838] which rely on smart contracts, crypto economic incentives, and pseudonymous jurors, rather than traditional legal reasoning. Arbitration is widely viewed as a suitable method for resolving smart-contract disputes, given its flexibility,[839] its capacity to incorporate specialized technical knowledge, and the relative ease of international enforcement of arbitral awards.[840] By contrast, decentralized-justice platforms render decisions through algorithmic or crypto-economic mechanisms —such as token-curated juries incentivized to reach coherent outcomes— rather than through conventional legal analysis.

Decentralized-justice systems resolve disputes through smart contracts that automate procedural steps, cryptographic techniques that authenticate submissions or trigger conditions, and crypto-economic incentive schemes that often derive from game theory to align juror decisions with expected fair outcomes.[841] Many decentralized justice systems use pseudonymous token holders as jurors who are rewarded for voting with the eventual consensus and penalized for dissenting.[842] Because these systems are built directly into blockchain infrastructures, their rulings can often be enforced "on-chain:" releasing escrowed assets, updating ownership records, or modifying parameters of a decentralized autonomous organization (DAO).[843] Where the subject matter remains on-chain, enforcement may occur automatically without the need for external courts or institutions.

Several notable BDR systems illustrate these developments. Aragon Court was one example. It was a decentralized arbitration mechanism designed to resolve disputes arising within decentralized autonomous organizations and blockchain-based platforms.[844] Kleros, another example, is a decentralized justice system built on the Ethereum

834 *See generally* Peter L. Michaelson & Sandra A. Jeskie, *Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts*, 74(4) Disp. Resol. J. 89 (2020), https://ssrn.com/abstract=3720876.

835 *See* American Arbitration Association, *Online Dispute Resolution*, ADR, https://www.adr.org/odr/ (last visited Jan. 9, 2026).

836 *See generally* Bianca Kremer, *Blockchains, Smart Contracts, and International Arbitration: The Emergence of a Crypto Autonomous Legal Order* (Sept. 19, 2022), (Ph.D. dissertation, Universität St. Gallen), https://www.alexandria.unisg.ch/handle/20.500.14171/108251. *See also* Michael Buchwald, *Smart Contract Dispute Resolution: The Inescapable Flaws Of Blockchain Based Arbitration*, 168 U. Penn. L. Rev. 1369, 1376 (2020), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn_law_review.

837 Michaelson & Jeskie, *supra* note 834 at 100.

838 Ast & Deffains, *supra* note 832 at 241, 247-253 (defining decentralized justice as requiring: (1) DAO structure on blockchain technology, (2) cryptoeconomic mechanism design, and (3) generation of perceptions of fairness);Federico Ast et al., *Decentralized Justice: State of the Art, Recurring Criticisms and Next-Generation Research Topics*, 6 Frontiers Blockchain 1 (2023), https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2023.1204090/full.

839 Michaelson & Jeskie, *supra* note 834, at 123-126.

840 *Id.*, at 128-130.

841 Ast & Deffains, *supra* note 832 at 250-251.

842 *Id.* at 248; *see also* Clément Lesaege, Federico Ast & William George, *Kleros Short Paper v1.0.7* 6-8 (Sept. 2019), https://kleros.io/whitepaper.pdf.

843 *See generally* Florence Guillaume & Sven Riva, *Blockchain Dispute Resolution for DAOs: The Rise of Decentralized Autonomous Justice*, in Blockchain and Private International Law, 602-641, (Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani eds., 2023), https://ssrn.com/abstract=4042704.

844 This conflict resolution mechanism relied on volunteer, non-expert judges to adjudicate commercial disputes through a community of jurors incentivized to render fair decisions using a staking mechanism. These jurors were randomly selected from a pool of token holders and were economically motivated to issue accurate and impartial verdicts. Those who voted with the majority were rewarded with dispute fees and a portion of tokens from those who voted with the minority. In 2023, the Aragon Association voted to dissolve and transferred product stewardship —including the legacy Court module— to a new structure; Aragon, *A New Chapter for the Aragon Project*, Aragon Blog (Nov. 2, 2023), https://blog.aragon.org/a-new-chapter-for-the-aragon-project/.

blockchain which uses token-based juries and incentive mechanisms to resolve a wide range of on-chain disputes.[845]

FIGURE 34.

The Kleros Court

When a dispute is submitted to the Kleros Court, jurors are drawn from a pool of users who have staked the platform's native token, Pinakion (PNK).[846] Both disputing parties must pay arbitration fees, while jurors lock PNK as stake, which may be partially forfeited, depending on the outcome.

Most dispute resolutions begin with a panel of three randomly selected jurors, who vote independently, typically on a binary (yes/no) basis, although more complex decision formats are possible depending on the smart contract. Once the jury reaches a majority decision, jurors who voted with the majority receive rewards funded by arbitration fees and a redistribution of PNK. Minority jurors lose a portion of their staked PNK. The losing party in the dispute ultimately bears the costs of the proceeding.

The system allows for multiple rounds of appeal, with each appeal requiring a larger jury and additional fees. In practice, the number of feasible appeals is limited by the number of jurors who have staked PNK, as each successive round requires more jurors and higher payments from the disputing parties.[847]

Designed to be transparent and decentralized, Kleros and similar dispute resolution mechanisms aim to offer an alternative to traditional courts by relying on crypto-economic incentives rather than institutional authority. Their design draws on a concept from game theory known as the Schelling point, or focal point.[848] The idea is that individuals tend to converge on the outcome they believe others will also select, based on shared expectations of what appears most reasonable or obvious. Because jurors are rewarded for voting with the eventual majority and penalized for diverging from it, they face economic incentives to coordinate on the outcome they anticipate other rational jurors will choose —typically the option that seems most intuitively obvious, natural, or fair within the context of the dispute.

Although these decentralized ODR systems may lack many procedural and substantive safeguards associated with judicial or arbitral processes —including formal due process guarantees, evidentiary rules, or institutional oversight— they are designed to generate outcomes that reflect widely shared intuitions about fairness, coherence, and efficiency within their user communities.[849]

845 Guillaume & Riva, *supra* note 843, at 616-619; Luis Bergolla, Karen Seif & Can Eken, *Kleros: A Socio-Legal Case Study of Decentralized Justice & Blockchain Arbitration*, 37 Ohio St. J. on Dispute Resolution 55-98 (2022), https://law.stanford.edu/wp-content/uploads/2022/10/10-BERGOLLA-55-98.pdf.

846 *See generally* Anna Zhuk, *Applying Blockchain to the Modern Legal System: Kleros as a Decentralised Dispute Resolution System*, 4 Int'l Cybersecurity L. Rev. 351-364 (2023), https://doi.org/10.1365/s43439-023-00086-x; Ast & Deffains, *supra* note 832.

847 Maahi Agarwal, *From Social Contracts to Smart Contracts: Navigating Decentralization, Blockchain and Kleros Arbitration*, Contemp. L. F. (Mar. 18, 2024), https://tclf.in/2024/03/18/from-social-contracts-to-smart-contracts-navigating-decentralization-blockchain-and-kleros-arbitration/.

848 Lucas Bergolla, Kerem Eken & Can Seif, *Kleros: A Socio-Legal Case Study of Decentralized Justice*, 37 Ohio St. J. On Disp. Resol. 55 (2022), https://ssrn.com/abstract=3918485; Yann Aouidef, Federico Ast & Bruno Deffains, *Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects*, 4 Frontiers Blockchain 1 (2021), https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2021.564551/full.

849 Guillaume & Riva, *supra* note 843, at 621-638; Florence Guillaume, *Decentralized Autonomous Organizations (DAOs) Before State Courts—How Can Private International Law Keep Up with Global Digital Entities?*, *in* Decentralised Autonomous Organization (DAO) Regulation: Principles And Perspectives For The Future, 164-168 (Madalena Perestrelo de Oliveira & Antonio Garcia Rolo eds., 2024), https://ssrn.com/abstract=4492934.

4.8. SUPPLY CHAIN

Global supply chains bring together actors scattered across multiple jurisdictions, making them highly vulnerable to geopolitical tensions, natural disasters, and sectoral disruptions. Effective management requires data exchange at the network level to build agility, ensure adaptability, and comply with regulatory obligations, including ethical sourcing and carbon footprint monitoring. Yet, global supply firms remain reluctant to share information with competitors or foreign authorities, partly due to confidentiality, competition risks, and data-protection constraints. They struggle to safeguard data security, maintain integrity, and retain control during data-sharing processes.

Blockchain technology offers potential solutions for global supply chains by facilitating secure and transparent exchanges. Through controlled access rights, immutable records, and verifiable audit trails, blockchain enables participants to share trade documents and operational data without losing control over sensitive information. This reduces bottlenecks, lowers transaction costs,[850] and enhances traceability, regulatory compliance, and coordination across otherwise siloed supply chain tiers.[851] Yet blockchain does not address the accuracy of off-chain data inputs, which still depend on trusted verification mechanisms.

Adoption, however, has not always been successful. While initiatives such as *WeTrade*, *Everledger*, and *TradeLens* demonstrated advanced technological capacity, each ultimately ceased operations due to structural obstacles. *WeTrade*, launched by a consortium of European banks to expand small and medium enterprise (SME) access to trade finance, closed in 2022 after losing investor backing and failing to develop a sustainable business model.[852] *Everledger*, founded in 2015 to track provenance in diamonds and luxury goods, collapsed in 2023 following the withdrawal of its largest investor and insufficient commercial revenues.[853] *TradeLens*, created by Maersk and IBM in 2018 to digitize shipping documentation, was discontinued in late 2022 following its announcement of industry reluctance to join a platform dominated by a single player, as well as the difficulty of achieving alignment in a fragmented sector.[854] These failures illustrate that the adoption of blockchain for supply chains requires not only technical expertise but also regulatory clarity, durable financing, and consensus around governance of permissioned networks.

By contrast, other blockchain applications have demonstrated tangible benefits. In the automobile industry *(See Appendix 8)*, blockchain ensures provenance and end-to-end traceability of vehicles. It enables manufacturers, logistics providers, and dealers to securely share real-time data while retaining ownership and complying with regulatory requirements. In global shipping, blockchain-based electronic Bills of Lading (eBLs) reduce errors, improve efficiency, and address supply chain disruptions *(See Appendix 9)*. In sustainability, blockchain-based bookkeeping and digital product passports allow suppliers to demonstrate recycled content. This approach

850 Biswaksen Mishra, et al., *Blockchain adoption in automotive supply chain: A systematic literature review amalgamated with bibliometric analysis technique and future research directions,* 81 Tech Soc'y102775, https://doi.org/10.1016/j.techsoc.2024.102775

851 Maher A. N. Agi, & Jha, Abhinav Kumar Jha, *Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption,* 247 Int'l J. Prod. Econ. 108458, https://doi.org/10.1016/j.ijpe.2022.108458.

852 Eleanor Wragg, *we.trade calls it quits after running out of cash*, Global Trade Review (June 6, 2022), https://www.gtreview.com/news/top-stories/we-trade-calls-it-quits-after-running-out-of-cash/.

853 Tess Bennett, *Government and Tencent-backed Aussie blockchain firm collapses*, Financial Review (May 8, 2023), https://www.afr.com/technology/government-and-tencent-backed-aussie-blockchain-firm-collapses-20230503-p5d58l.

854 Supply Chain Movement Quarterly, *Maersk and IBM pull the plug on TradeLens, supply chain movement*, Supply Chain Movement Quarterly (Dec. 15, 2022),https://www.supplychainmovement.com/maersk-and-ibm-pull-the-plug-on-tradelens/#:~:text=AP%20Moller-Maersk%20and%20IBM,is%20no%20longer%20sufficiently%20viable.

substantiates sustainability claims without disclosing sensitive data, thereby supporting compliance with environmental regulations *(See Appendix 10)*. Together, these applications highlight how blockchain, when supported by sound governance and viable business models, can enhance transparency, efficiency, and resilience in global supply chains.

4.9. DECENTRALIZED AI

Decentralized Artificial Intelligence (DeAI) refers to the design, training, and deployment of artificial intelligence systems across decentralized networks, rather than within a single centralized infrastructure.[855] Most AI models (especially large-scale systems) rely on centralized computational resources, data pipelines, and governance structures. This raises concerns about data privacy, opacity, and concentration of power. Blockchain-based approaches aim to mitigate these issues by providing transparency and decentralized coordination. Although DeAI initiatives are still emerging, many projects seek to democratize access to compute and data, limit excessive centralization, enhance privacy, and improve system resilience.[856]

Blockchain contributes several functionalities relevant to DeAI.[857] Decentralization reduces single points of failure and mitigates the risks associated with centralized data repositories or model stores. Cryptographic techniques and smart-contract-based permission controls help prevent tampering and ensure that only authorized parties can access sensitive information. Immutable ledgers reinforce transparency and auditability.[858] Token-based incentives reward data providers, model trainers, and validators, while tokenization enables datasets, models, and computational resources to be exchanged in decentralized marketplaces with transparent provenance and programmable access rules.[859] In most systems, the blockchain serves as the coordination and verification layer, while the computational workloads themselves run off-chain on distributed nodes.

Blockchain coordination allows compute users and providers to interact without relying on centralized cloud platforms,[860] including through decentralized marketplaces for compute, data, and models (e.g., Sahara AI,[861] IO.NET,[862] Akash Network[863]). Several decentralized training platforms, such as FLock.io,[864] Bittensor,[865] Numer.ai,[866] DisTrO,[867] use blockchain

855 Vid Keršič & Muhamed Turkanović, *A Review on Building Blocks of Decentralized Artificial Intelligence*, ICT Express, 486 (June 2025), https://doi.org/10.1016/j.icte.2025.04.001; see *also* Zhipeng Wang et al., *SoK: Decentralized AI (DeAI)*, ArXiv, 1-2 (Nov. 2024), https://arxiv.org/abs/2411.17461; Charlyn Ho, *The Era of Decentralized AI*, Forbes (Mar. 15, 2025), https://www.forbes.com/sites/digital-assets/2025/03/15/the-era-of-decentralized-ai/.

856 Mohamad Sheikho Al Jasem, Trevor De Clark & Ajay Kumar Shrestha, *Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems*, 16 Information 765 (2025), https://doi.org/10.3390/info16090765.

857 Wang et al., *supra* note 855, at 4.

858 *Id.,* at 6.

859 *Id.,* at 6.

860 *See* Attia Qammar et al., *Securing Federated Learning with Blockchain: A Systematic Literature Review*, 56 Artificial Intelligence Rev. 3951 (2022), https://link.springer.com/article/10.1007/s10462-022-10271-9.
Yanna Jiang et al., *Blockchained Federated Learning for Internet of Things: A Comprehensive Survey*, 56(10) ACM Computing Surveys, 258 (2024), https://arxiv.org/abs/2305.04513.

861 *Sahara AI: The Decentralized Blockchain Platform for an Open, Equitable, and Collaborative AI Economy* (2024), https://saharalabs.ai/learn/litepaper; Wang et al., *supra* note 855, at 8.

862 *What is the Internet of GPUs?* (2024), https://docs.iog.net/docs/what-is-the-internet-of-gpus; Wang et al., *supra* note 855, at 6.

863 Greg Osuri & Adam Bozanich, *AKT: Akash Network Token & Mining Economics* (2020), https://akash.network/roadmap/aep-5/economics.pdf; Wang et al., *supra* note 855, at 6.

864 FLock.io, *Flock: Federated Machine Learning on Blockchain* (2024), https://www.flock.io/whitepaper; Wang et al., *supra* note 855, at 7.

865 Yuma Rao, *Bittensor: A Peer-to-Peer Marketplace for Artificial Intelligence* (2021), https://bittensor.com/whitepaper.; Wang et al., *supra* note 855, at 7.

866 *Numerai Documentation* (2024), https://docs.numer.ai/; Wang et al., *supra* note 855, at 7.

867 Bowen Peng et al, *A Preliminary Report on DisTrO*, GitHub https://github.com/NousResearch/DisTrO/blob/83aa657ce7e1a088dd849bedc5978eacaa4880db/A_Preliminary_Report_on_DisTrO.pdf (last visited Jan. 15, 2026)

to coordinate and incentivize distributed model development.[868] Blockchain also supports decentralized and verifiable inference. Zero-knowledge systems,[869] such as Sertn, allow participants to prove that an inference was executed correctly without revealing underlying data, model parameters, or intermediate computations.[870] ORA implements "optimistic machine learning,"[871] in which inference outputs are presumed correct unless challenged, with interactive fraud-proof protocols enabling participants to contest suspicious results and pinpoint divergences.

Blockchain also supports emerging agentic AI ecosystems, where autonomous or semi-autonomous agents interact within decentralized environments. In such settings, identity, verification mechanisms, and token-based incentives enable agents to exchange resources, share data, and coordinate tasks without centralized intermediaries. Although still at an early stage, practical experimentation with decentralized agent frameworks is rapidly expanding. Early frameworks include the Layered Orchestration for Knowledgeful Agents (LOKA) protocol, which combines DIDs and smart contracts with a "Decentralized Ethical Consensus Protocol" to constrain agent behavior.[872] Other early frameworks are the Intelligent System of Emergent Knowledge (ISEK),[873] which uses blockchain-based reputation and incentives to coordinate human and AI agents; and Fetch.ai, which provides a decentralized marketplace for autonomous agents.[874]

Interoperability efforts are emerging alongside these developments. The Model Context Protocol (MCP)[875] developed by Anthropic, is primarily designed to connect AI systems to external tools and data sources,[876] while the Agent2Agent (A2A) protocol enables different agents to communicate and coordinate tasks across platforms.[877] Yet these protocols operate primarily at the communication level: They let agents talk to one another, but they do not help agents confirm to whom they are talking, assess whether the other party is trustworthy, or transfer payments for completed tasks. To fill these gaps, researchers argue that interoperability protocols should be combined with blockchain-based identity, verification, and incentive mechanisms, which would allow agents to collaborate reliably and transact in a decentralized, economically viable way.[878]

868 *See generally* Juncen Zhu et al., *Blockchain-Empowered Federated Learning: Challenges, Solutions, and Future Directions*, 55ACM COMPUTING SURVEYS, 240 (2023), https://dl.acm.org/doi/10.1145/3570953;
XiaoHui Yang & TianChang Li, *A Blockchain-Based Federated Learning Framework for Secure Aggregation and Fair Incentives*, 45 CONNECTION SCIENCE (2024), https://www.tandfonline.com/doi/full/10.1080/09540091.2024.2316018.

869 Kasra Abbaszadeh et al., *Zero-Knowledge Proofs of Training for Deep Neural Networks*, PROC. 2024 ACM SIGSAC CONF. ON COMPUTER & COMMUNICATIONS SECURITY 3731 (CCS '24), https://doi.org/10.1145/3658644.3670316.

870 Colin Gagich et al., *Sertn - A Verified Inference Network* (Apr. 2024), https://public.inferencelabs.com/sertn-whitepaper.pdf.

871 KD Conway et al., *opML: Optimistic Machine Learning on Blockchain*, ARXIV (Jan. 2024), https://arxiv.org/abs/2401.17555; ORA, *see also Fraud Proof Virtual Machine (FPVM) and Frameworks* (2024), https://docs.ora.io/doc/onchain-ai-oracle-oao/fraud-proof-virtual-machine-fpvm-and-frameworks.

872 Rajesh Ranjan, Shailja Gupta & Surya Narayan Singh, *Loka protocol: A decentralized framework for trustworthy and ethical AI agent ecosystems*, ARXIV, https://arxiv.org/pdf/2504.10915 (last visited Jan. 15, 2026).

873 Wei, Moshi & Sparks Li, *Intelligent System of Emergent Knowledge: A Coordination Fabric for Billions of Minds*, ARXIV, https://arxiv.org/abs/2506.09335 (last visited Jan. 15, 2026)

874 *Fetch.ai Documentation* (2023), https://fetch.ai/blog/know-your-validator-staking-land.

875 Model Context Protocol, *Model Context Protocol Specification* (June 18, 2025), https://modelcontextprotocol.io/specification/2025-06-18.

876 Model Context Protocol, *What is the Model Context Protocol (MCP)?* Model Context Protocol https://modelcontextprotocol.io/docs/getting-started/intro (last visited Jan. 15, 2026).

877 Rao Surapaneni et al, *Announcing the Agent2Agent Protocol (A2A)*, Google for Developers (Apr. 9, 2025) https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/.

878 Awid Vaziry, Sandro Rodriguez Garzon & Axel Küppe, *Towards Multi-Agent Economies: Enhancing the A2A Protocol with Ledger-Anchored Identities and x402 Micropayments for AI Agents*, ARXIV (July 24, 2025), https://www.arxiv.org/pdf/2507.19550; *see also* Zhenhua Zou, et al., *BlockA2A: Towards secure and verifiable agent-to-agent interoperability,* ARXIV (Sept. 21, 2025), https://arxiv.org/pdf/2508.01332.

In any case, blockchains and interoperability standards cannot by themselves decentralize model training, access control, governance, or ownership, particularly for closed-source, commercially controlled AI models.[879] Recognizing these limitations, researchers at the Massachusetts Institute of Technology (MIT) launched Project NANDA (Network Agents and Decentralized AI), which calls for open protocols, capability indexes, and agent-level tools that would allow AI systems to operate within a decentralized, peer-to-peer network rather than under centralized corporate control.[880] These initiatives illustrate both the expanding ambition of decentralized AI governance and the considerable technical and institutional challenges that remain.

4.10. NETWORK STATES

The "network state" movement envisions digitally native communities that form online around shared values, mobilize capital and coordination through technology, and, in some cases, seek to acquire physical territory to operate as quasi-sovereign political entities.[881] These projects aim to function alongside —or potentially in place of— traditional nation-states, offering members an alternative to conventional citizenship and state authority.

The concept of the "network state" was formalized by Balaji Srinivasan in his 2022 book *The Network State: How to Start a New Country*.[882] In Balaji's words, "a network state is a highly aligned online community with a capacity for collective action that crowdfunds territory around the world and eventually gains diplomatic recognition from pre-existing states".[883] Unlike traditional nation-states rooted in fixed geography, network states begin as online collectives and gradually develop institutional structures.[884] Blockchain technology plays an important role in this vision, providing infrastructure for decentralized governance, digital identity, crowdfunding, asset tokenization (including land), cryptocurrencies, and programmable governance rules enforced through smart contracts. In practice, the community would form a decentralized autonomous organisation and crowdfund enough capital to be able to set up a physical presence. The ultimate goal is to achieve diplomatic recognition from existing governments.

Several experiments illustrate how these ideas are being tested in practice. Próspera,[885] officially *Próspera ZEDE*, is a special economic zone on Roatán Island, Honduras, created under the country's Zones for Employment and Economic Development (ZEDE) framework. It functions with a high degree of administrative, fiscal, and regulatory autonomy compared with the rest of Honduras, governed by its own council and legal codes while still subject to certain Honduran laws. Venture capital and private investors finance the project which positions itself as a low-tax, minimal regulatory environment to attract

879 Abhishek Singh, et al., *A perspective on decentralizing AI* (2024), https://www.media.mit.edu/publications/decai-perspective/.

880 Project NANDA, *Project NANDA FAQ*, GitHub, https://projectnanda.org/#/, (last visited Jan. 15, 2026).

881 Carolyn Haskins, *A Mysterious School for the Network State Crowd is now in Session*, Wired (Sept. 23, 2024), https://www.wired.com/story/network-school-balaji-srinivasan/; *see also* Sebastian Widmann, *Network States -Revolutionary Idea to Potential New Asset Class*, Forbes (Dec. 20, 2023), https://www.forbes.com/sites/digital-assets/2023/12/20/network-states--revolutionary-idea-to-potential-new-asset-class/.

882 Balaji Srinivasan, The Network State: How To Start a New Country (2022), https://thenetworkstate.com/. *See also* Balaji Srinivasan, *The Network School*, Balajis.com (Aug. 16, 2024), https://balajis.com/p/network-school (stating that "the Network School is for those who understand that Bitcoin succeeds the Federal Reserve, that encryption is the only true protection against unreasonable search and seizure, that AI can deliver better opinions than any Delaware magistrate, and that democracy can be rejuvenated with cryptography").

883 Balaji Srinivasan, *The Network State in One Sentence*, *in* The Network State: How To Start a New Country (2022), https://thenetworkstate.com/the-network-state-in-one-sentence.

884 *What Is a Network State?* Logos Press Engine, (May 27, 2025), https://press.logos.co/article/what-is-a-network-state.

885 Rachel Corbett, *The For-Profit City that Might Come Crashing Down*, New York Times (Aug. 28, 2024), https://www.nytimes.com/2024/08/28/magazine/prospera-honduras-crypto.html

startups and ventures in technology, biotechnology, crypto, and related fields.[886] Businesses in Próspera can adopt foreign legal standards or propose bespoke regulations within the ZEDE's governance system.[887] Domestic and international critics have disparaged Próspera as a quasi "state within a state" that undermines Honduran sovereignty and constitutional norms.[888] In response, the Honduran Congress and executive moved to repeal the ZEDE law in 2022–2023,[889] and in 2024 the Supreme Court declared the ZEDE framework unconstitutional.[890] However, the project asserts that its legal stability agreements and international treaty protections allow continued operation. Arbitration proceedings are ongoing.[891]

Other projects pursue similar ambitions through different pathways. Praxis Nation presents itself as "the world's first Digital Nation" whose "purpose is to restore Western Civilization."[892] It is a venture-backed community which seeks to build a new city, governed by its online collective[893] and to develop "acceleration zones." These zones "are a new type of Special Economic Zone that accelerate technological progress in service of national priorities…by attracting technologists and developing an institutional structure that guides technological development and the reinvestment of proceeds."[894] Nation3, by contrast, presented itself as "the world's first internet native jurisdiction."[895] This project seeks to build a "solarpunk society," with "a Web3-powered, tax-free, inclusive community."[896]

Another initiative, AnotherNation, aims to establish a global network of community-governed "embassies" in major cities, such as Dubai, London, and Miami.[897] Rather than building new cities from scratch, it leverages existing urban infrastructure to create physical hubs for Web3 communities. These spaces are designed to be owned and governed collectively through decentralized mechanisms. Users currently acquire membership and "citizenship" through staking Ether and holding the project's native token ($NATION), underscoring the experimental nature of these governance models.[898]

Taken together, these initiatives demonstrate how crypto-native governance is expanding beyond financial applications into territorial and institutional design. Projects range from temporary pop-up communities and digital nations to private cities and special economic

886 Divya Gummuluru, *Próspera, Honduras: A Controversial Experiment in Corporate Governance*, Intn'l Rel. Rev. (Oct. 23, 2025), https://www.irreview.org/articles/2025/10/23/prspera-honduras-a-controversial-experiment-in-corporate-governance.

887 *See generally* Próspera Global, *Próspera FAQs* (Sept. 3, 2024), https://www.prosperaglobal.com/news/prospera-faqs.

888 Corbett, *supra* note 885.

889 Gustavo Palencia, *Honduran Congress Unanimously Nixes Special Economic Zones*, Reuters (Apr. 21, 2022), *https://www.reuters.com/world/americas/honduran-congress-unanimously-nixes-special-economic-zones-2022-04-21/*.

890 Luis Escalante, *Honduran Government Praises Repeal of the ZEDE Law as Investors Denounce Lies and Abuse*, Contra Corriente (Sept. 28, 2024), https://contracorriente.red/en/2024/09/28/honduran-government-praises-repeal-of-the-zede-law-as-investors-denounce-lies-and-abuse/.

891 Honduras Próspera Inc. v. Republic of Honduras, ICSID Case No. ARB/22/43, Decision on Preliminary Objections Pursuant to CAFTA-DR Article 10.20.5 (Feb. 26, 2025), https://icsidfiles.worldbank.org/icsid/ICSIDBLOBS/OnlineAwards/C11037/DS20407_En.pdf; *see also $10.775 Billion Claim Filed Against Government of Honduras*, Próspera Connect (Dec. 20, 2022), https://blog.prospera.co/10-775-billion-claim-filed-against-government-of-honduras/.

892 *The Digital Nation: Crypto's End Game*, Praxis Nation , https://www.praxisnation.com/news/network-state-cryptos-end-game (last visited Jan. 15, 2026).

893 Zoë Bernard, *Welcome to Praxis: The high tech, high technology Eden that will save the world*, Vanity Fair, https://www.vanityfair.com/news/praxis-dryden-brown?srsltid=AfmBOop7ksgYhdl32jDx6W_2BBzLU3lI9aIewyAHAh8Juqjbjypzu1bz; *see also Praxis Announces $525M Financing for New City*, Praxis Nation (Oct. 24, 2024), https://www.praxisnation.com/news/financing-announcement-10-24.

894 *Announcing Acceleration Zones*, Praxis Nation (Oct. 18, 2023), https://www.praxisnation.com/news/announcing-acceleration-zones

895 Nation3, https://nation3.org (last visited Jan. 15, 2026).

896 *Id*.

897 Another Nation, https://www.anothernation.xyz/ (last visited Jan. 15, 2026).

898 *Nation3 Constitution*, Nation3 (last visited Jan. 15, 2026), https://github.com/nation3/law/blob/main/Constitution.linked.md.

zones. While they adopt diverse strategies —tokenized citizenship, modular jurisdictions, or territorial acquisition— they share a common ambition: to redesign governance for the digital age. This ecosystem reflects growing dissatisfaction with traditional political institutions and a desire to experiment with alternative forms of social organization.

However, despite their technological optimism, network state projects face significant challenges. Experiments such as Próspera have sparked local resistance, legal disputes, and accusations of neo-colonialism. Critics argue that privatized governance risks undermining democratic accountability,[899] exacerbating inequality, and enabling wealthy actors to "exit" public institutions while continuing to benefit from them. These tensions expose a central paradox of the movement: Attempts to escape politics often reproduce it. Far from eliminating power struggles, network states raise fundamental questions about legitimacy, accountability, and the social costs of privatized sovereignty.

899 Morshed Mannan, *Technocratic Despotism in the Network State*, *in* Decoding Digital Authoritarianism 73 (Global Affairs Canada 2023), https://cdn.sanity.io/files/9xbysn2u/production/4d7f42a888168a1d66292f26cdc50b5e3ff8d698.pdf

KEY TAKEAWAYS

■ Blockchain enables people to **send and receive money** directly, across borders, without relying on banks. It can be especially useful for lowering the cost of remittances for global transactions. Today, cross-border payments increasingly rely on stablecoins, which combine the global reach of blockchain infrastructure with price stability.

■ **Tokenization and Decentralized Finance (DeFi)** illustrate how blockchain has transformed fundraising, asset representation, and financial services. After the 2017–2018 wave of Initial Coin Offerings (ICOs), regulators tightened enforcement, prompting a shift toward more compliant fundraising models, such as Security Token Offerings (STOs) and Initial Exchange Offerings (IEOs). In parallel, projects moved away from pure fundraising tokens toward governance and utility tokens that grant voting rights or access to protocol functions. DeFi has built on these foundations by offering open, programmable financial services through smart contracts.

■ **Blockchain-based recordkeeping** offers tamper-evident, time-stamped, and auditable logs that can strengthen the integrity of public and private records, though large-scale adoption remains limited due to legal and technical obstacles. Governments have piloted applications ranging from digital titles for vehicles to notarial systems and academic credentials.

■ Blockchain enables new **data-sharing** models, through cryptographic access controls, immutable provenance records, and smart-contract-based automation, giving users greater control over how their information is used. Although adoption remains slow due to technical and organizational hurdles, promising applications have emerged in sectors such as healthcare, insurance, and intellectual-property management.

■ **Blockchain-based identity systems** aim to move away from centralized, platform-controlled models by giving individuals greater control over their identifiers and credentials. They enable users to store credentials in digital wallets, verify them through cryptographic proofs, and disclose only the minimum necessary information for each interaction. These systems also face significant challenges, including burdensome management of access keys, limited interoperability, and unresolved legal and regulatory issues. Case studies —such as Human Passport, World Network, and ION— illustrate both the promise and the risks of these models, particularly around biometrics, centralization points, and overall usability.

■ **Blockchain-based social media** seeks to counter the dominance of centralized platforms by giving users control over their identities, social graphs, and data. These systems record identity and relationship information on shared, interoperable infrastructures, while storing content off-chain, enabling portability across applications, and reducing platform lock-in. They promise greater transparency, censorship resistance, and user autonomy. But they also introduce challenges, including complex moderation, usability burdens, and risks arising from immutable on-chain data. Social Finance (SocialFi) models add financial incentives to social interactions, while other approaches —like Farcaster, Lens, and DSNP— focus primarily on portability and decentralized control.

■ **Blockchain-based dispute-resolution** (BDR) mechanisms offer alternatives to traditional litigation in environments where cross-border activity, pseudonymity, and automation make court proceedings impractical. They include both blockchain-based arbitration and decentralized justice systems, such as Kleros. These systems rely on smart contracts and crypto-economic incentives to guide pseudonymous jurors to reach a consensus. Although these mechanisms can enforce outcomes directly on-chain, they generally lack the procedural and institutional safeguards associated with conventional judicial or arbitral processes.

■ Blockchain can improve **supply-chain** coordination by enabling secure data sharing, immutable records, and verifiable audit trails, which enhance transparency, traceability, and regulatory compliance without requiring firms to surrender control over sensitive information. Yet adoption has been uneven: Several major pilots failed due to governance, financing, and industry-coordination challenges. But successful applications —such as automotive traceability, electronic bills of lading, and sustainability tracking— have shown that blockchain, paired with robust governance and viable business models, delivers value.

■ **Decentralized AI (DeAI)** distributes AI development across decentralized networks, using blockchain to enhance transparency, security, coordination, and access to compute and data. Blockchain enables decentralized marketplaces for compute, training, inference, and agentic AI collaboration. However, DeAI remains relatively new, and its meaningful decentralization is still limited by technical constraints, interoperability gaps, and the continued dominance of closed-source, centrally controlled AI models.

■ **Network states** are digitally native communities that organize online, mobilize resources through blockchain-based tools, and sometimes seek physical territory and political recognition as alternatives to traditional states. While experiments, such as Próspera, Praxis Nation, or Nation3, illustrate efforts to redesign governance through tokenized and decentralized models, these projects face legal uncertainty and political resistance.

CHAPTER 5

Risks and Challenges

CHAPTER 5 TABLE OF CONTENTS

CHAPTER 5. RISKS AND CHALLENGES **171**
5.1. Crypto Market Vulnerabilities 173
5.1.1. Volatility and Challenges in Fundamental Valuation 173
5.1.1.A. The Volatility of Crypto-assets 173
5.1.1.B. The Debate About the "Intrinsic" Value of Crypto-assets 175
5.1.2. The Case of Stablecoins 178
5.1.3. The Risks of Non-Fungible Tokens (NFTs) 182
5.1.3.A. Speculative Risks 182
5.1.3.B. Legal Issues 183
1. Intellectual Property Rights 183
2. Trademark Law 185
3. Securities Law 186
5.1.4. Manipulations of Crypto Markets 187
5.1.5. Notable Bankruptcies 189
5.1.5.A. Voyager and Three Arrows Capital 189
5.1.5.B. Celsius Network 190
5.1.5.C. The FTX Collapse 191
5.2. Criminal and Illicit Behaviors 193
5.2.1. The Debate About the Prevalence of Blockchain-Enabled Criminal Activity 193
5.2.2. Criminal Activities Facilitated by Blockchain Features 196
5.2.2.A. Crypto Payments 196
1. Crypto Financing of Illicit Activities 196
2. Money Laundering 198
3. Sanctions Evasion 199
4. Ransomware 200
5.2.2.B. Crypto Scams 201
1. Initial Coin Offering (ICO) Scams 201
2. Scam Tokens 202
3. Exit Scams 204
4. Rug Pulls 204
5.3. Cyber Security Challenges 205
5.3.1. Hacks on the Application Layer 207
5.3.1.A. Protocol Exploits 207
1. Code-Execution Vulnerabilities 208
2. Oracle-Manipulation Vulnerabilities 209
5.3.1.B. Flash Loan Attacks 210
5.3.1.C. Bridge Hacks 210
5.3.1.D. Software Backdoors or Undocumented Functions 211
5.3.2. Attacks on Centralized Intermediaries 212
5.3.3. Individual User Targeting 214
5.3.3.A. Private Key Loss 215
5.3.3.B. Wrench Attack 215
5.4. Environmental Impact 216
5.4.1. Electricity Consumption 216
5.4.1.A. Level of Electricity Usage 216
5.4.1.B. Policy Initiatives to Curb Electricity Consumption 217
5.4.1.C. Towards Renewable Energy Sources 219
5.4.2. Water Consumption 221
5.5. Privacy Challenges 222
5.5.1. User Identification Using Transaction Histories and On-Chain Communications 222
5.5.2. Analysis of Information Included in Off-Chain Communications 225
5.5.3. The Disclosure of Personal Information to Administrators and Service Providers 225
5.5.4. Limitations of Privacy Tools 228
KEY TAKEAWAYS 230

CHAPTER 5
Risks and Challenges

Blockchains are developed in an environment that allows for a high degree of experimentation in governance and economic coordination, enabling decentralized approaches that would be difficult to implement within more rigid institutional frameworks. This openness has facilitated rapid innovation and the emergence of alternative organizational models; but, it has also entailed significant costs, including frequent project failures, governance breakdowns, and instances of fraud.

While the benefits of blockchains are well-known — including global accessibility, transparency, and tamper-resistant data storage— the core properties of blockchain systems also give rise to a broad set of risks and operational challenges. Decentralization, pseudonymity, and permissionless access, which underpin much of blockchain's appeal, simultaneously create conditions that enable market manipulation, criminal exploitation, and large-scale fraud. Transparency, often presented as a safeguard, generates its own tensions: It can expose users to surveillance and de-anonymization. And the computational demands of certain consensus mechanisms carry environmental costs that have attracted growing regulatory attention.

This chapter examines five principal categories of risks related to blockchain systems. However, it does not seek to offer a systematic or exhaustive account of all risks associated with blockchain systems. Many of the vulnerabilities it examines —such as cybersecurity threats, fraud, and market manipulation— are not unique to blockchain. Rather, this chapter provides an overview of the five categories of risk that have attracted the most sustained attention in policy, academic, and regulatory debates.

5.1. CRYPTO MARKET VULNERABILITIES

While the most visible scaling of blockchain technologies has occurred through the growth of cryptocurrencies, the predominant uses of cryptocurrencies for trading, lending and borrowing still occur with limited direct connection to the real economy or the traditional financial system.[900] This has fueled criticism that many crypto-assets function primarily as speculative instruments.

5.1.1. Volatility and Challenges in Fundamental Valuation

This section explores the high volatility of crypto-asset prices and the ongoing debate over whether these assets possess identifiable fundamental value.

5.1.1.A. The Volatility of Crypto-assets

Crypto-assets have exhibited pronounced and persistent price volatility. Their prices can change very rapidly, sometimes increasing or decreasing by large amounts within short periods of time.[901] Weekly price swings of 10% or more are not uncommon, and Bitcoin's annualized

900 Lieven Hermans et al., *Decrypting Financial Stability Risks in Crypto-Asset Markets*, Eur. Cent. Bank Fin. Stability Rev. (May 2022), https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html.

901 *Why is Crypto Volatile? How Do You Make the Best of It*, Paxful (Jan. 9, 2025), https://paxful.com/university/crypto-volatility.

volatility has often been three to four times that of major equity indices such as the Standard & Poor 500.[902]

This volatility stems from a combination of factors, including shifts in market sentiment, developments in regulation or enforcement, macroeconomic news, and various idiosyncratic events. As a result, crypto prices often experience rapid expansions followed by abrupt corrections.[903] During periods of stress in traditional markets, crypto-assets can be as volatile as other risky assets; but, during episodes of turmoil in crypto markets specifically, they can become far more volatile.[904] Because many crypto traders use leverage, even small price drops can trigger forced liquidations, which push prices down further and create a self-reinforcing cycle of declines.[905] In addition, most crypto-assets tend to move together, and the platforms that support them are closely interconnected. As a result, problems in one asset or on one platform can quickly spill over to others, making the entire ecosystem highly vulnerable to sudden shocks.[906]

Sustained volatility affects how these assets can be used in practice. It complicates price discovery, undermines risk management, and makes it difficult for holders to rely on tokens for medium-term planning or transactional purposes.[907] Part of this volatility reflects crypto's status as a relatively young market with global participation, immediate price discovery, and continuous 24/7 trading, all of which can make fluctuations appear more extreme.[908] Bitcoin, in particular, has, in certain periods, been less volatile than many popular mega-cap stocks and some prominent individual stocks. Some estimates suggest that its realized volatility has declined over time.[909] Still, the asset class remains widely perceived as highly volatile, and this perception is unlikely to change until markets mature further.[910]

This high volatility can harm investors and users and pose a risk of causing financial panics. These risks increase when crypto-assets —which generally do not generate cash flows like stocks or bonds— are borrowed, "re-lent," or used as collateral in leveraged transactions across the ecosystem. In such cases, a drop in their price can quickly undermine the value of the collateral backing loans, triggering liquidations and amplifying market instability. Volatility magnifies the sensitivity of the ecosystem to price movements, which adds to the fragility of the system overall.[911]

Over the past two years, a number of market observers and analysts have provided nuanced assessments of crypto-asset volatility, particularly in relation to Bitcoin. An analysis published by the Chartered Financial Analyst (CFA) Institute in 2024 pointed to a sustained

902 Zack Wainwright, *A Closer Look at Bitcoin's Volatility,* Fidelity Digital Assets (May 1, 2024), https://www.fidelitydigitalassets.com/research-and-insights/closer-look-bitcoins-volatility.

903 Pablo D. Azar et al., *The Financial Stability Implications of Digital Assets*, 30 Econ. Pol'y Rev. (Fed. Rsrv. Bank of New York) 1, 2-3 (Nov. 2024), https://www.newyorkfed.org/medialibrary/media/research/epr/2024/EPR_2024_digital-assets_azar.pdf.

904 *Id.* at 11-12.

905 *Id.* at 3.

906 *Id.* at 3, 12-13.

907 *Id.* at 32.

908 Alena Narinyani, *Crypto Market Volatility Explained: What It Is, Why Crypto Is So Volatile, and How to Manage It,* ECOS(Jan. 27, 2026), https://ecos.am/en/blog/crypto-market-volatility-explained-what-it-is-why-crypto-is-so-volatile-and-how-to-manage-it; Nrusingha Tripathy, Sarbeswara Hota, Debabrata Singh, Biswa Mohan Acharya, Subrat Kumar Nayak, *A Comprehensive Analysis of Bitcoin Volatility Forecasting Using Time-Series Econometric Models*, 178 Applied Soft Computing 113339 (2025), https://doi.org/10.1016/j.asoc.2025.113339; Omid Malekan, *What Skeptics Get Wrong About Crypto's Volatility*, Harv. Bus. Rev. (July 6, 2022), https://hbr.org/2022/07/what-skeptics-get-wrong-about-cryptos-volatility.

909 Wainwright, *supra* note 902.

910 *Id.*

911 Azar et al., *supra* note 903.

decline in Bitcoin's realized volatility since 2021, albeit from historically elevated levels.[912] Commentators in the financial press, including *MarketWatch* and *Forbes*, have similarly suggested that, during certain periods, Bitcoin's volatility has been comparable to that of some high-volatility equities, including individual large-capitalization technology stocks such as Tesla or NVIDIA.[913] According to estimates cited by *Bloomberg* in 2025, the increasing participation of long-term, buy-and-hold institutional investors has contributed to a reduction in Bitcoin's annualized volatility over the past decade, from exceptionally high levels in its early years to figures in the range of those observed for some established publicly traded companies.[914] At the same time, liquidity conditions in major crypto-asset markets have improved, with bid-ask spreads[915] for leading tokens increasingly resembling those of highly liquid instruments in traditional financial markets.[916]

Notwithstanding these developments, market participants caution against over-interpreting signs of maturation. As Bullish CEO and former NYSE president Tom Farley recently remarked, significant price fluctuations remain an intrinsic feature of Bitcoin markets, noting that "the volatility is real" and is likely to remain a persistent source of uncertainty for investors.[917]

5.1.1.B. The Debate About the "Intrinsic" Value of Crypto-assets

One of the most contested issues in the field is the debate over whether crypto-assets possess "intrinsic" or "fundamental" value. The disagreement reflects deeper differences about how economic value is determined, what constitutes a legitimate asset, and how to interpret evolving financial technologies. While this policy report is not the right place to develop the conceptual underpinnings of the debate, this section outlines the main aspects and protagonists.

Many economists and traditional finance practitioners argue that cryptocurrencies lack the characteristics typically associated with long-term value.[918] Bitcoin has been a particular target of criticism. Jamie Dimon, CEO of JP Morgan Chase, has stated that "Bitcoin itself has no intrinsic value."[919] Warren Buffett described it as

912 See Wainwright, *supra* note 902; Andrew Keenan & Vibhu Gomatam, *Still Misperceived? A Fresh Look at Bitcoin Volatility*, CFA Inst. (June 12, 2024), https://blogs.cfainstitute.org/investor/2024/06/12/still-misperceived-a-fresh-look-at-bitcoin-volatility/.

913 Andrey Sergeenkov, *How Volatile Is Bitcoin Compared to Other Assets*, Forbes (Aug. 16, 2024), https://www.forbes.com/sites/digital-assets/2024/08/16/how-volatile-is-bitcoin-compared-to-other-assets/; Frances Yue, *Stocks Have Been More Volatile than Bitcoin Lately. That Doesn't Happen Very Often*, MarketWatch (Apr. 15, 2025), https://www.marketwatch.com/story/stocks-saw-more-volatility-than-bitcoin-did-amid-tariff-chaos-that-doesnt-happen-often-903c0afd. It is important to note that the realized volatility for regular stock was higher than for Bitcoin in large part because of the uncertainty associated with the United States imposing high tariffs against various nations.

914 *Bitcoin Volatility Collapse Forces Risk-Loving Traders Elsewhere*, Bloomberg (Aug. 22, 2025) https://www.bloomberg.com/news/articles/2025-08-22/bitcoin-volatility-collapse-forces-risk-loving-traders-elsewhere.

915 Adam Hayes, *How to Calculate the Bid-Ask Spread*, Investopedia (updated Jan. 26, 2025), https://www.investopedia.com/articles/investing/082213/how-calculate-bidask-spread.asp A bid-ask spread is the range between the highest price buyers are willing to pay for an asset and the lowest price sellers are willing to accept. The larger the spread, the less liquid the asset is, because supply and demand are harder to match.

916 *See, e.g.*, Alexander Brauneis et al., *How to Measure the Liquidity of Cryptocurrency Markets*, 124 J. Banking & Fin. 106041, 5 (Mar. 2021) https://www.sciencedirect.com/science/article/pii/S0378426620303022 (the Bitcoin and USD pair and the Ethereum and USD pair both have high liquidity); Alexander Brauneis et al., *Bitcoin Unchained: Determinants of Cryptocurrency Exchange Liquidity*, 69 J. Empirical Fin. 106, 107-08 (Dec. 2022) https://www.sciencedirect.com/science/article/pii/S0927539822000822 (Bitcoin has seen bid-ask spreads that are lower than those of many large-cap equities).

917 *Tom Farley Says Bitcoin Volatility Will Persist*, MSN (Dec. 17, 2025), https://www.msn.com/en-us/money/personalfinance/bitcoin-s-volatility-is-to-stay-for-a-long-time-former-nyse-president/ar-AA1RzyOz

918 Paul Krugman has contended that cryptocurrencies serve "no useful purpose" and that "their market value rested on nothing but "technobabble and libertarian derp," Paul Krugman, *How 2024 Became a Crypto Election*, N.Y. Times (Aug. 1, 2024), https://www.nytimes.com/2024/08/01/opinion/crypto-trump.html; Charlie Munger's criticisms have been even more categorical, calling cryptocurrencies "disgusting," "immoral," and a "disgrace," Jeannine Mancini, *Charlie Munger was Disgusted by Cryptocurrency, Deeming It Immoral and Worthless: 'It's Like Somebody Else is Trading Turds and You Decide, I Can't Be Left Out'*, Yahoo Fin. (Dec. 13, 2023), https://finance.yahoo.com/news/charlie-munger-disgusted-cryptocurrency-deeming-183817664.html.

919 Rocio Fabbro, *Jamie Dimon says Bitcoin has 'No Intrinsic Value,'* Yahoo Fin. (Jan. 13, 2025), https://finance.yahoo.com/news/jamie-dimon-says-bitcoin-no-144055964.html.

"rat poison squared."[920] From a more formal economic perspective, Nassim Nicholas Taleb contends that Bitcoin's expected value approaches zero because it yields no cash flows and is not tied to productive economic activity.[921] Nouriel Roubini maintains that cryptocurrencies fail to perform the core functions of money, emphasizing that they are not units of account, are not scalable means of payment, and are not stable stores of value.[922] Robert Shiller has suggested that the "ultimate source of value" of cryptocurrencies is "so ambiguous that it has a lot to do with our narratives rather than reality."[923] Institutional policymakers have expressed similar concerns. Christine Lagarde, President of the European Central Bank, has argued that "crypto assets are highly speculative, very risky … worth nothing … based on nothing, there [are] no underlying assets to act as an anchor of safety."[924]

These critics generally converge on the view that fungible crypto-assets behave more like speculative commodities or unbacked claims whose prices are driven by sentiment, liquidity conditions, and momentum rather than measurable fundamentals.[925] In conventional financial theory, an asset's "intrinsic value" is linked to cash-flow fundamentals (such as dividends, coupons, or residual claims) or, in the case of commodities, to consumption or industrial utility. Fiat currencies, although not redeemable for commodities, are backed by the legal authority of the state, their status as legal tender, and the ability of public institutions to stabilize their value. By contrast, most fungible crypto-assets do not offer claims on cash flows, ownership rights, or underlying pools of assets; nor are they legal tender.[926] Their value, therefore, depends on network participation, protocol utility, and coordinated expectations among users.[927]

Prominent figures within the crypto ecosystem defend the proposition that crypto-assets can possess real economic value, albeit of a different kind than traditional financial instruments. Vitalik Buterin, co-founder of Ethereum, emphasizes token utility, arguing that tokens derive value from their role in enabling access to decentralized computation, applications, and digital services.[928] Under this view, tokens function as access or coordination devices within a digital infrastructure. Other supporters advance a scarcity-based and macro-monetary thesis, most notably articulated by Michael Saylor, co-founder of MicroStrategy and a leading advocate for Bitcoin. Saylor describes Bitcoin as "digital gold," a digital substitute for

920 Tae Kim, *Warren Buffet says Bitcoin is 'Probably Rat Poison Squared'*, CNBC, (May 6, 2018), https://www.cnbc.com/2018/05/05/warren-buffett-says-bitcoin-is-probably-rat-poison-squared.html; Jessica Bursztynsky, Warren Buffett: Cryptocurrency 'Has No Value'- 'I Don't Own Any and Never Will,' CNBC (Feb. 24, 2020), https://www.cnbc.com/2020/02/24/warren-buffett-cryptocurrency-has-no-value.html.

921 Nassim Nicholas Taleb, *Bitcoin, Currencies, and Fragility*, arXiv:2106.14204, at 2 (2021), https://arxiv.org/abs/2106.14204.

922 Katie Greifeld, *ETF IQ: Nouriel Roubini (Still) Doesn't Like Cryptocurrencies,* BLOOMBERG (Nov. 29, 2024), https://www.bloomberg.com/news/newsletters/2024-11-29/etf-iq-nouriel-roubini-still-doesn-t-like-cryptocurrencies;"I'm skeptical for lots of reasons about cryptocurrencies and Bitcoin because they're not currencies. They're not units of account. They're not a scalable means of payment. They're not a stable store of value. And if you want wealth generation rather than high volatility, you have to stay away from those types of assets." *See also*, Nouriel Roubini, *Testimony for the Hearing of the US Senate Committee on Banking, Housing and Urban Affairs,* 115th Cong. (Oct. 11, 2018), https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf.

923 Stephanie Landsman, *Robert Shiller: 'Wild West' Mentality is Gripping Housing, Stocks and Crypto*, CNBC (May 24, 2021), https://www.cnbc.com/2021/05/23/robert-shiller-sees-wild-west-in-housing-stock-and-crypto-markets.html.

924 Johanna Treeck, *Crypto Assets Are 'Worth Nothing,' Says ECB's Christine Lagarde*, POLITICO (May 21, 2022), https://www.politico.eu/article/crypto-assets-worth-nothing-ecb-christine-lagarde/

925 *Crypto: The Basics*, FINANCIAL CONDUCT AUTHORITY, (May 10, 2024) https://www.fca.org.uk/investsmart/crypto-basics; BANK FOR INT'L SETTLEMENTS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 2 (July 2023), https://www.bis.org/publ/othp72.pdf; and, Eswar Prasad, *The Brutal Truth About Bitcoin*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/14/opinion/bitcoin-cryptocurrency-flaws.html.

926 *Id.* Prominent examples include DOGE, bitcoin's BTC, Ethereum's ETH, Solana's SOL, and Uniswap's UNI. *See* Miles Jennings et al., *Defining Tokens*, A16Z CRYPTO (Mar. 5, 2025), https://a16zcrypto.com/posts/article/defining-tokens/.

927 Jon Cunliffe, Deputy Governor for Financial Stability, Bank of England, Speech Given at SIBOS: Is 'Crypto' a Financial Stability Risk? (Oct. 13, 2021), https://www.bankofengland.co.uk/speech/2021/october/jon-cunliffe-swifts-sibos-2021; Maria Teresa Chimienti et al., *Understanding the Crypto-Asset Phenomenon, Its Risks and Measurement Issues*, ECB ECON. BULL., (May 2019), https://www.ecb.europa.eu/press/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html.

928 Vitalik Buterin, *On Bitcoin Maximalism, and Currency and Platform Network Effects*, ETHEREUM FOUNDATION BLOG (Nov. 20, 2014), https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects.

the historically valued hard asset. This position holds that Bitcoin's technical scarcity (fixed, finite token supply) and cryptographic security lend it value and that it can serve as a hedge against inflation of fiat currencies.[929] Some institutional investors have adopted this perspective; BlackRock CEO Larry Fink, formerly skeptical, later endorsed the thesis that Bitcoin can serve as a form of "digitalized" hard asset.[930]

Given these divergent perspectives, scholars and practitioners have attempted to develop various valuation theories for fungible tokens.[931] One approach holds that tokens confer rights of access to network services; if demand for those services grows, so does token value.[932] A second approach emphasizes that value increases with user adoption and activity within the ecosystem, a dynamic often associated with "Metcalfe's Law."[933] A third line of reasoning argues that all asset values are ultimately grounded in collective beliefs and expectations.[934] In this view, cryptocurrencies are not fundamentally different from other assets whose worth depends on market sentiment and coordinated expectations. A further perspective likens crypto-assets to commodities without cash flows, such as gold, which still have market value due to scarcity, liquidity, and demand for hedging. In these frameworks, prices are shaped by supply-and-demand forces and market sentiment.[935] Finally, value may derive from the costliness of producing secure, globally verifiable transactions and from the ability of decentralized systems to facilitate economic coordination without centralized trust. Under this view, fungible tokens may warrant a non-zero valuation even in the absence of traditional cash flows.

A balanced view may be that the value proposition for most fungible cryptocurrencies is more speculative and less anchored than that of traditional financial assets.[936] Cryptocurrency investors, particularly retail investors, may be risk seekers insufficiently skeptical of new investment opportunities or caught up in the fear of missing out (FOMO).[937] This may cause them to bid up token prices far beyond their "fundamental" value. A 2023 study by the Bank for International Settlements found that, on net, retail investors in most countries lost money on Bitcoin purchases.[938] At the same time, long-horizon data show that Bitcoin has persisted through multiple market cycles, maintained uninterrupted network uptime, and

929 Andrew Rocco, *Unpacking Michael Saylor's Bitcoin Gold Rush,* Yahoo Finance (Nov. 11, 2024), https://finance.yahoo.com/news/unpacking-michael-saylors-bitcoin-gold-204500318.html.

930 Helene Braun, *BlackRock's Larry Fink: Bitcoin Is 'Legitimate Financial Instrument'*, Coindesk (July 15, 2024), https://www.coindesk.com/business/2024/07/15/blackrocks-larry-fink-bitcoin-is-legitimate-financial-instrument

931 Fernando García-Monleón et al., *Intrinsic Value in Crypto Currencies*, 162 Tech. Forecasting & Soc. Change 120393 (2021), https://www.sciencedirect.com/science/article/abs/pii/S0040162520312191.

932 Lin William Cong, Ye Li, & Neng Wang, *Tokenomics: Dynamic Adoption and Valuation,* NBER Working Paper No. w27222, (May 2020), https://ssrn.com/abstract=3609674.

933 Timothy F. Peterson, *Metcalfe's Law as a Model for Bitcoin's Value*, 7 ALTERNATIVE INV. ANALYST REV., no. 2, Q2 2018, at 9, https://caia.org/sites/default/files/metcalfeslaw_websiteupload_7-5-18.pdf; *see also* Timothy F. Peterson, *Metcalfe's Law as a Model for Bitcoin's Value* (Jan. 22, 2018), https://ssrn.com/abstract=3078248 or http://dx.doi.org/10.2139/ssrn.3078248.

934 David Henderson, *Crypto, Investment, and Intrinsic Value*, Econlib (Dec. 11, 2024), https://www.econlib.org/crypto-investment-and-intrinsic-value/.

935 *What Defines the Price of Cryptocurrency?*, OSL (Feb. 4, 2025), https://osl.com/academy/article/what-defines-the-price-of-cryptocurrency; Andrew Bloomenthal, *What Determines Bitcoin's Price?*, Investopedia (Oct. 11, 2024), https://www.investopedia.com/tech/what-determines-value-1-bitcoin/; Carla Tardi, *Animal Spirits: Meaning, Definition in Finance, and Examples*, Investopedia(Feb. 21, 2023), https://www.investopedia.com/terms/a/animal-spirits.asp; Adam Morgan McCarthy, *'Animal Spirits' in Bitcoin Prompt Warnings of Wild Price Swings as It Nears New Record*, DLNews (Mar. 4, 2024), https://www.dlnews.com/articles/snapshot/bitcoin-markets-flash-volatility-warning-amid-animal-spirits/.

936 Jon Cunliffe, *Is 'Crypto' a Financial Stability Risk?* Bank of England, Speech at SIBOS (Oct. 13, 2021), https://www.bankofengland.co.uk/speech/2021/october/jon-cunliffe-swifts-sibos-2021.

937 *Digital Asset and "Crypto" Investment Scams - Investor Alert*, SEC, (Sept. 1, 2021), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/digital-asset-and-crypto-investment-scams-investor-alert.

938 Bank for Int'l Settlements, *The Crypto Ecosystem: Key Elements and Risks* 12 (July 2023), https://www.bis.org/publ/othp72.pdf; Giulio Cornelli et al., *Crypto Shocks and Retail Losses*, BIS Bull. No. 69 (Feb. 20, 2023), https://www.bis.org/publ/bisbull69.pdf.

outperformed many major asset classes over multi-year periods.[939] The coexistence of these observations underscores the complexity of the valuation problem: Long-term resilience and adoption coexist with substantial retail losses, extreme volatility, and widespread failures among non-Bitcoin tokens.

5.1.2. The Case of Stablecoins

Stablecoins *(See section 2.4.1.C)* have become a major focus of regulatory attention. They entered the center of global policy debates in 2019 when Facebook (now Meta) announced *Libra*, a global stablecoin.[940] Libra's launch prompted immediate scrutiny from U.S. and international regulators, triggering congressional hearings[941] and cross-agency coordination through the Financial Stability Oversight Council (FSOC) Working Group on Digital Assets.[942] Libra was later renamed Diem and discontinued in 2022.

From an economic and functional perspective, stablecoins fall into two broad categories: asset-backed and algorithmic.

- **Asset-backed stablecoins** —such as Tether's USDT *(See Figure 35)* and Circle's USDC *(See Figure 14)*— are issued by centralized intermediaries that hold collateral, which may include bank deposits, short-term Treasury bills, commercial paper (historically), or other liquid assets. These intermediaries manage issuance and redemption and are operationally similar to money market funds or e-money issuers.

939 *Bitcoin Returns vs. Major Asset Classes*, Visual Capitalist (Feb. 6, 2024), https://www.visualcapitalist.com/bitcoin-returns-vs-major-asset-classes/; *Has the Bitcoin Network Ever Gone Down?*, Bitbo https://bitbo.io/calendar/downtime/ (last visited Jan. 15, 2026).

940 Jörg Mayer, Crypto Assets and Central bank Digital Currencies: Potential Implications for Developing Countries, U.N. Conf. on Trade & Dev., UNCTAD/GDS/2023/1, at 1 (2023), https://unctad.org/system/files/official-document/gds2023d1_en.pdf.

941 An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors; Hearing Before the H. Comm. on Fin. Servs., 116th Cong. (2019), https://www.congress.gov/116/chrg/CHRG-116hhrg42452/CHRG-116hhrg42452.htm

942 Steven T. Mnuchin, Sec'y of the Treasury, *Press Briefing on Virtual Currencies and Facebook's Libra* (July 15, 2019), https://home.treasury.gov/news/press-releases/sm731.

FIGURE 35.

The Tether (USDT) controversy

Tether Ltd issues USDT, a U.S. dollar-pegged stablecoin marketed as redeemable one-to-one against U.S. dollar-denominated reserves.[943] Tether dominates the global stablecoin sector, representing more than 60% of the total stablecoin market cap,[944] with $143 billion worth of USDT tokens.[945] The company has long been the subject of intense scrutiny and sustained controversy due to longstanding concerns about the adequacy and transparency of its reserves.[946]

Tether claims that every USDT is backed "1:1 by U.S. dollars." However, in 2019, the Tether's General Counsel stated in court filings that Tether's cash and cash equivalents were, at one point, approximately only 74% of outstanding tethers.[947] In the same filings, the General Counsel (GC) clarified that Tether also held additional reserves in less liquid forms and argued that maintaining cash reserves equal to 100% of outstanding tokens was neither novel nor necessary.[948] Drawing an analogy to commercial banking, the GC noted that banks operate under a fractional reserve system, holding only a small fraction of customer deposits in cash, and emphasized that Tether's cash reserves exceeded typical regulatory minimums for banks.[949] The GC further asserted that Tether had never lacked the funds necessary to process customer redemptions.[950]

In 2021, the New York Attorney General's Office concluded an investigation into Tether and its affiliated exchange, Bitfinex, regarding allegations of improperly misappropriating millions of dollars to cover up an apparent loss of $850 million of commingled client and corporate funds.[951] The matter was settled for $18.5 million, with Tether admitting no wrongdoing.

Continued

943 *Tether Transparency Page (USDT)*, TETHER, https://tether.to/en/transparency/?tab=usdt (last visited Jan. 15, 2026).

944 Stablecoins Circulating, DefiLlama, https://defillama.com/stablecoins (last visited Jan. 15, 2026).

945 *See* Kyle Baird, *Tether Inches Closer to Long-Promised USDT Audit After Trump Clears Regulatory Roadblocks*, DLNEWS (Mar. 22, 2025), https://www.dlnews.com/articles/regulation/tether-nears-full-usdt-audit-after-trump-clears-roadblocks/.

946 In re *Tether Holdings Ltd., CFTC No. 22-04* (Oct. 15, 2021) https://www.cftc.gov/media/6646/enftetherholdingsorder101521/download

947 Stuart Hoegner, Affirmation of Gen. Counsel, Tether Ltd., *In re Letitia James v. iFinex Inc. et al.*, *No. 450545/2019* (N.Y. Sup. Ct. Apr. 30, 2019), https://media.kalzumeus.com/tether-docs/bitfinex-response-to-nyag.pdf

948 "Beyond Tether's cash on hand, additional reserves are available, though in less liquid form. That Tether does not now keep liquid, cash reserves equal to 100 percent of the outstanding tethers is not only disclosed to customers, but hardly a novel concept. Commercial banks operate under a "fractional reserve" system whereby they keep cash hand representing only a small fraction of customer deposits, deploying the rest via investments. According to the Federal Reserve website, the banks must keep cash reserves representing, at most, only 10 percent of their liabilities. (Ex. G, at 1.) Tether's cash is far more than that, and the company has never lacked the funds to process a redemption." Affidavit of Stuart Hoegner para 33–35, People v. iFinex Inc., No. 450545/2019 (N.Y. Sup. Ct. Apr. 30, 2019), https://amycastor.com/wp-content/uploads/2019/01/408190972-stuart-hoegner-affidavit-4-30.pdf.

949 *Understanding Tether's Peg and Reserves*, TETHER (May 21, 2022), https://tether.io/news/understanding-tethers-peg-and-reserves/. Scott Nevil, *Understanding Fractional Reserve Banking: How It Fuels Economic Growth*, INVESTOPEDIA (Sep. 9, 2025), https://www.investopedia.com/terms/f/fractionalreservebanking.asp. Olena Kocherhina, *Tether Earned Over $10B in 2025 and Increased Its Reserves to Record Levels*, INCRYPTED (Jan. 2, 2026), https://incrypted.com/en/tether-earned-over-10b-in-2025-and-increased-its-reserves-to-record-levels/.

950 *Id.* Tether.

951 Press Release, N.Y. State Att'y Gen. Letitia James, *Attorney General James Announces Court Order Against "Crypto" Currency Company Under Investigation for Fraud* (Apr. 24, 2019) https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company; Nikhilesh De, *NY AG's $850M Probe of Bitfinex, Tether Ends in an $18.5M Settlement,* COINDESK (Sept. 14, 2021), *https://www.coindesk.com/markets/2021/02/23/ny-ags-850m-probe-of-bitfinex-tether-ends-in-an-185m-settlement*.

FIGURE 35. (continued)

The Tether (USDT) controversy (continued)

Beyond reserve transparency, Tether has faced allegations that its issuance patterns have influenced cryptocurrency markets. Academic studies —most notably a 2018 study by Griffin and Shams (University of Texas at Austin)[952] —have argued that large issuances of USDT were correlated with major increases in Bitcoin's price and may have been used to support markets during downturns.[953] The U.S. Commodity Futures Trading Commission (CFTC) fined Tether $41 million for making misleading claims regarding the composition of its reserves.[954]

Although Tether now publishes third-party attestations of its reserves,[955] the controversy persists.[956] The precise composition of the assets backing USDT remains partially opaque. The absence of a full, independent audit remains a central point of criticism.[957]

- **Algorithmic stablecoins** take a fundamentally different approach. Instead of relying on real-world collateral, they use smart-contract-based monetary rules and arbitrage mechanisms to adjust supply to maintain a peg, typically to the U.S. dollar. This means algorithmic stablecoins are not backed by valuable collateral in the real world and depend on the algorithm, and arbitrageurs, to maintain their stable value.[958] This structure makes them far more fragile. TerraUSD (UST), which relied on a dual-token "seigniorage" model involving LUNA, collapsed spectacularly in May 2022, falling from $1 to near-zero within days *(See Figure 27)*. The Terra collapse, erasing tens of billions of dollars in market value and triggering cascading failures across the crypto ecosystem, became a paradigmatic example of the vulnerabilities inherent in uncollateralized algorithmic designs.

U.S. federal banking regulators initially adopted a highly cautious stance toward stablecoins and crypto-related activities. A report on stablecoins from the President's Working Group on Financial Markets, issued in November 2021 under then President Joe Biden,[959] highlighted various financial risks from stablecoins, such as runs "on the bank" and payment system disruptions. The U.S. Federal Reserve also voiced concerns about stablecoins

952 John M. Griffin and Amin Shams, *Is Bitcoin Really Un-Tethered?* 75 J. Fin. 1913 (2020), https://ssrn.com/abstract=3195066.

953 Nikhilesh De, *Tether Manipulation Pushed Up Bitcoin's Price, Researchers Find*, CoinDesk (Sept. 13, 2021), https://www.coindesk.com/markets/2018/06/13/tether-manipulation-pushed-up-bitcoins-price-researchers-find; see *also* Arianne Bonacua, *Tether's Impact on the Cryptocurrency Market*, Markets.Com (Jan. 30, 2024) https://www.markets.com/de/education-centre/tether-on-cryptocurrency-market/,

954 Press Release, Commodity Futures Trading Comm'n, *CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million* (Oct. 15, 2021), https://www.cftc.gov/PressRoom/PressReleases/8450-21.

955 *Transparency Reports,* Tether, https://tether.to/ru/transparency/?tab=reports (last visited Jan. 15, 2026); Tether, *Tether Acknowledged by U.S. Authorities for Freezing $1.6M Connected to Terrorism Financing, Tether (July 23, 2025),* https://tether.io/news/tether-acknowledged-by-u-s-authorities-for-freezing-1-6m-connected-to-terrorism-financing/

956 José Oramas, *Consumer Watchdog Flags Tether for Lack of Transparency in US Dollar Reserves Audit*, Crypto News Australia (Sept. 13, 2024), https://cryptonews.com.au/news/consumer-watchdog-flags-tether-for-lack-of-transparency-in-us-dollar-reserves-audit-123350/.

957 Hannah Lang & Elizabeth Howcroft, *Tether Is In Talks With 'Big Four' Firm About Reserve Audit, Ceo Says*, Reuters (Mar. 21, 2025), https://www.reuters.com/technology/tether-is-talks-with-big-four-firm-about-reserve-audit-ceo-says-2025-03-21/

958 Bank for Int'l Settlements, *The Future Monetary System*, BIS annual economic Report 2022 (June 2022), https://www.bis.org/publ/arpdf/ar2022e3.htm.

959 President's Working Group on Financial Markets, Federal Deposit Insurance Corporation & Office of the Comptroller of the Currency, *Report on Stablecoins* (Nov. 1, 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

and their interaction with the broader financial system,[960] emphasizing that the absence of robust regulatory frameworks heightened systemic vulnerabilities.[961] In a January 2023 Joint Statement,[962] the Office of the Comptroller of the Currency (OCC), the Federal Reserve, and the FDIC emphasized a range of risks: fraud, legal uncertainties surrounding custody, misleading disclosures, market volatility, and the susceptibility of stablecoins to runs and broader financial contagion within the crypto sector. The regulators warned that issuing or holding crypto-assets on open, public, or decentralized networks was "highly likely to be inconsistent with safe and sound banking practices." They also expressed significant concerns about business models heavily concentrated in crypto-related activities.[963] In a policy statement from January 27, 2023,[964] the Federal Reserve identified certain crypto-asset activities as presenting heightened supervisory concern and presumptively impermissible. These activities included banks' direct ownership of crypto-assets for their own account (i.e., holding as principal) and the issuance of crypto tokens other than so-called "dollar tokens."

Against this backdrop, Congress has moved toward formal regulation. In July 2025, President Trump signed into law the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) *(See section 7.2.4.D.1.)*.[965] The legislation focuses specifically on "payment stablecoins," defined as digital assets designed for use as a means of payment or settlement. The Act establishes a comprehensive federal framework for the issuance and oversight of payment stablecoins and seeks to address regulatory concerns through prudential supervision. Notably, the law directs federal and state regulators —including the Federal Reserve Board, the OCC, the National Credit Union Administration (NCUA), and state supervisory agencies— to issue implementing rules to govern capital, liquidity, and risk-management standards for permitted issuers. It also imposes strict reserve requirements to ensure full and timely redemption of outstanding payment stablecoins, effectively bringing stablecoin issuance within the traditional regulatory perimeter.

In December 2025, the Federal Reserve rescinded its 2023 policy statement and replaced it with a new policy statement that signals a more innovation-friendly approach, citing an "evolving understanding of the crypto-asset sector".[966] This happened in parallel with the Federal Reserve's, FDIC's, and OCC's repeal of other 2022–2023 guidance that had taken a skeptical view of crypto-related activities. The 2025 policy statement removes from the record the 2023 statement's activity-specific prohibitions and provides that the Federal Reserve may authorize

960 Pablo Azar et al., *The Financial Stability Implications of Digital Assets,* Fed. Res. Bank of N.Y., Staff Rep. No. 1034 (Sept. 2022), https://www.newyorkfed.org/research/staff_reports/sr1034

961 Pablo D. Azar et al., *The Financial Stability Implications of Digital Assets*, 30 Econ. Pol'y Rev. 1 (Fed. Res. Bank of N.Y. Nov. 2024), https://www.newyorkfed.org/medialibrary/media/research/epr/2024/EPR_2024_digital-assets_azar.pdf.

962 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation & Office of the Comptroller of the Currency, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (Jan. 3, 2023), https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

963 *Id.*

964 Federal Reserve policy statement PDF Board of Governors of the Federal Reserve System, *Policy Statement on Section 9(13) of the Federal Reserve Act,* (Jan. 27, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230127a2.pdf.; Davis Polk client update Davis Polk & Wardwell LLP, *Crypto's Integration into the Traditional Financial System Is Under More Pressure* (Jan. 5, 2026), https://www.davispolk.com/insights/client-update/cryptos-integration-traditional-financial-system-under-more-pressure

965 *See generally* Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025 (GENIUS Act), Pub. L. No. 119-27, 139 Stat. 419 (2025).

966 Jessie Jiaxu Wang, *Banks in the Age of Stablecoins: Implications for Deposits, Credit, and Financial Intermediation,* Fed. Res. Bd., FEDS Notes, (Dec. 17, 2025), https://www.federalreserve.gov/econres/notes/feds-notes/banks-in-the-age-of-stablecoins-implications-for-deposits-credit-and-financial-intermediation-20251217.html; Chuan Du, Ria Sonawane, and Cy Watsky, *In the Shadow of Bank Runs: Lessons from the Silicon Valley Bank Failure and Its Impact on Stablecoins,* Fed. Res. Bd., FEDS Notes, (Dec. 17, 2025), https://www.federalreserve.gov/econres/notes/feds-notes/in-the-shadow-of-bank-run-lessons-from-the-silicon-valley-bank-failure-and-its-impact-on-stablecoins-20251217.html; Davis Polk & Wardwell LLP, *Federal Reserve and FDIC Take Crypto-Friendly Steps* (Dec. 22, 2025), https://www.davispolk.com/insights/client-update/federal-reserve-and-fdic-take-crypto-friendly-steps

uninsured state banks that are Federal Reserve member banks —or applicants for membership— to engage in certain activities that may not be permissible for national banks or insured state banks.

5.1.3. The Risks of Non-Fungible Tokens (NFTs)

Non-fungible tokens (NFTs) present a range of risks and legal uncertainties (for a presentation of NFTs, *See section 2.4.2*). Some resemble those associated with fungible cryptocurrencies —such as volatility, fraud, and market manipulation— while others arise from the tokenization of digital or physical assets, particularly concerning intellectual property and consumer expectations.

5.1.3.A. Speculative Risks

Fundraising through NFTs surged dramatically in 2021. The rapid expansion of NFT marketplaces enabled the buying and selling of diverse assets, including digital art, collectibles, and event tickets. A turning point came when Christie's auctioned a digital artwork entitled *Everydays: The First 5000 Days,* by an artist known as Beeple, for an unprecedented $69 million.[967] The event triggered a wave of speculative activity, with collections such as CryptoPunks,[968] Bored Ape Yacht Club,[969] and basketball highlight reels,[970] reaching multi-million-dollar valuations. Celebrities eagerly acquired profile picture NFTs;[971] major brands introduced digital collectibles;[972] and trading volumes on platforms such as OpenSea soared to billions of dollars per month.[973] Even traditional auction houses and art galleries embraced the trend.[974]

Yet the market's explosive growth proved unsustainable.[975] By mid-2022, NFT trading volumes had fallen by over 90% from their peak, and floor prices declined sharply for even the most prominent collections.[976] NFTs that once sold for tens of thousands of dollars became difficult to resell for a few hundred. While some early sellers realized significant gains, many later entrants incurred substantial losses.[977] Even celebrity-backed NFT projects saw price declines of 90% or more.[978] The contraction was particularly pronounced in the art-related NFT market: Sales of art-related NFTs rose from about $20 million in 2020[979] to a peak of $2.9 billion in 2021[980] before dropping back to $1.2 billion in 2023.[981] Many NFT projects proved to be poorly conceived or outright fraudulent, leaving investors with worthless digital assets.[982]

967 Beeple, *Everydays: The First 5000 Days*, Christie's https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924 (Mar. 11, 2021).

968 Cryptopunks, https://cryptopunks.app/ (last visited Jan. 15, 2026).

969 Bored Ape Yacht Club, OpenSea, https://opensea.io/collection/boredapeyachtclub (last visited Jan. 15, 2026).

970 Adam Wells, *Warriors' Stephen Curry Releases NFT to Commemorate Breaking NBA's 3-Point Record*, Bleacher Report, Dec. 17, 2021. https://bleacherreport.com/articles/10021212-warriors-stephen-curry-releases-nft-to-commemorate-breaking-nbas-3-point-record

971 Caroline Goldstein, "*Which Celebrities Have NFTs as Profile Pics?*" Artnet (Jan. 26, 2022),https://news.artnet.com/market/nft-celebrity-profile-pics-2064502

972 Maghan McDowell and Madeleine Schulz, The *Vogue Business NFT Tracker*, Vogue (Dec. 17, 2024).https://www.voguebusiness.com/technology/the-vogue-business-nft-tracker

973 Casey Wagner, *OpenSea Hits $3B in Monthly NFT Volume*, Blockworks (Aug. 23, 2021), https://blockworks.co/news/opensea-hits-3b-in-monthly-nft-volume.

974 Elizabeth Howcroft, *Insight: The New Masters: How auction houses are chasing crypto millions*, Reuters, (Nov. 9, 2021), https://www.reuters.com/business/finance/new-masters-how-auction-houses-are-chasing-crypto-millions-2021-11-08/

975 Brian McGleenon, *What Happened to NFTs?*, Yahoo Finance (July 15, 2024), https://uk.finance.yahoo.com/news/what-happened-to-nfts-094039263.html.

976 *NFT Trading Volumes Collapse 97% from January Peak*, Bloomberg, (Sept. 28, 2022) https://www.bloomberg.com/news/articles/2022-09-28/nft-volumes-tumble-97-from-2022-highs-as-frenzy-fades-chart; Yuqian Lim, *The NFT Crash: Blue Chip NFT Floor Price Down 83%*, Coingecko (updated Sept. 26, 2023)

977 Stacey Vanek Smith, *Is it RIP for the NFT?*, Marketplace (Dec. 22, 2023), https://www.marketplace.org/story/2023/12/22/nft-market-crashes-value-worthless.

978 Immanual John Milton, *The Disastrous Record of Celebrity Crypto Endorsements*, Bloomberg (Aug. 1, 2022), https://www.bloomberg.com/features/2022-crypto-celebrity-endorsements/.

979 *Id.*

980 Clare McAndrew, *The Art Basel & UBS Survey of Global Collecting 2024*, (Arts Econ. 2024), https://theartmarket.artbasel.com/download/The-Art-Basel-and-UBS-Survey-of-Global-Collecting-in-2024.pdf.

981 What Next for NFTs as the Crypto Markets Rallies?, Art Basel (July 11, 2024), https://www.artbasel.com/stories/nft-crypto-art-market-transformation?lang=en.

982 Deborah Seifert and Christophe Van Linden, *Fraud Risks in the Market for Nonfungible Tokens*, The CPA Journal, July/Aug. 2024 (updated Jan. 2025). https://www.cpajournal.com/2025/01/08/fraud-risks-in-the-market-for-nonfungible-tokens/

Beyond their volatility, NFTs suffer from poor liquidity; owners may struggle to sell them unless they accept steep discounts.[983] Collections that were once highly valued became nearly unsellable, as liquidity in secondary markets diminished. Unlike equities or bonds, NFTs do not trade on deep markets with continuous buyers. Price discovery is highly subjective and complicated by the absence of intrinsic value, cash flows, or standardized valuation metrics.

The NFT ecosystem has also been plagued by fraudulent practices, including wash trading, misleading promotions, counterfeit collections, and "rug pulls," where creators abandon projects after initial sales *(See section 5.2.2.B.)*. A report issued by the U.S. Department of Treasury in May 2024 found that, while NFTs are rarely being used "for proliferation financing or terrorist financing," they are still "highly susceptible to use in fraud and scams."[984] The report recommended several mitigation measures, chief among them to engage and educate consumers and local law enforcement, to continue enforcing existing laws, and to encourage private actors to develop solutions for identifying scams.[985]

Taken together, the risk profile of speculative NFTs resembles that of highly speculative collectibles or early-stage venture investments —often without the regulatory protections or market infrastructure associated with traditional financial instruments. At the same time, the market has progressively shifted toward more "utility-driven" applications, such as gaming assets, loyalty and rewards programs, and ticketing.[986] This broader digital-collectibles market reached approximately $8.8 billion in 2024,[987] with 2025 trading activity projected to remain in the mid-single-digit billions of U.S. dollars.[988] This evolution suggests a gradual transition away from predominantly speculative art NFTs toward more functional applications.

5.1.3.B. Legal Issues

NFTs also raise complex legal questions. The ownership of a token does not necessarily correspond to ownership of the underlying asset or related intellectual property rights. Most NFTs merely reference or point to an asset stored off-chain. Unless expressly provided by contract, the transfer of an NFT does not convey copyright, reproduction rights, or other proprietary interests.

1. Intellectual Property Rights

Intellectual property disputes are among the most common legal challenges. For example, the sale of a work of art represented by an NFT may transfer the ownership of the token, but it does not necessarily transfer the copyright vested in the artwork.[989] Blockchain records cannot prevent off-chain infringements, such as unauthorized reproductions or misuse. Many buyers do not appreciate that they are acquiring only a pointer to an asset or metadata, not the underlying rights.

983 Eric Ravenscraft, *NFTs Don't Work the Way You Might Think They Do,* WIRED (June 12, 2022), https://www.wired.com/story/nfts-dont-work-the-way-you-think-they-do/.

984 U.S. DEP'T OF THE TREASURY, *Illicit Finance Risk Assessment of Non-Fungible Tokens* 1 (May 2024), https://home.treasury.gov/system/files/136/Illicit-Finance-Risk-Assessment-of-Non-Fungible-Tokens.pdf.

985 *Id.* at 21.

986 Harris Bickle, *How Multi-Utility NFTs Are Redefining the Digital Asset Landscape,* BUILTIN (June 13, 2025), https://builtin.com/articles/multi-utility-nfts

987 Mohammad Shahid, *NFT Sales Hit $8.8 Billion in 2024, Despite Mixed Market Trends*, BE(IN)CRYPTO, https://beincrypto.com/nft-sales-2024-growth-challenges/ (Jan. 2, 2025); Ezra Reguerra, *NFTs Record $8.8B Sales Volume in 2024 - CryptoSlam*, COINTELEGRAPH (Dec. 31, 2024), https://cointelegraph.com/news/nft-total-sales-volume-2024-data-december.

988 ART BASEL & UBS, The Art Basel & UBS Global Art Market Report 2024 (Arts Eco. 2024), as summarized in *What Next for NFTs as the Crypto Market Rallies?* (July 11, 2024), https://www.artbasel.com/stories/nft-crypto-art-market-transformation; Ezra Reguerra, *NFTs Record $8.8B Sales Volume in 2024 — CryptoSlam*, COINTELEGRAPH (Dec. 30, 2024), https://cointelegraph.com/news/nft-total-sales-volume-2024-data-december; Binance Square, *NFT Sales Hit $8.8 Billion in 2024*, BEINCRYPTO (Jan. 1, 2025), https://www.binance.com/en/square/post/18378858860098; OKX RESEARCH, *NFT Trading Volume 2025: Trends & Insights and Market Shifts* (2025), https://www.okx.com/en-us/learn/nft-trading-volume-2025-trends-insights.

989 *See generally* Timothy Chan, *The Nature of Property in Crypto-assets*, 43 LEGAL STUDIES 480, (2023) https://www.cambridge.org/core/journals/legal-studies/article/nature-of-property-in-cryptoassets/6B882C05BD3D9A7A924FBE41C359E92E (noting that whether the sale of a crypto asset also transfers the legal rights associated with the asset sold is an open question that rests on the theory underpinning what property is exchanged in a crypto asset sale).

FIGURE 36.

SpiceDAO

In 2021, an anonymous crypto collective known as SpiceDAO paid approximately $3 million for a rare physical copy of Alejandro Jodorowsky's illustrated production book (often referred to as the *"Dune Bible"*) created for his unproduced adaptation of *Dune*.[990] After the purchase, the collective announced that it would create NFTs for each individual page of the book and offer the NFTs for sale.[991]

However, the acquisition of the physical book did not include any copyright or reproduction rights in either Frank Herbert's *Dune* novel or the artwork contained in the production book. As a result, minting and selling NFTs that reproduced the pages would have infringed multiple copyrights held by Herbert's estate and by the various artists involved in the production book, including Jodorowsky and his collaborators.[992] Specifically, Spice DAO would have needed permission from Herbert's estate (for the Dune novel) and from Jodorowsky and his co-authors (for the production book artwork).[993]

Once these legal constraints became apparent, the NFT project was effectively abandoned.[994] This episode underscores that NFTs can represent ownership within a blockchain ecosystem but cannot override traditional legal frameworks.

In March 2024, the U.S. Patent and Trademark Office and the U.S. Copyright Office issued a joint report about the potential uses of NFTs for intellectual property and how intellectual property rules apply to NFTs.[995] That report noted new and creative uses for NFTs to be used in branding, marketing, and developing new and interesting art and inventions that could fall under intellectual property protections. It also found opportunities for artists and inventors to establish clearer ownership over their works and to collect royalties with greater ease.[996] At the same time, the report noted concerns over piracy, infringement, and counterfeiting.[997] On the question of whether NFTs require amendments to existing intellectual property rules or entirely new laws, the report stated that they do not and that NFTs, while novel, do not raise entirely new legal issues.[998]

990 Adi Robertson, *They Spent $3 Million on a Dune Script Bible - Now What?*, The Verge (Feb. 28, 2022), https://www.theverge.com/2022/2/28/22950868/spice-dao-crypto-jodorowsky-dune-bible-collective-writing-contest; Adrienne Westenfeld, "The Saga of the *Dune* Crypto Bros And Their Very Pricey Mistake Is At Its End," Esquire (July 28, 2022), https://www.esquire.com/entertainment/books/a38815538/dune-crypto-nft-sale-mistake-explained/.

991 Christian Suzanne Davik, *The Art of NFTs: Copyright, Contracts, and the Fallacy of Ownership*, 59 Ga. L. Rev. 207 (2024), https://georgialawreview.org/wp-content/uploads/2025/01/Davik_The-Art-of-NFTs.pdf; Gabriella Angeleti, *Crypto group shamed for spending $3m on 'Dune' book, mistakenly believing it had acquired copyright to produce NFTs*, The Art Newspaper (Jan. 17, 2022), https://www.theartnewspaper.com/2022/01/17/nft-group-shamed-jodorowsky-dune-book-copyright

992 Jessica Rizzo, *The* Dune *NFT Fiasco Is the Least of Crypto's Legal Worries*, Wired (Jan. 19, 2022), https://www.wired.com/story/nft-cryptocurrency-art-regulation-law/.

993 Christian Suzanne Davik, *The Art of NFTs: Copyright, Contracts, and the Fallacy of Ownership*, 59 Ga. L. Rev. 207 (2024), https://georgialawreview.org/wp-content/uploads/2025/01/Davik_The-Art-of-NFTs.pdf.

994 Adrienne Westenfeld, *The Saga of the Dune Crypto Bros and Their Very Pricey Mistake Is at Its End*, Esquire (July 28, 2022, 9:24 AM), https://www.esquire.com/entertainment/books/a38815538/dune-crypto-nft-sale-mistake-explained/.

995 U.S. PTO and U.S. Copyright Office, *Non-Fungible Tokens and Intellectual Property: A Report to Congress* (Mar. 2024), https://www.uspto.gov/sites/default/files/documents/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf.

996 *Id.* at iv & 71.

997 *Id*. at 72.

998 *Id.* at 72.

2. Trademark Law

Trademark disputes have also emerged. Few cases have gone to trial, but among the ones that have, the courts have often ruled against the NFT creator.

In *Hermès International v. Rothschild*,[999] Mason Rothschild (whose real name is Sonny Estival) sold NFTs with images of his "MetaBirkins" —a faux fur handbag with blurred colorful images based on the Hermes-trademarked Birkin handbags.[1000] Hermes' trademark did not include downloadable digital representations of their trademarked bag. Rothschild contended that the NFTs were expressive digital art pieces and that his NFTs should be considered free speech. His argument relied on the *Rogers* test,[1001] a judicial tool for determining whether expressive art that incorporates the use of a trademarked image is protected under the First Amendment. The jury, however, rejected Rothschild's argument, finding that the MetaBirkins explicitly misled consumers into believing Hermès had authorized them and determined the NFTs violated Hermès' trademark rights.

In *Nike v. StockX*, Nike sued StockX for infringing the famous shoe company's trademark when StockX, a popular reseller of sneakers and other apparel, created Vault NFTs. Vault NFTs were a new trading idea where the company would allow users to purchase and trade NFTs that linked to physical items housed in a StockX warehouse.[1002] Among these NFTs were those that depicted Nike sneakers. Nike sued StockX for trademark infringement and consumer confusion caused by StockX's unauthorized sales.[1003] Both parties finally settled the case and stated in a joint statement that they had resolved the case "amicably" on confidential terms.[1004]

999 *Hermes Int'l v. Rothschild*, No. 1:22-cv-00384 (S.D.N.Y. June 23, 2023), https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv00384/573363/140/.

1000 Rosemary Feitelberg, *Hermès' and Mason Rothschild's Legal Battle Over 'MetaBirkins' NFTs Continues*, WWD (Mar. 19, 2024), https://wwd.com/fashion-news/fashion-scoops/hermes-mason-rothschilds-leawsuit-metabirkins-nfts-1236268689/.

1001 The "*Rogers* Test" derives from *Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989), in which the Second Circuit held that the Lanham Act, 15 U.S.C. § 1125(a), does not bar use of a trademark in an artistic work unless (1) the use has no artistic relevance to the work, or (2) it explicitly misleads as to the source or content of the work. The test was designed to balance trademark protections against First Amendment rights in expressive works. It was subsequently adopted by multiple federal circuits. Its scope was significantly narrowed by the U.S. Supreme Court in *Jack Daniel's Properties, Inc. v. VIP Products LLC*, 599 U.S. 140 (2023), which held unanimously that the Rogers Test does not apply when a defendant uses a trademark as a source identifier for its own goods or services — that is, "when the challenged use of a mark is as a mark." The Court's majority declined to rule on whether the Rogers Test remains valid in other contexts, leaving that question open for future resolution. A concurrence by Justice Gorsuch (joined by Justices Thomas and Barrett) further cautioned lower courts to "handle Rogers with care," noting that the constitutional basis for the test remains unsettled.

1002 StockX, *StockX Launches Vault NFTs*, (Jan. 18, 2022), https://stockx.com/about/stockx-launches-vault-nfts/.

1003 Blake Brittain, *StockX Blasts Nike Counterfeiting Claims in NFT Trademark Fight*, Reuters (June 6, 2022), https://www.reuters.com/legal/litigation/stockx-blasts-nike-counterfeiting-claims-nft-trademark-fight-2022-06-06/.

1004 Blake Brittain, *Nike Settles Lawsuit Against StockX Over NFTs, Counterfeiting*, Reuters (Aug. 29, 2025), https://www.reuters.com/legal/litigation/nike-settles-lawsuit-against-stockx-over-nfts-counterfeiting-2025-08-29/

FIGURE 37.

Yuga Labs v. Ripps (2025)

Yuga Labs Inc. v. Ripps[1005] involves the parodied use of a famous NFT collection known as Bored Ape Yacht Club (BAYC), created by Yuga Labs. NFT artist Ryder Ripps[1006] and an associate named Jeremy Cahen were both very critical of Yuga Lab's BAYC line of NFTs. Ripps claimed that BAYC was latently promoting neo-Nazi and racist imagery.[1007] In what Ripps claimed was an attempt to satirize the highly popular, celebrity endorsed BAYC NFT collection, he and Cahen created their own collection of NFTs that used the same "digital image file pointers"[1008] to sell a collection of copied NFTs called "RR/BAYC."[1009]

The district court rejected Ripps' First Amendment defense and awarded Yuga Labs a little over $1.5 million in damages, which ultimately grew to roughly $8.8 million with fees and costs.[1010]

On appeal, the Ninth Circuit U.S. Court of Appeals issued a pivotal decision: It held that NFTs constitute "goods" within the meaning of federal trademark law.[1011] It rejected the characterization of NFTs as mere "digital deeds" or authentication mechanisms, emphasizing instead that consumers perceive NFTs as commercial products with independent economic value. The court underscored that NFTs are actively marketed and traded in commerce, confirming their commercial character. The court further concluded that Yuga Labs held valid and enforceable trademark rights and rejected Ripp's First Amendment and fair-use defenses. The case will now return to the district court for trial, since likelihood of consumer confusion must be proven at trial.

3. Securities Law

NFTs face legal challenges from another angle as well. Some authorities, such as the U.S. SEC, have contested the positioning of NFTs as art or creative works expressing an idea. In two 2023 enforcement actions, the SEC claimed NFTs blurred the line between art and investment or fundraising transactions.[1012] It argued that NFTs were unregistered securities. In one case, Impact Theory, a Los Angeles-based media entertainment company,[1013] raised $30 million by selling NFTs that the company's founders said should be taken as an investment in the company itself, with potential future benefits down the line.[1014]

1005 *Yuga Labs, Inc. v. Ripps*, No. CV 22-4355-JFW(JEMx), 2022 WL 18024480 (C.D. Cal. Dec. 16, 2022); https://law.justia.com/cases/federal/appellate-courts/ca9/22-56199/22-56199-2023-10-30.html

1006 Joseph Bernstein, *What's More Provocative Than Sincerity*, N.Y. Times (Mar. 30, 2023), https://www.nytimes.com/2023/03/30/style/ryder-ripps-bored-apes-kanye.html.

1007 Blake Brittain, *Artist Fires Back at Bored Ape Lawsuit With Racism Accusations*, Reuters (Aug. 15, 2022), https://www.reuters.com/legal/litigation/artist-fires-back-bored-ape-lawsuit-with-racism-accusations-2022-08-15/.

1008 Christa J. Laser, *Legal Issues in Blockchain, Cryptocurrency, and Non-Fungible Tokens (NFTs)*, 102 Neb. L. Rev. 761, 796 (2023), https://digitalcommons.unl.edu/nlr/vol102/iss4/3.

1009 David Kappos et al., *The Nail and the Hammer: The Role of Copyrights and Trademarks in NFT Projects*, World Trademark Rev. (Oct. 21, 2022), https://www.cravath.com/a/web/87bQqy577jw23AM2s5p6Gc/4G3UDA/world-trademark-review-the-nail-and-the-hammer-kappos-rosenthal-larrea-b.pdf.

1010 Yuga Labs, Inc. v. Ripps, No. 22-56199, 2023 WL 7165417 (9th Cir. Oct. 30,2023) (mem.), https://cases.justia.com/federal/appellate-courts/ca9/22-56199/22-56199-2023-10-30.pdf; Blake Brittain, *Artist Owes $1.5 mln in Damages for Fake Bored Ape NFTs, Judge Says,* Reuters (Oct. 26, 2023), https://www.reuters.com/legal/litigation/artist-owes-15-mln-damages-fake-bored-ape-nfts-judge-says-2023-10-26/

1011 *Yuga Labs, Inc. v. Ripps*, No. 24-879, slip op. (9th Cir. July 23, 2025), https://cdn.ca9.uscourts.gov/datastore/opinions/2025/07/23/24-879.pdf; David Zaslowsky, *NFTs, Trademarks, and the Ninth Circuit: A Pivotal Decision in Yuga Labs Inc. v. Ryder Ripps* (Aug. 4, 2025), https://blockchain.bakermckenzie.com/2025/08/04/nfts-trademarks-and-the-ninth-circuit-a-pivotal-decision-in-yuga-labs-inc-v-ryder-ripps/

1012 Press Release, U.S. Sec & Exch. Comm'n, *SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs* (Aug. 28, 2023), https://www.sec.gov/news/press-release/2023-163; Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Creator of Stoner Cats Web Series for Unregistered Offering of NFTs* (Sept. 13, 2023), https://www.sec.gov/news/press-release/2023-178.

1013 Impact Theory, https://impacttheory.com/ (last visited Jan. 15, 2026)

1014 *Id.*

Similarly, Stoner Cats 2, a company that was raising funds for an eponymous animated web series, raised about $8 million through the sale of related NFTs.[1015] The NFT creators encouraged investors to buy the NFTs by noting their value could increase once the web series was created. In both cases, the SEC characterized the NFT sales as unregistered offerings of investment contracts and tailored its remedies to target the profit expectation features it had identified.[1016] Both cases signal the SEC's willingness to treat NFT issuers as securities offerors where profit expectations are built into the offering, regardless of its creative framing.[1017]

But the SEC's enforcement posture toward NFTs appears to have evolved over the past eighteen months. In 2024, the SEC filed a Wells Notice (letter of intent to take action) against OpenSea,[1018] a leading NFT marketplace. The letter asserted that NFTs traded on OpenSea constituted unregistered securities.[1019] In February 2025, however, several news outlets reported that OpenSea stated that the SEC had closed its investigation.[1020]

A similar dynamic can be observed in judicial decisions. In September 2025, a judge of the U.S. District Court for the Central District of California dismissed a lawsuit brought by investors against Yuga Labs. The court held that the plaintiffs failed to plausibly allege that the Bored Ape Yacht Club NFTs, ApeCoin (APE), or other Yuga Labs products constituted securities under U.S. law.[1021]

5.1.4. Manipulations of Crypto Markets

Since the earliest days of Bitcoin, cryptocurrency trading markets have been marked by persistent concerns about manipulation and fraudulent activity.[1022] Early investigations into platforms such as Mt. Gox *(See Figure 45)* revealed extensive fabricated trading volume[1023] and other abusive practices, setting a precedent for the lack of integrity that has characterized many segments of the crypto asset ecosystem.[1024] Unlike regulated capital markets —which rely on mandatory disclosure regimes, standardized reporting, and strict separation of intermediary functions— crypto asset markets generally operate without comparable obligations. Issuers and service providers typically do not furnish audited, consistent, or complete information to market participants,[1025] and centralized exchanges are not subject to comprehensive market-surveillance or conflict-of-

1015 For Stoner Cats, see *supra* note 1012.

1016 *Id.*; Jones Day, *SEC Brings Its First Enforcement Action Against Nonfungible Token Sellers* (Sept. 2023), https://www.jonesday.com/en/insights/2023/09/sec-brings-its-first-enforcement-action-against-nonfungible-token-sellers.

1017 Both cases ended in settlements. Impact Theory consented to a cease and desist order, agreed to destroy NFTs in its possession, eliminated secondary market royalties, and paid more than $6 million in penalties to an SEC-mandated Fair Fund for affected purchasers. SEC, *In the Matter of Impact Theory, LLC*, Release No. 33-11226, File No. 3-21585 (Aug. 28, 2023), available at https://www.sec.gov/files/litigation/admin/2023/33-11226.pdf; Stoner Cats 2 LLC similarly consented to a cease and desist order, agreed to destroy its NFTs and waive future royalties, and paid a $1 million civil penalty, also distributed through a Fair Fund. SEC, *In the Matter of Stoner Cats 2, LLC*, Release No. 33-11233, File No. 3-21655 (Sept. 13, 2023), available at https://www.sec.gov/files/litigation/admin/2023/33-11233.pdf.

1018 Aoyon Ashraf, *OpenSea Gets 'Wells Notice' From SEC, Which Calls NFTs Sold on Platform 'Securities'*, CoinDesk (Aug, 29, 2024), https://www.coindesk.com/policy/2024/08/28/opensea-gets-wells-notice-from-sec-calling-nfts-sold-on-platform-securities.

1019 MacKenzie Sigalos, *OpenSea Receives Wells Notice from SEC, Regulators Says NFTs are Securities*, CNBC (Aug. 28, 2024), https://www.cnbc.com/2024/08/28/sec-issues-wells-notice-to-nft-marketplace-opensea.html.

1020 Brady Dale, *SEC Closes Investigation Into OpenSea, Furthering New Stance on Crypto Industry*, Axios (Feb. 21, 2025), https://www.axios.com/2025/02/21/crypto-policy-sec-opensea-coinbase.

1021 *Real v. Yuga Labs*, Inc., No. 2:22-cv-08909 FMO (BFMx), 2025 WL 3437389 (C.D. Cal. Sept. 30, 2025) https://www.courtlistener.com/docket/66623942/288/adonis-real-v-yuga-labs-inc/.

1022 *See generally* U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Sept. 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf [hereinafter U.S. Dept. of the Treasury, Crypto-Assets].

1023 Neil Gandal, J.T. Hamrick, Tyler Moore & Tali Oberman, *Price Manipulation in the Bitcoin Ecosystem*, 95 J. Monetary Econ. 86 (2018), https://tylermoore.utulsa.edu/jme17.pdf.

1024 Tali Oberman et al., *Price Manipulation in the Bitcoin Ecosystem*, CEPR VoxEU (June 22, 2017), https://cepr.org/voxeu/columns/price-manipulation-bitcoin-ecosystem (documenting a spike in 2013 caused by fraudulent trades on the largest exchange at the time, Mt. Gox).

1025 U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses, supra* note 1022, 29.

interest safeguards.[1026] This structural opacity creates significant information asymmetries between insiders and retail purchasers and undermines overall market integrity.

In the absence of robust conduct and disclosure rules, centralized cryptocurrency trading platforms are especially vulnerable to abusive practices that would be unlawful in regulated securities or commodities markets. These practices include wash trading, pump-and-dump schemes, insider trading, coordinated price manipulation, and oracle manipulation.[1027] For several years, the U.S. Securities and Exchange Commission (SEC) declined to approve spot Bitcoin exchange-traded funds (ETFs), citing concerns about fraud and manipulation in the underlying spot markets.[1028] In 2023, however, the U.S. Court of Appeals for the D.C. Circuit, in *Grayscale Investments, LLC v. SEC*, vacated the SEC's denial of Grayscale's proposal to convert its existing Bitcoin Trust into a spot Bitcoin exchange-traded product (ETP). The court concluded that the agency had acted arbitrarily and capriciously.[1029] Following this decision, the SEC approved multiple spot Bitcoin ETPs in January 2024.[1030] These approvals allow Bitcoin-based ETPs to trade on regulated U.S. stock exchanges, including the New York Stock Exchange, Nasdaq and Cboe BZX Exchange[1031].

Nevertheless, empirical research continues to support the SEC's longstanding concerns regarding market manipulation. A widely cited National Bureau of Economic Research (NBER) study has estimated that more than 70% of reported trading volume on unregulated cryptocurrency exchanges consists of wash trading, that is, spurious or fabricated transactions designed to inflate trading activity.[1032] Additionally, the blockchain analytics firm Chainalysis estimated that approximately $2.57 billion in suspicious activity occurred in 2024, although the firm emphasizes that demonstrating conduct that satisfies the legal definition of market manipulation remains difficult in practice.[1033]

One of the most common and recognizable forms of manipulation is the "pump-and-dump" scheme. These schemes involve coordinated market manipulation intended to artificially inflate the price of a cryptocurrency, enabling the perpetrators to sell at the peak for substantial profit.[1034] Typically, the manipulators begin by quietly acquiring, at minimal cost, large quantities of a low-value, low-liquidity cryptocurrency. They then engage in aggressive promotional activity across social media platforms, messaging applications, online forums, and so-called "insider channels," often making false or misleading claims regarding partnerships, technological innovations, or endorsements by public figures. As unsuspecting investors are drawn in by the hype, demand increases and the price rises sharply. Once the price reaches a desirable level, the perpetrators

1026 Int'l Org. of Sec. Comm'ns, Policy (IOSCO), *Policy Recommendations for Crypto and Digital Asset Markets* 25-28 (Nov. 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.

1027 TRM Labs, *Common Market Manipulation Typologies in Crypto and How to Spot Them* (Feb. 28, 2024), https://www.trmlabs.com/resources/blog/common-market-manipulation-typologies-in-crypto-and-how-to-spot-them.

1028 U.S. Sec. & Exch. Comm'n, Order Disapproving a Proposed Rule Change, as Modified by Amendment No. 1, to List and Trade Shares of Grayscale Bitcoin Trust under NYSE Arca Rule 8.201-E (Commodity-Based Trust Shares), Exchange Act Release No. 34-95180 (June 29, 2022), https://www.sec.gov/files/rules/sro/nysearca/2022/34-95180.pdf.

1029 *See Grayscale Investments, LLC v. SEC*, 82 F.4th 1239 (D.C. Cir. 2023). The court held that the SEC acted arbitrarily and capriciously by failing to adequately explain its different treatment of similar products.

1030 U.S. Sec. & Exch. Comm'n, Order Granting Accelerated Approval of Proposed Rule Changes, as Modified by Amendments Thereto, to List and Trade Bitcoin-Based Commodity-Based Trust Shares and Trust Units, Exchange Act Release No. 34-99306 (Jan. 10, 2024), https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf.

1031 *See SEC Approves Bitcoin Exchange-Traded Products (ETPs)*, Cong. Rsch. Serv., IF12573 (Jan. 2024), https://www.congress.gov/crs-product/IF12573.

1032 Lin William Cong, Xi Li, Ke Tang & Yang Yang, *Crypto Wash Trading*, Nat'l Bureau of Econ. Rsch., Working Paper No. 30783 (2022), https://www.nber.org/papers/w30783.

1033 Chainalysis, *Market Manipulation: Suspected Wash Trading on Select Blockchains May Account for Up To $2.57 Billion in Trading Volume* (Feb. 13, 2025), https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/.

1034 *See* Press Release, Commodity Futures Trading Comm'n, *CCFTC Issues First Pump-and-Dump Virtual Currency Customer Protection Advisory* (Feb. 15, 2018), https://www.cftc.gov/PressRoom/PressReleases/7697-18; see *also* Datavisor, *Pump and Dump: The Crypto Scheme of Imagined Value*, https://www.datavisor.com/wiki/pump-and-dump-scams/ (last visited Jan. 15, 2026).

liquidate their holdings en masse, triggering a rapid collapse in value that leaves retail investors with essentially worthless tokens.

While these "pump-and-dump" schemes are unlawful in regulated securities markets, they have proliferated in the cryptocurrency space due to regulatory gaps, the continuous operation of digital asset markets, and the relative anonymity afforded by online communication platforms.[1035] These schemes are frequently coordinated through social media groups on Telegram and Discord, and they typically target cryptocurrencies with low market capitalization and limited trading volume.

Regulators have increasingly sought to address these risks. In late 2024, the SEC charged three firms and nine individuals with executing millions of dollars in wash trades across 60 cryptocurrencies, creating the illusion of liquidity to lure unsuspecting investors.[1036] These firms offered market manipulation-as-a-service to crypto issuers. At the issuers' behest, the firms generated artificial trading volume, manipulating the price of the crypto-assets in question.[1037] The market making firms pleaded guilty to parallel criminal charges relating to their fraudulent manipulation of trading volumes, to artificially increase the trading price and volume of tokens for their clients.[1038] These enforcement actions confirmed long-standing allegations about covert manipulation practices in the industry and further demonstrate how, in the absence of comprehensive regulation, crypto markets remain structurally vulnerable to misconduct.

5.1.5. Notable Bankruptcies

The development of crypto-asset markets has been accompanied by a series of high-profile corporate failures that have exposed recurring structural weaknesses in the ecosystem. While early incidents—such as the 2014 collapse of Mt. Gox *(See Figure 45)*—highlighted deficiencies in infrastructure and internal controls,[1039] the wave of failures between 2022 and 2023 revealed more systemic vulnerabilities linked to leverage, interconnectedness, liquidity mismatches, and governance failures.

The collapse of the Terra–Luna stablecoin in May 2022 *(See Figure 27)* triggered cascading disruptions across crypto markets, leading to the insolvency of several highly leveraged firms, including Three Arrows Capital (3AC), Voyager Digital, and Celsius. These failures were followed by the collapse of FTX in November 2022, one of the largest cryptocurrency exchanges, which exposed profound deficiencies in governance, risk management, and the segregation of customer assets.

Taken together, these episodes underscore the structural risks inherent in the crypto ecosystem: concentrated counterparty exposure, opaque organizational structures, inadequate risk management, and the absence of robust regulatory and supervisory safeguards.

5.1.5.A. Voyager and Three Arrows Capital

Voyager was an American cryptocurrency lending and brokerage platform that froze approximately $1.3 billion in customer assets in mid-2022.[1040] The sharp downturn

1035 *Id.*

1036 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Three So-Called Market Makers and Nine Individuals in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities* (Oct. 9, 2024), https://www.sec.gov/newsroom/press-releases/2024-166.

1037 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Three So-Called Market Makers and Nine Individuals in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities* (Oct. 9, 2024), https://www.sec.gov/newsroom/press-releases/2024-166.

1038 Press Release, U.S. Dep't of Justice, *Cryptocurrency Financial Services Firm "Gotbit" and Founder Plead Guilty to Market Manipulation and Fraud Conspiracy* (Mar. 21, 2025), https://www.justice.gov/usao-ma/pr/cryptocurrency-financial-services-firm-gotbit-and-founder-plead-guilty-market.

1039 Mt Gox Co., Ltd., Report (under Article 157 of the Bankruptcy Act), Tokyo Dist. Ct. 2014 (fu) No. 3830 (July 23, 2014), https://www.mtgox.com/img/pdf/20140723_report_en.pdf.

1040 *Crypto Lender Voyager Digital Files for Bankruptcy*, Reuters (July 6, 2022), https://www.reuters.com/technology/crypto-lender-voyager-files-bankruptcy-2022-07-06 /

in crypto markets placed acute pressure on many firms, but Voyager was particularly vulnerable because of its outsized, unsecured exposure to the hedge fund Three Arrows Capital (3AC).

Three Arrows Capital (3AC) was placed on a path toward liquidation in late June 2022, during the broader crypto market crash.[1041] The fund had accumulated highly leveraged and concentrated positions, including significant exposure to distressed projects such as Terra/Luna. When the TerraUSD (UST) stablecoin lost its peg in May 2022 and the value of Luna collapsed to near zero *(See Figure 27)*, 3AC's already fragile balance sheet deteriorated rapidly. Unable to meet margin calls, unwind its positions, or secure sufficient liquidity, the fund defaulted on multiple loans, including several hundred million dollars owed to Voyager Digital.[1042]

This default critically undermined Voyager's balance sheet. The company lacked the liquidity and capital reserves necessary to absorb such a large unsecured loss, leaving it effectively insolvent. In July 2022, Voyager suspended trading, deposits, and withdrawals, and soon thereafter filed for Chapter 11 bankruptcy protection.[1043] Customers were unable to access their funds for an extended period, creating substantial uncertainty and hardship. In December 2022, Voyager announced a deal in which Binance.US would acquire Voyager's assets. However, by April 2023, Binance.US formally terminated the asset purchase agreement.[1044] After the termination, Voyager indicated it would proceed to exercise an option to return cryptocurrency and cash directly to its customers through the Voyager platform. The episode underscored the systemic vulnerabilities of crypto-lending platforms, particularly their exposure to highly leveraged counterparties and interconnected risks within the digital-asset ecosystem.

5.1.5.B. Celsius Network

Celsius was another large American cryptocurrency lending platform that suspended customer withdrawals in June 2022, amid extreme market volatility triggered by the broader collapse of several major crypto-assets.[1045] The company filed for Chapter 11 bankruptcy protection in July 2022, leaving approximately $4.7 billion in customer assets inaccessible.[1046]

Celsius's business model involved accepting cryptocurrency deposits from users and offering high-yield returns, which it funded through lending activities and various investment strategies.[1047] However, the platform operated with significant asset-liability mismatches: It promised short-term liquidity to users while locking up assets in long-term or illiquid

1041 Alex Hern & Dan Milmo, *Three Arrows Capital to Become Latest Casualty of Crypto Crash*, Guardian (June 29, 2022) https://www.theguardian.com/technology/2022/jun/29/three-arrows-capital-to-become-latest-casualty-of-crypto-crash; *Bankrupt Three Arrows' Liquidators Seek $1.3 Billion from Fund's Founders*, Reuters (June 27, 2023), https://www.reuters.com/technology/crypto-lender-voyager-files-bankruptcy-2022-07-06/

1042 *Three Arrows Capital Crypto Hedge Fund Defaults on Voyager Loan*, CNBC (June 27, 2022) https://www.cnbc.com/2022/06/27/three-arrows-capital-crypto-hedge-fund-defaults-on-voyager-loan.html; *Yoyager Digital Issues Default Notice to Three Arrows Capital*, Coindesk (June 27, 2022), https://www.coindesk.com/business/2022/06/27/voyager-digital-issues-default-notice-to-3ac-draws-down-75m-of-alameda-revolver; *Crypto Hedge Fund Three Arrows Captial Fails to Meet Margin Calls: FT*, Reuters (June 16, 2022) https://www.reuters.com/business/finance/crypto-hedge-fund-three-arrows-capital-fails-meet-margin-calls-ft-2022-06-16/.

1043 Hannah Lang, *Crypto Lender Voyager Digital Suspends Withdrawals, Deposits*, Reuters (July 1, 2022) https://www.reuters.com/markets/us/crypto-lender-voyager-digital-suspends-withdrawals-deposits-2022-07-01/

1044 *Binance.US Calls off $1.3 Billion Deal for Voyager's Assets*, Reuters (Apr. 25, 2023), https://www.reuters.com/markets/deals/binanceus-calls-off-13-bln-deal-voyagers-assets-2023-04-25

1045 Ryan Browne et al., *Crypto Lender Celsius Pauses Withdrawals Due to ' Extreme Market Conditions'*, CNBC (June 13, 2022), https://www.cnbc.com/2022/06/13/crypto-lender-celsius-pauses-withdrawals-bitcoin-slides.html.

1046 Elizabeth Napolitano, *The Fall of Celsius Network: A Timeline of the Crypto Lender's Descent Into Insolvency*, CoinDesk (May 11, 2023), https://www.coindesk.com/markets/2022/07/15/the-fall-of-celsius-network-a-timeline-of-the-crypto-lenders-descent-into-insolvency; Federal Trade Commission, Compl. for Permanent Injunction, Monetary Relief, and Other Relief, No. 1:23-cv-6009 (July 13, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2223137celsiusnetworkcomplaint.pdf.

1047 Michael Hiltzik, *Shame, Suicide Attempts, 'Financial Death' - The Devastating Toll of a Crypto Firm's Failure*, L.A. Times (Aug. 12, 2022), https://www.latimes.com/business/story/2022-08-12/column-celsius-bankruptcy-shows-how-small-crytpo-investors-lost-out; *How Crypto Lender Celsius Stumbled on Risky Bank-Like Investments*, Reuters (June 15, 2022), https://www.reuters.com/business/finance/how-crypto-lender-celsius-stumbled-risky-bank-like-investments-2022-06-15/.

investments.[1048] This structural imbalance made the platform particularly vulnerable during market downturns.

Investigations and bankruptcy filings revealed that Celsius used customer funds to engage in high-risk trading and investment practices, including exposure to volatile DeFi protocols and speculative positions.[1049] Furthermore, regulatory authorities and creditors raised serious concerns that Celsius may have functioned, in part, as a Ponzi scheme, using deposits from new customers to meet withdrawal demands and maintain the illusion of profitability.[1050] The founder and CEO of Celsius, Alex Mashinsky, was sentenced to 12 years imprisonment for his fraud and market manipulation.[1051]

5.1.5.C. The FTX Collapse

Despite the failures of several major crypto firms earlier in 2022, FTX continued operating until early November 2022, when its financial position rapidly deteriorated. At the time, FTX was one of the world's largest digital-asset exchanges, with roughly $10 billion in daily trading volume and a $32 billion valuation.[1052] Founded by Samuel Bankman-Fried, FTX marketed itself as a trustworthy, sophisticated, and risk-managed exchange.[1053] Bankman-Fried repeatedly asserted that customer deposits were segregated, safely held in custody, and never used by the company. He also insisted that Alameda Research, his affiliated trading firm, operated independently from FTX.[1054]

This narrative collapsed after a media article revealed that Alameda Research's balance sheet relied heavily on FTX Tokens (FTT), a native token created by FTX itself.[1055] Alameda held approximately $5.8 billion in unlocked FTT, and FTX and Alameda collectively controlled roughly 80% of the total FTT supply.[1056] This concentration allowed the two companies to assign a high notional valuation to FTT and then use that token as collateral to secure loans and inflate their balance sheets. Because FTT lacked external backing and was thinly traded outside the FTX ecosystem, the structure was inherently fragile and highly susceptible to any shock affecting FTT's price.

Once Alameda's dependence on FTT became public, both FTX and Alameda confronted an acute liquidity crisis.[1057]

1048 Neelanjut Das et al., *Celsius Balance Sheet Has An Asset-Liability Mismatch of Nearly $1.2 Billion, Show Court Documents*, Outlook Money (Updated Sep. 6, 2024), https://www.outlookmoney.com/news/celsius-balance-sheet-has-an-asset-liability-mismatch-of-nearly-1-2-billion-show-court-documents-news-209348; Fed. Trade Comm'n, *FTC Reaches Settlement with Crypto Platform Celsius Network; Charges Former Executive with Duping Consumers* (July 13, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-reaches-settlement-crypto-platform-celsius-network-charges-former-executives-duping-consumers.

1049 *See* Compl., *People v. Mashinsky*, Index No. Unassigned (N.Y. Sup. Ct. filed Jan. 5, 2023), https://ag.ny.gov/sites/default/files/mashinsky_complaint.pdf; Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Celsius Network Limited and Founder Alex Mashinsky with Fraud and Unregistered Offer and Sale of Securities* (July 13, 2023), https://www.sec.gov/newsroom/press-releases/2023-133.

1050 *See*, e.g. Nikhilesh De, *Celsius Misled Investors About Financial Health, Vermont Regulator Alleges*, CoinDesk (May 11, 2023), https://www.coindesk.com/policy/2022/09/07/celsius-misled-investors-about-financial-health-vermont-regulator-alleges.

1051 Press Release, U.S. Dep't of Justice, Founder of Celsius Sentenced to 12 Years for Fraud and Market Manipulation (May 8, 2025), https://www.justice.gov/usao-sdny/pr/founder-celsius-sentenced-12-years-fraud-and-market-manipulation .

1052 *Crypto Exchange FTX Valued at $32 Bln as SoftBank Invests*, Reuters (Jan. 31, 2022) https://www.reuters.com/markets/us/crypto-exchange-ftx-valued-32-bln-softbank-invests-2022-01-31; Shange Fu et al., *FTX Collapse: A Ponzi Story*, ArXiv (Dec. 19, 2022) https://arxiv.org/pdf/2212.09436.

1053 Nemit Shroff & Cate Reavis, *Sam Bankman-Fried's FTX*, , MIT Sloan School of Management, Case Study (Jan 17, 2024), https://mitsloan.mit.edu/sites/default/files/2024-06/Sam%20Bankman-Fried%27s%20FTX.pdf.

1054 Alison Frankel, *In the SEC's Suit Against Bankman-Fried, What About the Customers?*, Reuters (Dec. 13, 2022), https://www.reuters.com/markets/us/secs-suit-against-bankman-fried-what-about-customers-frankel-2022-12-13/; *Sam Bankman-Fried Says He "Didn't Ever Try to Commit Fraud"*, Reuters (Dec. 1, 2022), https://www.reuters.com/technology/sam-bankman-fried-says-he-didnt-ever-try-commit-fraud-2022-11-30/; *How a Secret Software Change Allowed FTX to Use Client Money*, Reuters (Dec. 13, 2022), https://www.reuters.com/technology/how-secret-software-change-allowed-ftx-use-client-money-2022-12-13/

1055 Ian Allison, *Divisions in Sam Bankman-Fried's crypto empire blur on his trading titan Alameda's balance sheet*, CoinDesk, (Nov 2, 2022), https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet

1056 *FTX Token Falls 80% Despite Binance Bailout as Alameda Contagion Spreads to Bitcoin*, CoinDesk (Nov. 8, 2022), https://www.coindesk.com/markets/2022/11/08/ftx-token-falls-80-despite-binance-bailout-as-alameda-contagion-spreads-to-bitcoin; *Blockchain Analysis: The Collapse of Alameda and FTX*, Nansen (Nov. 16, 2022), https://research.nansen.ai/articles/blockchain-analysis-the-collapse-of-alameda-and-ftx.

1057 Allison, *supra* note 1055; Rise and Fall of Crypto Exchange FTX, Reuters (Nov. 16, 2022), https://www.reuters.com/markets/currencies/rise-fall-crypto-exchange-ftx-2022-11-10/; John J. Ray III, *Decl. of John J. Ray III in Support of Chapter 11 Petitions & First Day Pleadings*, In re FTX Trading Ltd., No. 22-11068 (Bankr. D. Del. Nov. 17, 2022), https://bankruptcy-proxy-api.dowjones.ai/cases/Delaware_Bankruptcy_Court/1--22-bk-11068/FTX_Trading_Ltd/docs/24.pdf.

Subsequent investigations confirmed that FTX had routed significant amounts of customer deposits to Alameda over several years. According to regulatory complaints and sworn bankruptcy filings, customer funds were used to cover trading losses,[1058] finance investments, and support other expenditures.[1059] These practices were obscured through internal accounting systems, intercompany transfers, and inflated valuations of FTT used as collateral. Bankruptcy filings further indicated that FTX materially misrepresented its financial condition and operated with limited internal governance controls.[1060]

Market confidence evaporated after Binance announced that it would liquidate its FTT holdings, accelerating a crisis that was already underway.[1061] Within days, FTX, Alameda Research, and approximately 130 affiliated entities filed for Chapter 11 bankruptcy in the United States.[1062] By then, the shortfall in customer funds was estimated at roughly $8 billion.[1063] Post-bankruptcy investigations confirmed that Bankman-Fried had orchestrated a multi-year scheme to misappropriate customer assets, using them to subsidize Alameda's losses and fund personal expenditures and political giving.[1064] He was later convicted on multiple counts of fraud and sentenced to 25 years in prison, a conviction he has since appealed.[1065] Two of his key lieutenants, Caroline Ellison and Ryan Salame, also received custodial sentences.[1066]

FTX's collapse represents one of the most significant failures in the history of the crypto sector and a major financial fraud case under U.S. law. Experts argue that weak prudential oversight and pervasive opacity allowed FTX to construct an unsustainable leverage system.[1067] The system was based on issuing an uncollateralized native token, maintaining concentrated control over its supply, and using that token as collateral for extensive borrowing. Importantly, however, FTX was a centralized cryptocurrency exchange that operated in a manner comparable to traditional financial intermediaries. The misconduct that led to its collapse relied on discretionary control over customer assets, opaque internal accounting, and undisclosed transfers between affiliated entities. Fully decentralized exchanges, which operate through automated smart contracts and do not take custody of user funds, generally do not allow for this type of misuse of customer deposits — though they remain exposed to other vulnerabilities.

1058 Angus Berwick, *Exclusive: At Least $1 Billion of Client Funds Missing at Failed Crypto Firm FTX—Sources,* Reuters (Nov. 13, 2022), https://www.reuters.com/markets/currencies/exclusive-least-1-billion-client-funds-missing-failed-crypto-firm-ftx-sources-2022-11-12/; Complaint at 1, *CFTC v. FTX Trading Ltd.*, No. 1:22-cv-10503 (S.D.N.Y. filed Dec. 13, 2022), https://www.cftc.gov/media/7986/enfftxtradingcomplaint121322/download; Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX* (Dec. 13, 2022), https://www.sec.gov/newsroom/press-releases/2022-219

1059 *SEC Press Release, FTX Charges* (Dec. 13, 2022), https://www.sec.gov/newsroom/press-releases/2022-219.

1060 John J. Ray III, who was appointed CEO of FTX in the aftermath of its collapse, declared: "Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here. From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, unsophisticated and potentially compromised individuals, this situation is unprecedented;" Ray Decl., *supra* note 1057, at 5; CFTC Compl., *supra* note 1058; Complaint, *SEC v. Ellison*, No. 1:22-cv-10794 (S.D.N.Y. filed Dec. 21, 2022) https://www.sec.gov/files/litigation/complaints/2023/comp25617.pdf.

1061 Angus Berwick & Tom Wilson, *Exclusive: Behind FTX's Fall, Battling Billionaires and Failed Bid to Save Crypto*, Reuters (Nov. 10, 2022), https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/; Lisa Pauline Mattackal & Medha Singh, *Cryptoverse: So Long, Solona? Ether Rival Clobbered by FTX Crash*, Reuters (Nov. 16, 2022) https://www.reuters.com/technology/cryptoverse-so-long-solana-ether-rival-clobbered-by-ftx-crash-2022-11-15/

1062 *Cryptocurrency Exchange FTX Files for Bankruptcy Protection in U.S.*, Guardian (Nov. 11, 2022), https://www.theguardian.com/technology/2022/nov/11/cryptocurrency-exchange-ftx-files-for-bankruptcy-protection-in-us

1063 Press Release, U.S. Dep't of Justice, *Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes* (Mar. 28, 2024), https://www.justice.gov/archives/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes.

1064 *Id*.

1065 B*ankman-Fried Sentenced to 25 Years for Multi-Billion Dollar FTX Fraud*, Reuters (Mar. 28, 2024) https://www.reuters.com/technology/sam-bankman-fried-be-sentenced-multi-billion-dollar-ftx-fraud-2024-03-28; *United States v. Bankman-Fried*, No. 24-961 (2d Cir., appeal filed Apr. 11, 2024).

1066 *FTX Executives Salame and Ellison See Reduced Prison Sentences*, UNLOCK (Dec. 26, 2024), https://www.unlock-bc.com/135160/ftx-executives-salame-and-ellison-see-reduced-prison-sentences/.

1067 David Vidal-Tomás et al., *FTX's Downfall and Binance's Consolidation: The Fragility of Centralised Digital Finance*, 625 Physica A, 11 (2023), https://eprints.lse.ac.uk/119902/1/FTX_s_downfall.pdf

The collapse nevertheless intensified an ongoing trend toward centralization in the crypto industry.[1068] Binance's dominance increased markedly after FTX's failure, with its share of global trading volume rising from 48.7% in early 2022 to 66.7% by year's end.[1069] In contrast to the decentralized, peer-to-peer vision set out by Nakamoto, the cryptocurrency sector appears to be consolidating around large, centralized intermediaries that operate much like traditional financial institutions, yet often remain outside comprehensive regulatory oversight.[1070]

5.2. CRIMINAL AND ILLICIT BEHAVIORS

While blockchain transparency may assist law-enforcement investigations *(See section 5.5.1)*, the main features of decentralized systems —pseudonymity, permissionless access, and the absence of intermediaries— enable exploitation by criminals. Criminal actors exploit these features in two principal ways: first, by using cryptocurrency as a medium of exchange for illegal activities; and second, by directly attacking blockchain infrastructure to steal digital assets. This section examines the first category: how criminals leverage blockchain's structural features for illicit finance, fraud, and scams. Section 5.3 addresses the second category: direct technical attacks on blockchain systems themselves.

The absence of centralized authority or built-in monitoring mechanisms creates structural conditions that enable criminal exploitation such as fraud executed directly on-chain and the use of cryptocurrency as payment for off-chain criminal conduct. However, as discussed in section 5.2.1., actual measured criminal activity on blockchains remains a small fraction of total transaction volume —significantly lower when compared to illicit activity in traditional finance. The examples studied in section 5.2.2. illustrate the range of criminal schemes that blockchain's features enable.

5.2.1. The Debate About the Prevalence of Blockchain-Enabled Criminal Activity

While blockchain's pseudonymity and decentralization support important, legitimate use cases, these same characteristics can also create conditions attractive to criminals. Unlike many internet-based services, public blockchains generally do not require user identification or even basic web credentials.[1071] Anyone can generate unlimited wallet addresses at no cost and deploy self-executing smart contracts without approval from a trusted intermediary. As a result, transactions can be carried out under pseudonyms and outside the traditional framework in which financial intermediaries collect identifying information and enforce compliance obligations.

Moreover, because decentralized networks lack a single administrative point of control, law-enforcement agencies cannot rely on the presence of a centralized entity that can be identified, investigated, or subpoenaed. With traditional financial services, at least one, and often all, entities involved in a transaction are obliged to conduct checks for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT).[1072] But decentralized systems lack a central party responsible for monitoring such activity and ensuring compliance with the law.[1073] This structural lack of accountability provides opportunities for criminal actors

1068 *Id*.

1069 *Id*.

1070 *Id*.

1071 Europol, *Europol Spotlight- Cryptocurrencies: Tracing the Evolution of Criminal Finances* (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

1072 U.S. Dep't of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

1073 Fin. Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* at paras 67, 101, 106 (2021), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

to conceal illicit activity —opportunities that do not exist in fully intermediated legacy payment systems, such as credit cards or bank transfers.[1074]

Historically, many blockchain service providers, particularly early centralized exchanges, operated with minimal safeguards against illicit activity and, in some cases, tolerated or failed to prevent money-laundering practices.[1075] Over the past decade, however, anti-money laundering and counter-terrorist financing (AML/CFT) obligations, together with KYC requirements,[1076] have progressively expanded to the crypto-asset sector and have increasingly aligned across jurisdictions. In particular, the Financial Action Task Force (FATF), an international AML standards-setting body,[1077] extended its longstanding Recommendation 16, traditionally applicable to banks and wire transfers, to virtual assets and Virtual Asset Service Providers (VASPs), in 2019.[1078] This requirement, commonly known as the "Travel Rule," obliges covered intermediaries to collect, retain, and transmit identifying information about the originator and beneficiary of a transaction.[1079]

In practice, Travel Rule compliance in blockchain-based systems is primarily implemented by intermediaries at key points in the transaction lifecycle. These include custodial wallet providers, centralized exchanges, and other services acting as on- and off-ramps between crypto-assets and fiat currency.[1080] Reflecting this shift, a 2020 industry survey reported that approximately 77% of crypto-asset service providers conducted AML/CFT and KYC checks for all customer accounts.[1081] By contrast, decentralized finance (DeFi) protocols generally operate outside the conventional VASP framework, since non-custodial, decentralized applications are often not classified as VASPs. Only certain developers, operators, or governance participants — where they exercise sufficient control or influence— may fall within the scope of VASP regulation.[1082] Protocol developers have not, to date, been consistently treated as obligated entities.[1083] This regulatory gap represents a growing concern as DeFi platforms increasingly facilitate large volumes of transactions[1084] without corresponding oversight mechanisms.

1074 *Id.*; see *also* U.S. Dep't of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 16 (2022), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

1075 Europol, *supra* note 1072 at 8-9.

1076 Anti-Money Laundering (AML) and Know Your Customer (KYC) are core elements of regulatory compliance frameworks aimed at preventing financial crimes such as money laundering, fraud, and terrorist financing. AML comprises the rules and practices used to detect and deter illicit financial activity, while KYC—one of its central components—requires institutions to verify the identity of individuals or entities before establishing a business relationship, Fed. Fin. Insts. Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual: Suspicious Activity Reporting* (rev. 2020), https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04

1077 The FATF is a "soft law," intergovernmental standard-setting body in which states cooperate to develop and promote policies to combat money laundering, terrorist financing, and proliferation financing. Created by the G7 in 1989 in response to rising concerns about illicit financial flows, the FATF issues non-binding recommendations that member jurisdictions commit to implement domestically. Compliance is monitored through a peer-review process known as mutual evaluations, and non-compliant jurisdictions may face significant reputational and economic consequences. *See Fin. Action Task Force*, https://www.fatf-gafi.org/en/home.html (last visited Jan. 15, 2026).

1078 Fin. Action Task Force, *The FATF Recommendations*, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html (last visisted Jan. 15, 2026).

1079 The "travel rule" was recently incorporated into EU law. See section 7.3.4.B; Regulation (EU) 2023/113, on information accompanying transfers of funds and certain crypto-assets, art. 14-17, 2023 O.J. (L150) 1, https://eur-lex.europa.eu/eli/reg/2023/1113/oj.

1080 Tom Barbereau and Balázs Bodó, *Beyond financial regulation of crypto-asset wallet software: In search of secondary liability*, 49 Comp. L. & Sec. Rev. 105829 (2023), https://www.sciencedirect.com/science/article/pii/S0267364923000390.

1081 20% applied them selectively based on transaction thresholds, behavioral patterns, or user location. Only 3% performed no KYC checks. The same study showed higher compliance rates when fiat transactions were involved (72%) than when activity was entirely crypto-to-crypto (46%). Apolline Blandin et al., *3rd Global Crypto-asset Benchmarking Study* 54-55, Cambridge Ctr. for Alt. Fin., Univ of Cambridge, (Sept. 2020), https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

1082 *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021), summarized in Merkle Science, *Key Takeaways from the FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Nov. 2, 2021), https://www.merklescience.com/blog/key-takeaways-from-the-fatf-updated-guidance-on-vas-and-vasps; Galaxy Digital, *FATF's Finalized Guidance for Virtual Asset Service Providers* (Oct. 28, 2021), https://www.galaxy.com/insights/research/fatf-finalized-guidance-virtual-asset-service-providers (noting that DeFi applications and software are not VASPs as such, and that only certain creators/owners/operators with sufficient control may be treated as VASPs).

1083 Fin. Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* 29-32 (June 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.

1084 Chainalysis, *Decentralized Exchanges' On-Chain Transaction Volumes Grow* (Sept. 19, 2023), https://www.chainalysis.com/blog/defi-dexs-web3/ (reporting that between April 2021 and April 2022, approximately $224 billion was sent on-chain to DEXs versus $175 billion to centralized exchanges, giving DEXs "a confident lead in on-chain transaction volume").

Within this framework, it remains uncertain whether blockchain significantly increases the *overall* risk or prevalence of criminal activity or merely provides an additional channel for misconduct that already exists. Crypto markets are vulnerable to misconduct and unfair harms.[1085] However, even if the reputational association between cryptocurrency and crime persists,[1086] available data suggest that criminal activity on public blockchains is less prevalent than commonly perceived.[1087] In absolute terms, Chainalysis estimated that illicit crypto addresses received approximately $24.2 billion in 2023, describing this as a lower-bound estimate subject to upward revision as additional illicit addresses are identified.[1088] However, data suggest that illicit activity represents a small share of overall crypto transaction volume. According to Chainalysis's *2025 Crypto Crime Report*, the proportion of total crypto transaction volume linked to identified illicit addresses had declined to approximately 0.14%, in 2024, down from 0.61% in 2023.[1089] Historically, this figure has remained below 1%. When the volumes of legitimate transactions rise, the absolute amount of criminal activity tends to rise as well, but its relative share remains low.[1090] These figures call into question the claim that blockchain technology has materially increased global criminal activity beyond what long-established channels —such as bank transfers, informal value-transfer systems, or bulk cash— already facilitate.[1091] The volume of illicit on-chain activity generally increases as the overall blockchain ecosystem expands, but not at a faster rate than legitimate use increases.[1092]

Nonetheless, regulators worry that, as blockchain adoption grows, more traditional criminal networks, including narcotics traffickers and human-smuggling organizations, may eventually learn to exploit blockchain tools and privacy-enhancing technologies.[1093] These concerns are heightened by the fact that many U.S.-based crypto asset service providers still show inconsistent compliance with anti-money-laundering obligations, with some failing to comply entirely or failing to comply in a meaningful way.[1094] While some regulators have warned that the technology may facilitate illicit finance or pose national-security risks,[1095] some industry stakeholders contend that exaggerating the scale of crypto-enabled crime risks distorting the policy debate.[1096]

1085 U.S. Dep't of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, *supra* note 1022, 25–33

1086 Board of Governors of the Federal Reserve System, Fed. Deposit Ins. Corp. & Office of the Comptroller of the Currency, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (Jan. 3, 2023), https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf?utm_source; Chainalysis, *2025 Crypto Crime Report* (2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

1087 Chainalysis, Cryptocurrency and Terrorism Financing: Correcting the Record (Oct. 18, 2023), https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/.

1088 *Id.* at 3 (reporting that "2023 saw a significant drop … to a total of $24.2 billion" and cautioning that these figures are lower-bound estimates that will likely increase as additional illicit addresses are identified and historic activity is incorporated).

1089 Chainalysis, *The 2025 Crypto Crime Report* 4 (2025), https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf.

1090 *2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-chain Crime Becomes Increasingly Diverse and Professionalized*, Chainalysis (Jan. 15, 2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

1091 See U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 4 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf; Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances* (2022) https://oipol.org/wp-content/uploads/2022/01/europol-spotlight-cryptocurrencies-tracing-the-evolution-of-criminal-finances.pdf; Simon Butler, *Criminal Use of Cryptocurrencies – A Great New Threat or Is Cash Still King?* (Royal Holloway Univ. of London), https://pure.royalholloway.ac.uk/ws/files/42792707/Accepted_Manuscript.pdf

1092 *2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-chain Crime Becomes Increasingly Diverse and Professionalized*, Chainalysis (Jan. 15, 2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

1093 U.S. Gov't Accountability Off., *As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Law Enforcement,* (Feb. 24, 2022), https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement.

1094 Treasury Department, *2024 National Money Laundering Risk Assessment* 59-62 (Feb. 2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

1095 Exec. Order No. 14,067, Ensuring Responsible Development of Digital Assets, 87 Fed. Reg. 14,143, WH (Mar. 9, 2022), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

1096 Jennifer J. Schulp et al., *Overstating Crypto Crime Won't Lead to Sound Policy*, Cato Institute (Jan. 27, 2023), https://www.cato.org/blog/overstating-crypto-crime-wont-lead-sound-policy.

Furthermore, it is important to emphasize that all transactions on public blockchains are permanently recorded, publicly accessible, and increasingly traceable using advanced analytics. This makes it easier to detect and deter illicit behavior. Firms such as Chainalysis[1097] and Elliptic[1098] have developed sophisticated tools that map transaction flows and identify patterns associated with illicit activity. Law-enforcement and regulatory agencies have adapted their investigative techniques and supervisory approaches,[1099] enabling significant improvements in forensic investigation. While traditional finance systems identify only a very small proportion of illicit actors,[1100] tracking criminal activity on open blockchains can, in many cases, be easier than tracking transactions in the traditional financial system.[1101]

However, this transparency advantage does not extend uniformly across all crypto-assets. Privacy coins such as Monero and Zcash *(See section 2.6.4.)* employ cryptographic techniques that obscure transaction details, making them significantly more challenging for law enforcement to trace. While privacy coins represent a relatively small share of overall cryptocurrency transaction volume, their use in illicit transactions is disproportionately high.[1102] This creates an ongoing investigative challenge that partially undermines the transparency advantages of public blockchains.

5.2.2. Criminal Activities Facilitated by Blockchain Features

Blockchain's structural features have enabled diverse forms of criminal exploitation, ranging from payments for illegal activities to sophisticated fraud schemes targeting investors.[1103]

5.2.2.A. Crypto Payments

Blockchain-enabled criminal activities extend far beyond cybercrime. They encompass any form of misconduct that requires moving or storing monetary value.[1104] The most common forms include illicit finance, money laundering, terrorism financing, sanctions evasion, and ransomware campaigns.[1105]

1. Crypto Financing of Illicit Activities

In the early stages of the ecosystem, cryptocurrencies were rapidly adopted on darknet marketplaces. The most emblematic example was Silk Road, an original darknet marketplace for drugs and other unlawful goods and services.[1106]

1097 Jonathan Levin, Testimony, Oversight of the Financial Stability Oversight Council: Risks and Regulatory Gaps in the Rising U.S. Digital Asset Market (Mar. 17, 2022), https://www.banking.senate.gov/imo/media/doc/Levin%20Testimony%203-17-223.pdf

1098 *How Elliptic's Blockchain Analysis Brings Visibility to Crypto Transaction*s, Bitcoin Mag., https://bitcoinmagazine.com/press-releases/how-elliptics-blockchain-analysis-brings-visibility-to-crypto-transactions

1099 TRM Labs, *The Crypto Maturity Model: How Law Enforcement Agencies Are Scaling Blockchain Intelligence* (May 20, 2025), https://www.trmlabs.com/resources/blog/the-crypto-maturity-model-how-law-enforcement-agencies-are-scaling-blockchain-intelligence.

1100 Elliot Berman, *Beyond Traditional Red Flags: How Hybrid Threat Finance is Revolutionizing Financial Crime Detection* (Nov. 4, 2025), https://www.amlrightsource.com/resources/beyond-traditional-red-flags-how-hybrid-threat-finance-is-revolutionizing-financial-crime-detection.

1101 Chainalysis Team, *Senate Hearing on "Understanding the Role of Digital Assets in Illicit Finance" Underscores the Value of Blockchain Transparency* (Mar. 22, 2022), https://www.chainalysis.com/blog/senate-hearing-underscores-value-of-blockchain-transparency/; see *also* Fin. Action Task Force, Countering Ransome Financing 4 (Mar. 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf

1102 Prachi Pandey, *Privacy Coins: Legitimate Uses and Illicit Risks Explained*, Merkle Science (July 29, 2024), https://www.merklescience.com/blog/privacy-coins-legitimate-uses-and-illicit-risks-explained.

1103 U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses, supra* note 1022, at 26.

1104 Europol, *supra* note 1072, 16-25; U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, *supra* note 1022, 16-25.

1105 FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, (June 2014), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; Europol, *supra* note 1072.

1106 U.S. Attorney's Office, Press Release, *Southern District of New York, Manhattan U.S. Attorney Announces The Indictment Of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website* (Feb. 4, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

FIGURE 38.

Silk Road (2013)

Silk Road was a darknet marketplace that operated from approximately 2011 until its shutdown by the U.S. government in 2013. It facilitated anonymous transactions using Bitcoin to allow users to buy and sell illegal drugs, goods, and services beyond the reach of traditional law enforcement authorities.[1107] As part of the dark web, Silk Road operated as a hidden service on the anonymous communication network Tor, allowing users to buy and sell goods anonymously. Silk Road accepted bitcoin as payment and so became popularly associated and nearly synonymous with bitcoin.[1108] Silk Road is credited for introducing "a million people to bitcoin" and etching the first connection between bitcoin and online crime.[1109]

Silk Road's founder Ross Ulbricht was apprehended in 2013[1110] and convicted in 2015 for drug distribution, money laundering, and other related charges.[1111] Though Ulbricht received a life sentence for his crimes, President Donald Trump granted Ulbricht a full and unconditional pardon in 2025, fulfilling a pledge the incoming president made to crypto supporters and libertarians.[1112]

Even after the demise of the Silk Road, cryptocurrencies have been used to finance a wide range of unlawful activities, including terrorism and state-sponsored threats.[1113] For instance, U.S. authorities have documented that North Korean groups generate significant revenue through cyber-enabled theft and laundering of virtual currency. Those proceeds are used to fund the regime's ballistic-missile and weapons of mass destruction programs.[1114] The North Korean-affiliated Lazarus Group, responsible for major cyber intrusions, is estimated to have stolen over $6 billion in crypto-assets[1115] that directly support the country's nuclear program.[1116]

Terrorist organizations have also experimented with cryptocurrency fundraising.[1117] Terrorist groups such as ISIS and Hamas have reportedly received transfers in crypto,[1118] prompting sustained attention from U.S. lawmakers and intelligence agencies. These developments have fueled ongoing debates about how to strengthen AML/CFT controls without undermining legitimate uses of decentralized technologies.[1119]

1107 National Security Archive, *Silk Road: Investigation of a DEA and Secret Service Agents Involvement with an Online Black Market Site* (Dec. 13, 2019), https://nsarchive.gwu.edu/news/cyber-vault/2019-12-13/silk-road-investigation-dea-secret-service-agents-involvement-online-black-market-site.

1108 *Silk Road- an Overview,* Sci. Direct Topics, https://www.sciencedirect.com/topics/computer-science/silk-road;

1109 David Yaffe-Bellany et al., *How Trump Was Persuaded to Pardon an Online Drug Kingpin*, N.Y. Times (Jan. 22, 2025), https://www.nytimes.com/2025/01/22/technology/ross-ulbricht-trump-pardon.html.

1110 Press Release, U.S. Attorney's Office, Southern District of New York, *Manhattan U.S. Attorney Announces The Indictment Of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website* (Feb. 4, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

1111 *Id.*; *United States v. Ross William Ulbricht*, 858 F.3d 71 (2d Cir. 2017); Aarti Shahani, *Jury Convicts Ross Ulbricht of Operating Drug Marketplace*, NPR (Feb. 5, 2015), https://www.npr.org/2015/02/05/383988611/jury-convicts-ross-ulbricht-of-operating-drug-marketplace.

1112 *Trump Pardons Founder of Drug Marketplace Whose Case Had Become a Cause Célèbre*, Politico (Jan. 21, 2025), https://www.politico.com/news/2025/01/21/trump-pardons-ulbricht-silk-road-00199848; Charles Bethea, *Why Trump Freed Ross Ulbricht, the Silk Road's Dread Pirate Roberts*, New Yorker (Jan. 27, 2025), https://www.newyorker.com/news/the-lede/why-trump-freed-ross-ulbricht-the-silk-roads-dread-pirate-roberts.

1113 Fin. Action Task Force, *supra* note 1073, at paras 10, 18.

1114 *Treasury Targets Actors Facilitating Illicit DPRK Financial Activity,* U.S. Dep't of the Treasury (Apr. 18, 2023),https://home.treasury.gov/news/press-releases/jy1435

1115 Patricia Kowsmann, *How North Korea Cheated Its Way to Crypto Billions*, Wall St. J. (Apr. 3, 2025), https://www.wsj.com/world/asia/north-korea-cryptocurrency-580d7d3f; *see also* Kole Zellers, *Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme*, 12 Penn. St. J.L. & Int'l Aff. 261 (2024), https://elibrary.law.psu.edu/jlia/vol12/iss2/10.

1116 Robert MacMillan & Dustin Volz, *How North Korea's Hacker Army Stole $3 Billion in Crypto, Funding Nuclear Program*, Wall St. J. (June 11, 2023), https://www.wsj.com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782.

1117 *Hamas Militants Behind Israel Attack Raised Millions in Crypto*, Wall St. J. (Oct. 10, 2023), https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a. The exact amount actually financed is in debate. Rena S. Miller, Liana W. Rosen & Paul Tierno, *Terrorist Financing: Hamas and Cryptocurrency Fundraising*, Cong. Res. Srv, (Dec. 9, 2024), https://crsreports.congress.gov/product/pdf/IF/IF12537.

1118 TRM Labs, *2025 Crypto Crime Report* 9-11 (2025), https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67f7132b33d3535ca28a54a4_TRM_2025%20Crypto%20Crime%20Report.pdf; *In Wake of Moscow Attack: Understanding ISIS' Use of Cryptocurrencies*, TRM Labs (Mar. 23, 2024), https://www.trmlabs.com/post/in-wake-of-moscow-attack-understanding-isis-use-of-cryptocurrencies.

1119 *Miller et al.*, *supra* note 1117.

2. Money Laundering

From the inception of cryptocurrency markets, regulators have emphasized the technology's vulnerability to money laundering.[1120] Blockchain introduces specific dynamics in money laundering: Accounts (wallet addresses) can be created quickly and at no cost; each account can be used to receive and transfer money only once, breaking the funds-tracing chain; large, low-cost money laundering schemes with thousands of transfers can be executed using computer scripts; and the rapid increases in exchange rates for some cryptocurrencies (e.g., 10,000% growth) make it easy to explain unexpected wealth.[1121]

Regulators have expressed concern about privacy coins *(See section 2.6.4.)*, which opacity makes it even more difficult to trace the source and destination of transactions.[1122] Although current evidence suggests their adoption for illicit activity remains limited,[1123] exchanges worldwide face pressure to delist them because of their inherent opacity.[1124]

A laundering technique unique to crypto is mixing (also known as blending or tumbling), in which funds from multiple users are blended together to obscure the origin and ownership of funds *(See section 2.6.2.)*. While mixers can be used legitimately to restore privacy on transparent blockchains, they are also widely used to obfuscate criminal proceeds.[1125] According to the U.S. Treasury, mixers have facilitated ransomware payments, state-sponsored hacking, and evasion of sanctions, and they have raised "an acute money laundering and national security risk."[1126]

Enforcement actions in recent years underscore the scale of compliance failures. The extent of these violations has been so pervasive that they have incurred some of the largest fines on record. Among those subject to enforcement actions are the largest cryptocurrency exchanges, such as Binance[1127] and BitMEX,[1128] and smaller developer outfits, such as Tornado Cash *(See section 6.5.3)* and Samourai Wallet *(See section 7.2.3)*.[1129]

1120 Fin. Action Task Force, *supra* note 1083.

1121 *Money Laundering Through Cryptocurrencies*, United Nations, https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html (last visited Jan. 15, 2026).

1122 Fin. Action Task Force, *supra* note 1083.

1123 Eric Silfversten et al., *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes*, RAND (May 6, 2020), https://www.rand.org/pubs/research_reports/RR4418.html.

1124 Alexander Culafi, *Monero and the Complicated World of Privacy Coins*, TechTarget (Jan. 24, 2022) https://www.techtarget.com/searchsecurity/news/252512394/Monero-and-the-complicated-world-of-privacy-coins?Offer=abt_pubpro_AI-Insider; N.Y. State Dep't of Fin. Servs., *Industry Letter: Proposed Updates to Guidance Regarding Listing of Virtual Currencies* (Sept. 18, 2023), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230918_guidance_vc_listing.

1125 *Crypto Mixers: How They Work and How to Stop Them*, Chainalysis (Aug. 23, 2022) https://www.chainalysis.com/blog/crypto-mixers/.

1126 *FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing,* Fin. Crimes Enf't Network (Oct. 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

1127 Press Release, U.S. Dep't of Just., Off. of Pub. Affs., *Binance and CEO Plead Guilty to Federal Charges in $4B Resolution*, (Nov. 21, 2023) https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution; Press Release, U.S. Dep't of Treasury, *U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws,* (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925.

1128 Press Release, U.S. Att'y's Off. for the S. Dist. of N.Y., *Global Cryptocurrency Exchange BitMEX Fined $100 Million For Violating Bank Secrecy Act,* (Jan. 15, 2025), https://www.justice.gov/usao-sdny/pr/global-cryptocurrency-exchange-bitmex-fined-100-million-violating-bank-secrecy-act.

1129 Peter Van Valkenburgh, *Analysis: The Disappointing Denial of Tornado Dev's Motion to Dismiss*, Coin Center (Oct. 8, 2024), https://www.coincenter.org/analysis-the-disappointing-denial-of-tornado-devs-motion-to-dismiss/; Peter Van Valkenburgh, *Coin Center Fellow Michael Lewellen Is Suing the DOJ over Their Criminalization of Software Development*, Coin Ctr. (Jan. 16, 2025), https://www.coincenter.org/coin-center-fellow-michael-lewellen-is-suing-the-doj-over-their-criminalization-of-software-development/.

FIGURE 39.

Blender (2022)

On May 6, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on Blender.io, a cryptocurrency mixing service designed to conceal the origin and destination of Bitcoin transactions submitted to the mixing service.[1130] According to OFAC, North Korean state-sponsored hackers used Blender.io to facilitate malicious cyber activities and launder stolen virtual currency. OFAC's investigation further found that Blender.io had processed transactions for ransomware groups linked to Russia. As a result of the sanctions, all property and interests in property of Blender.io that are located in the United States or held by U.S. persons must be frozen and reported to OFAC. The sanctions also prohibit providing or receiving any funds, goods, or services to, from, or for the benefit of Blender.io.

3. Sanctions Evasion

Blockchain's decentralized and pseudonymous nature makes it a potentially attractive tool for individuals and entities seeking to evade international economic sanctions. Economic sanctions are imposed by governments and international organizations to restrict dealings with designated individuals, entities, or countries, often in response to illicit activities or violations of international law. Crypto enables cross-border transfers of value without regulated financial intermediaries, allowing sanctioned actors to bypass systems that would otherwise freeze or block transactions.[1131]

The U.S. Treasury has documented several cases in which sanctioned actors used cryptocurrencies to evade restrictions, such as those imposed on Russia,[1132] including for the purchase of high-tech weapons parts.[1133] Since Russia's invasion of Ukraine, Russian oil companies have turned to crypto to bypass Western sanctions.[1134] Iran and North Korea have also used crypto to circumvent U.S. sanctions, pay for imports, and make up for lost revenues.[1135] As global adoption increases, the risk is that cryptocurrencies could dilute the effectiveness of sanctions imposed by the U.S. and EU. At the same time, advancements in blockchain tracing tools and analytics may help limit the evasion of such sanctions by improving detection capabilities.[1136]

1130 Press Release, U.S. Treasury Dept., *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats* (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.

1131 Gov't Accountability Office, *The Effectiveness of Economic Sanctions At Risk from Digital Asset Growth* (Jan. 16, 2024), https://www.gao.gov/blog/effectiveness-economic-sanctions-risk-digital-asset-growth.

1132 Press Release, U.S. Dep't of the Treasury, *Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions* (Dec. 4, 2024), https://home.treasury.gov/news/press-releases/jy2735.

1133 Angus Burwich & Ben Foldy, *Inside the Russian Shadow Trade for Weapons Parts, Fueled by Crypto*, Wall St. J. (Apr. 1, 2024), https://www.wsj.com/finance/currencies/crypto-fuelsrussian-shadow-trade-for-weapons-parts-1bfdc1a1?mod=hp_listb_pos3.

1134 Francisco Rodrigues, *Russia Turns to Crypto to Bypass Western Sanctions in Oil Trade: Reuters*, CoinDesk (Mar. 14, 2025), https://www.coindesk.com/markets/2025/03/14/russia-turns-to-crypto-to-bypass-western-sanctions-in-oil-trade-reuters.

1135 William Alan Reinsch & Andrea Leonard Palazzi, *Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia*, CSIS (Dec. 20, 2022), https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia.

1136 Gov't Accountability Office, *supra* note 1131.

4. Ransomware

Ransomware is a cyber-extortion tactic in which attackers deny victims access to their computer systems —or threaten to release stolen data— unless the victims pay a ransom. While ransomware predates cryptocurrency, digital assets have become the preferred method of ransom payment due to their liquidity, speed, and irreversibility.[1137] The FATF and U.S. Department of Homeland Security now describe crypto as a "near universal form of ransom payments" in such ransomware attacks.[1138]

Ransomware imposes heavy costs on private and public entities alike.[1139] One of the most disruptive attacks occurred in 2021 on the Colonial Pipeline, the operator of a major U.S. oil and gas infrastructure. The attack forced the temporary shutdown of the U.S.'s largest refined products pipeline, disrupting fuel supplies on the East Coast.[1140] In 2023 alone, criminal actors allegedly obtained around $1 billion in ransomware payments, although there is a lack of comprehensive data on the amount of ransomware attacks and the use of crypto in those attacks.[1141]

FIGURE 40.

Ransomware-as-a-service

Beyond the use of cryptocurrency as a payment instrument for ransom demands, some ransomware operations have also experimented with incorporating blockchain infrastructure into their technical architecture.[1142] For instance, the Cerber ransomware operation, active primarily between 2016 and 2017, functioned as a ransomware-as-a-service (RaaS) model that allowed non-technical affiliates to deploy malware while developers maintained it in exchange for a share of the criminal proceeds.[1143] In this model, affiliates conducted the attacks while the operators provided the malware and supporting infrastructure.

Rather than rely solely on hardcoded server addresses — which defenders can easily block— Cerber used infected machines as proxies to query hardcoded Bitcoin wallet addresses via public Bitcoin APIs to retrieve small pieces of encoded data stored in the blockchain. Once Cerber decoded this data, it extracted updated configuration information, including the IP address of the attacker's command-and-control (C2) server, enabling the malware to dynamically update its communications channel. Because this information had been embedded in advance in transactions associated with those wallet addresses, the malware could retrieve it directly from the blockchain. This technique allowed the malware to resume operations by retrieving a new server address recorded in the blockchain, even after defenders had shut down its previous command-and-control infrastructure.

1137 U.S. Sen. Comm. on Homeland Sec. & Govt. Affairs, *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns, at 1* (2022), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf.

1138 U.S. Sen. Comm. on Homeland Sec. & Govt. Affairs, *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns,* at 2-4 (2022), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf; FATF, *Countering Ransomware Financing* (Mar. 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf

1139 FATF, *supra* note 1138.

1140 Jen Easterly & Tom Fanning, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years* (May 7, 2023), https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

1141 Medha Singh, *Crypto Ransom Attack Payments Hit Record $1 Billion in 2023 - Chainalysis*, Reuters (Feb. 7, 2024), https://www.reuters.com/technology/cybersecurity/crypto-ransom-attack-payments-hit-record-1-billion-2023-chainalysis-2024-02-07/.

1142 *See generally* José Antonio Gómez Hernández et al., *Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges*, 12 Electronics 4494 (2023), https://doi.org/10.3390/electronics12214494.

1143 Taylor Monahan, *Blockchain Malware's Neverending Novelty*, MetaMask Security Blog, (Nov. 3, 2025), https://metamask.io/news/blockchain-malwares-neverending-novelty.

5.2.2.B. Crypto Scams

From the earliest days of Bitcoin to the present, crypto ecosystems have been repeatedly exploited through fraudulent schemes, resulting in tens of billions of dollars in cumulative losses.[1144] Crypto scams remain the most prominent sources of consumer complaints to regulators. In 2024, the FBI's Internet Crime Complaint Center reported $9.3 billion worth of losses "with a nexus to cryptocurrency" in the United States alone —a 66% increase from 2023.[1145]

Several structural features of crypto markets contribute to this phenomenon, including the ease of issuing tokens on permissionless blockchains, the pseudonymous nature of transactions, the ability to transfer funds globally and instantaneously without intermediaries, and the limited availability of consumer-protection mechanisms on many platforms.

This section provides an overview of the principal categories of crypto scams and selected illustrative cases. Additional examples —such as exit scams (Appendix 14), romance scams, and wallet drainers (Appendix 15)— are discussed in the Appendices.

1. Initial Coin Offering (ICO) Scams

The ICO boom of 2017-2018 enabled many legitimate fundraising efforts but also produced a wave of fraudulent offerings. ICOs allowed businesses to raise capital by issuing digital tokens in exchange for fiat or other crypto-assets.[1146] However, a significant number of projects overstated technical claims, misused funds, or were outright fraudulent.

One famous example involved OneCoin, a pyramid scheme in which Karl Sebastian Greenwood and Ruja Ignatova (dubbed as the "Cryptoqueen" in the press) collected approximately $4 billion before being exposed.[1147] OneCoin began operations in 2014 and was based in Sofia, Bulgaria. It marketed and sold a fraudulent cryptocurrency through a global multi-level-marketing (MLM) network.[1148] The scheme used Bitcoin's popularity to convince investors that OneCoin was the next "can't miss" opportunity. Greenwood pleaded guilty and a U.S. district court judge sentenced him to 20 years in prison. The Federal Bureau of Investigation added Ignatova, who is believed to be a fugitive from the law, on its Ten Most Wanted Fugitives list. There were more than 3.5 million victims who invested in OneCoin and lost more than $4 billion from the scheme.[1149]

1144 *See* Xuan-Thao Nguyen, *Crypto Losses* 2024 U. Ill. L. Rev. 1119, 1141 (2024), https://digitalcommons.law.uw.edu/faculty-articles/1107.

1145 Fed. Bureau of Investigation, Cryptocurrency Fraud Report 35 (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

1146 European Securities Markets Authority, *Advice: Initial Coin Offerings and Crypto-Assets* 11 (2019), https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

1147 Faith Karimi, *This 'Cryptoqueen' Scammed Investors Out of $4 Billion, the FBI Says. Then She Boarded a Plane and Disappeared*, CNN Business (Jan. 22, 2023), https://www.cnn.com/2023/01/22/business/ruja-ignatova-cryptoqueen-fbi-most-wanted-cec/index.html.

1148 Press Release, U.S. Dep't of Justice, S. Dist. of N.Y., *Co-Founder of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced to 20 Years in Prison* (Sept. 12, 2023), https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison.

1149 *Id.*

FIGURE 41.

BitConnect (2018)

The cryptocurrency investment platform BitConnect collapsed in 2018 after raising $2.4 billion in a Ponzi scheme.[1150] Launched in 2016, the platform claimed to generate profits, promising returns of up to 1% per day.[1151]

Investors deposited Bitcoin, received BitConnect Coin (BCC), and locked it for preset periods so the platform could generate profits by exploiting fluctuations in the cryptocurrency markets using its so-called "BitConnect Trading Bot and Volatility Software." In addition, BitConnect employed a multi-level marketing structure, incentivizing users to recruit new investors by offering commissions and bonuses. However, no verifiable evidence ever emerged to indicate the alleged trading bot existed, and investigations revealed that the returns paid to earlier investors were funded primarily by the deposits of newer participants.

In early 2018, regulatory authorities in Texas and North Carolina issued cease-and-desist orders against BitConnect, citing concerns over securities fraud and unlicensed investment operations.[1152] Shortly thereafter, BitConnect shut down, causing BCC to lose more than 90% of its value within days and leaving investors with billions in losses.[1153] Subsequent SEC charges and U.S. federal indictments targeted the platform's promoters[1154] and founder.[1155] Many victims were unable to recover their funds, with restitution efforts in 2023 recovering only a small fraction (approximately $17,646,801 of the total $2 billion funds lost).[1156]

2. Scam Tokens

Scam tokens are fraudulent digital assets created to deceive investors, often by mimicking legitimate projects and promising unrealistic returns or using fake affiliations and endorsements. Private research found that over 200,000 scam tokens were deployed to blockchains between September 2020 and December 2022.[1157] Another 2024 analysis found that nearly 60% of tokens launched in 2024 were "malicious in nature."[1158]

Scammers often create counterfeit versions of legitimate cryptocurrencies by imitating well-known names, logos, or branding. For example, they may issue tokens with

1150 Press Release, Fed. Bureau of Investigation, *Seeking Potential Victims in Bitconnect Investigation* (Mar. 1, 2021), https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/seeking-potential-victims-in-bitconnect-investigation; *FBI Looking for Investors Who Lost Money in Cryptocurrency Ponzi Scheme*, News 5 Cleveland (Feb. 20, 2019), https://www.news5cleveland.com/news/local-news/cleveland-metro/fbi-looking-for-investors-who-lost-money-in-cryptocurrency-ponzi-scheme; U.S. Dep't of Justice, *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme* (Feb. 25, 2022), https://www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

1151 *Fraud Deconstructed: Cryptocurrency Execs Charged for $2.4 Billion Ponzi Scheme*, BDO Canada, https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme.

1152 Nikhilesh De, *US State Regulators Hit BitConnect With Second Cease-And-Desist*, CoinDesk (Jan. 11, 2018), https://www.coindesk.com/markets/2018/01/11/us-state-regulators-hit-bitconnect-with-second-cease-and-desist

1153 Press Release, U.S. Dep't of Justice, *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme* (Feb. 25, 2022), https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

1154 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Global Crypto Lending Platform and Top Executives in $2 Billion Fraud (Sept. 1, 2021), https://www.sec.gov/newsroom/press-releases/2021-172.

1155 Press Release, U.S. Dep't of Justice, *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme* (Feb. 25, 2022), https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

1156 Press Release, IRS, *Victims of BitConnect Scheme to Receive More Than $17 Million to Compensate for Losses* (Jan. 12, 2023), https://www.irs.gov/compliance/criminal-investigation/victims-of-bitconnect-scheme-to-receive-more-than-17-million-to-compensate-for-losses.

1157 Solidus Labs, *The 2022 Rug Pull Report* (Dec. 2022), https://www.soliduslabs.com/reports/rug-pull-report.

1158 Oliver Knight, *More Than Half of Crypto Tokens Debuted in 2024 Were Malicious: Blocaid*, CoinDesk, (Dec. 19, 2024). https://www.coindesk.com/business/2024/12/19/more-than-half-of-crypto-tokens-debuted-in-2024-were-malicious-blockaid.

misleading names, such as "Ethereum 2.0" or "Bitcoin Pro," to falsely suggest an affiliation with established projects.[1159] During Ethereum's transition to proof of stake, fraudulent "ETH2" tokens proliferated, falsely claiming that users had to swap their Ether for upgraded versions.[1160]

Fake endorsements also amplify deception. Scammers routinely impersonate public figures through hijacked or fabricated social media accounts. These fraudulent accounts often advertise so-called "cryptocurrency giveaways," falsely promising to multiply any cryptocurrency sent by the user: for example, "Send 1 BTC, receive 2 BTC in return."[1161] In the six months leading up to May 2021, U.S. consumers reported over $2 million in losses tied to scams impersonating billionaire Elon Musk.[1162] Fraudulent YouTube livestreams using recycled interviews have similarly misled victims by displaying QR codes linked to scam wallets.[1163] Similar tactics have been employed using fake accounts impersonating Vitalik Buterin, the co-founder of Ethereum.[1164] Victims are instructed to "validate" their wallets or participate in non-existent airdrops or token migrations.[1165]

Celebrity endorsements without proper disclosure have also played a role. In 2022, the SEC charged reality TV star Kim Kardashian for promoting the EthereumMax (EMAX) token without revealing she had been paid $250,000 to do so.[1166] Earlier, professional boxer Floyd Mayweather and music producer DJ Khaled settled similar charges involving the Centra Tech ICO,[1167] whose founders were later convicted of criminal fraud.[1168]

In the past few years, the rise of decentralized exchanges (DEXs) has dramatically lowered the barriers to launching tokens. On permissionless DEXs like Uniswap *(See section 4.2.3.)*, developers can create and list a token within minutes and at negligible cost, with no audits, registration, KYC, or platform gatekeeping. This renders the creation of scam tokens very easy and cheap. Empirical studies of tokens listed on major DEXs, such as Uniswap V2, have found that a very large proportion of newly created tokens display characteristics strongly associated with scams,[1169] with a significant fraction of liquidity pools drained within hours or days.[1170]

1159 *See* Raphael Sanis, *Ethereum Merge Scams: Bad Actors Profit from Paradigm Shift,* CAPITAL.COM (Sept. 8, 2022), https://capital.com/ethereum-merge-scams; David Canellis, *Bitcoin Fraudsters Target Head of $230B Fund in Latest Facebook Scam*, TNW (Nov. 26, 2019), https://thenextweb.com/news/bitcoin-facebook-cryptocurrency-scam-fraud-temasek.

1160 *See Ethereum Security and Scam Prevention*, ETHEREUM, (Sept. 13, 2024) https://ethereum.org/en/security; Raphael Sanis, *Ethereum Merge Scams: Bad Actors Profit from Paradigm Shift,* CAPITAL.COM (Sept. 8, 2022), https://capital.com/ethereum-merge-scams.

1161 Xigao Li et al., *Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams*, in Network and Distributed System Security (NDSS) Symposium 2023, https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f584_paper.pdf.

1162 Emma Fletcher, *Cryptocurrency Buzz Drives Record Investment Scam Losses*, FTC (May 17, 2021), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses.

1163 Logos of legitimate companies, such as SpaceX and Tesla, are often misused to lend an appearance of credibility. Pihu Yadav, *Beware! Elon Musk Deepfake Livestream Scams Thousands With Fake Crypto Scheme*, CNBC TV18 (Aug. 25, 2024), https://www.cnbctv18.com/technology/elon-musk-deepfake-youtube-live-scam-warning-cryptocurrency-online-fraud-19465212.htm.

1164 James Hunt, *The Merge: Verified Twitter Accounts Impersonate Ethereum Co-Founder to Push Scams*, THE BLOCK (Sept. 14, 2022), https://www.theblock.co/post/169911/the-merge-verified-twitter-accounts-impersonate-ethereum-co-founder-to-push-scams. Impersonators create counterfeit social media profiles claiming to represent Buterin and frequently promote false offers related to "Ethereum 2.0 upgrades."

1165 Felix Ng, *3 Ways Scammers Will Try to Fool You Over Ethereum's Merge*, COINTELEGRAPH (Sept. 14, 2022), https://cointelegraph.com/news/3-ways-scammers-will-try-to-fool-you-over-ethereum-s-merge.

1166 Press Release, U.S. SEC. & EXCH. COMM'N, *SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security* (Oct. 3, 2022), https://www.sec.gov/newsroom/press-releases/2022-183; David Zaslowsky, *Kim Kardashian's Crypto Post Costs Her $1.26 Million* BAKER MCKENZIE BLOG (Dec. 12, 2022), https://blockchain.bakermckenzie.com/2022/10/12/kim-kardashians-crypto-post-costs-her-1-26-million/.

1167 Press Release, U.S. SEC. & EXCH. COMM'N, *Two Celebrities Charged With Unlawfully Touting Coin Offerings* (Nov. 29, 2018), https://www.sec.gov/newsroom/press-releases/2018-268.

1168 Tanzeel Akhtar, *Centra Tech Co-Founder Gets 8 Years for Crypto Fraud*, COINDESK (Jan. 23, 2024), https://www.coindesk.com/markets/2021/03/05/centra-tech-co-founder-gets-8-years-for-crypto-fraud.

1169 Bruno Mazorra et al., *Do Not Rug on Me: Zero-Dimensional Scam Detection,* ARXIV (Jan. 18, 2022), https://arxiv.org/abs/2201.07220.; Alisa Kalacheva et al., *Detecting Rug Pulls in Decentralized Exchanges: The Rise of Meme Coins* (unpublished manuscript) (Oct. 9, 2024), https://ssrn.com/abstract=4981529.

1170 Abdulrahman Alhaidari et al., *SolRPDS: A Dataset for Analyzing Rug Pulls in Solana Decentralized Finance, in Proc. Fifteenth ACM Conf.on Data & Application Sec. and Privacy* 293 (2025), https://dl.acm.org/doi/10.1145/3714393.3726487.

In 2024, Pump.fun emerged as one of the most prolific sources of scam tokens.[1171] The platform enables users to create and launch their own meme coins *(See section 2.4.1.D.)* within minutes and at negligible cost, dramatically lowering the barriers to token issuance. Its permissionless architecture, automated token-generation tools, and powerful distribution mechanics have made it a central vector for mass-produced tokens.[1172] As a result, the platform has faced growing public and regulatory scrutiny: The U.K. Financial Conduct Authority issued a consumer warning in late 2024,[1173] major promotional accounts associated with Pump.fun were suspended on X in 2025,[1174] and a class-action lawsuit was filed against it in the United States, alleging unregistered securities offerings and the facilitation of widespread fraud.[1175]

3. Exit Scams

An exit scam occurs when operators of a crypto exchange, platform, or project abruptly cease operations and disappear with user funds.[1176] For instance, in 2019, the Chinese wallet/exchange PlusToken vanished with over $2 billion collected from users *(See Appendix 14)*. Typically, the perpetrators first establish a business that appears legitimate then abruptly shut down the platform. Users discover that they are unable to access their funds, the website has been taken off-line, and all communication channels have been severed. Exit scams are particularly dangerous in cryptocurrency because transactions are typically irreversible, pseudonymous, and often occur in regulatory gray areas with limited investor protections.

4. Rug Pulls

Rug pulls are similar to exit scams: Developers launch what appears to be a legitimate cryptocurrency or decentralized finance (DeFi) project, attract investor capital, and then abruptly abandon the project while absconding with the invested funds.[1177] But with rug pulls, the scammer develops a crypto token, deploys it on a blockchain, and convinces investors to buy it –typically, through a decentralized exchange rather than a centralized platform.

Rug pulls typically include:[1178]

- The creation of a seemingly credible token or DeFi project, often accompanied by a professional website, a detailed white paper, and an active social media presence.
- The establishment of a liquidity pool by pairing the newly created token with a well-established cryptocurrency, such as Ether (ETH), on a decentralized exchange.
- The aggressive promotion of the project, often by making exaggerated or false claims about expected returns or technological innovation, to attract retail investors.
- The execution of the fraud once a substantial amount of liquidity has been accumulated, by withdrawing all funds from the liquidity pool, selling their token holdings, and abandoning the project. This causes the token's value to collapse to near zero, leaving investors with worthless assets and no means of redress.

1171 Solidus Labs, *Solana Rug Pulls & Pump-and-Dumps,* CoinDesk (May 7, 2025), https://www.coindesk.com/business/2025/05/07/98-of-tokens-on-pump-fun-have-been-rug-pulls-or-an-act-of-fraud-new-report-says.

1172 *Id.*

1173 FCA Warning: *Pump.fun,* Fin. Conduct Auth. (Mar. 12, 2024), https://www.fca.org.uk/news/warnings/pumpfun.

1174 *Pump.fun and Other Memecoin Accounts Suspended From X in Apparent Crackdown*, CoinDesk (June 17, 2025), https://www.coindesk.com/markets/2025/06/17/pumpfun-and-other-memecoin-accounts-suspended-from-x-in-apparent-crackdown.

1175 Cheyenne Ligon, *Pump.Fun Hot With Proposed Class Action Lawsuit Alleging Securities Violations*, CoinDesk (Jan. 30, 2025), https://www.coindesk.com/policy/2025/01/30/pump-fun-hit-with-proposed-class-action-lawsuit-alleging-securities-violations

1176 *What is a Rug Pull? DeFi Scams Explained*, Solidus Lab Blog (Oct. 27, 2022), https://www.soliduslabs.com/post/rug-pull-crypto-scams.

1177 Nina Semczuk, *What is a Rug Pull?*, Bankrate (Mar. 3, 2025), https://www.bankrate.com/investing/what-is-a-rug-pull/.

1178 *Id.; see* Haffizzuddin Fahmi Hashim, *Decoding DeFi: The Future of Finance or a Hacker's Playground? (Part 2)*, F-Secure (May 1, 2025) https://www.f-secure.com/us-en/partners/insights/decoding-defi-the-future-of-finance-or-a-hacker-s-playground-part-2.

Rug pulls have become increasingly prevalent within the DeFi ecosystem,[1179] largely due to the minimal barriers to creating tokens and the absence of effective regulatory oversight.[1180] Several high-profile cryptocurrency frauds illustrate the scale and frequency of rug pulls and related schemes:

- **Squid Game Token (2021)**: In 2021, the Squid Game Token —named after the popular Netflix series— experienced a price surge of 75,000% before the developers disappeared with approximately $3.3 million.[1181] Investors were unable to sell their tokens due to restrictive features embedded in the smart contract.[1182]
- **AnubisDAO (2021)**: AnubisDAO raised $60 million but vanished within 24 hours of its token launch, leaving investors with no recourse.[1183]
- **Luna Yield (2021)**: Luna Yield, a Solana-based decentralized finance (DeFi) project, disappeared with an estimated $10 million in investor funds.[1184]
- **Compounder Finance (2020)**: In 2020, Compounder Finance, another DeFi platform, exploited a backdoor in its smart contracts to steal approximately $11 million from users.[1185]

While enforcement actions have increased substantially in recent years *(See section 7.2.)*, the scale, sophistication, and diversity of crypto-enabled scams continue to evolve, from ICO frauds and exit scams to DEX-based rug pulls and the more sophisticated schemes discussed in the Appendices 14 and 15.

5.3. CYBER SECURITY CHALLENGES

A common claim in favor of decentralization is that it enhances security by reducing single points of failure.[1186] In centralized architectures, the compromise of one entity —whether it be a cloud provider, a payment processor, or a financial intermediary— can jeopardize the data and assets of millions of users. Decentralized networks mitigate this risk by distributing validation and control across multiple nodes or validators, making it far more difficult for an attacker to seize control of the system as a whole.

Yet decentralization does not eliminate security vulnerabilities.[1187] While Section 5.2 examines how criminals use blockchain as a payment mechanism or to exploit its features for fraud, this section focuses on direct attacks against blockchain infrastructure itself. Those attacks target the technical vulnerabilities in protocols,

1179 The Rug Pull Report, CertiK (Oct.7, 2023), https://www.certik.com/resources/blog/the-rug-pull-report; *see also*: Phuong Duy Huynh et al, *Serial Scammers and Attack of the Clones: How Scammers Coordinate Multiple Rug Pulls on Decentralized Exchanges*, in proceedings of the ACM on Web Conference 2025 (WWW '25). Association for Computing Machinery, New York, NY, USA, 1016–1033, https://doi.org/10.1145/3696410.3714919.

1180 *The Rise of Rug Pulls: How DeFi Projects Exploit Investors*, OSL (Apr. 17, 2025), https://www.osl.com/hk-en/academy/article/the-rise-of-rug-pulls-how-defi-projects-exploit-investors .

1181 *Squid Game Crypto Token Collapses in Apparent Scam*, BBC (Nov. 1, 2021), https://www.bbc.com/news/business-59129466; Camomile Shumba, *'Squid Game' Token Goes Offline After Skyrocketing 75,000% - and That Means the 'Scam' is Over, CoinGecko Says*, Bus. Insider (Nov. 3, 2021), https://markets.businessinsider.com/news/currencies/the-squid-game-token-scam-website-socials-offline-coingecko-crypto-2021-11;

1182 *On the Trail of the Squid Game Scammers*, TRM Blog (Jan. 12, 2023), https://www.trmlabs.com/resources/blog/on-the-trail-of-the-squid-game-scammers#:~:text=Within%20weeks%20of%20SQUID%E2%80%99s%20launch,scammers%20walked%20away%20with%20millions.

1183 Carla Mozée, *A Crypto Project That Raised $60 Million Overnight Using a Dog Meme Saw All of That Money Go Missing in What May Have Been a Phishing Attack*, Bus. Insider (Oct. 31, 2021), https://markets.businessinsider.com/news/currencies/crypto-project-phishing-attack-anubisdao-olympusdao-token-sale-2021-10.

1184 Jose Oramas, *Luna Yield, A Solana Yield Aggregator, Rug-Pulls and Steals Almost $10 Million*, CryptoPotato (Aug. 22, 2021), https://cryptopotato.com/luna-yield-a-solana-yield-aggregator-rug-pulls-and-steals-almost-10-million/.

1185 William Foxley, *$10.8M Stolen, Developers Implicated in Alleged Smart Contract 'Rug Pull'*, CoinDesk (Sept. 14, 2021), https://www.coindesk.com/tech/2020/12/02/108m-stolen-developers-implicated-in-alleged-smart-contract-rug-pull.

1186 Loïc Miller and Marc-Oliver Pahl, *Collaborative Cybersecurity Using Blockchain: A Survey*, arXiv, (2024), https://arxiv.org/abs/2403.04410; *see also*, Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Network*, RAND Corp. Res. Memorandum 3420 (Aug. 1964), https://www.rand.org/pubs/research_memoranda/RM3420.html.

1187 *See* Mike Orcutt, *Once Hailed as Unhackable, Blockchains Are Now Getting Hacked*, MIT Tech. Rev. (Feb. 19, 2019), https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

applications, and intermediaries, and they exploit human error among individual users. A substantial and growing body of research documents the weaknesses that persist in blockchain protocols and their surrounding infrastructures.[1188] As adoption of blockchain expands and the value locked in blockchain-based services increases, the crypto ecosystem is becoming an increasingly attractive target for sophisticated attackers seeking to steal digital assets through exploitation of code vulnerabilities, operational failures, and social engineering.

Over the past several years, multiple malicious exploits have succeeded, collectively costing users and projects tens of billions of dollars. According to estimates cited by the U.S. Department of the Treasury, roughly $3.2 billion in digital assets was stolen in 2021 much of it from DeFi protocols, with most of these funds proving unrecoverable.[1189] Some trackers reported a modest decline in losses in 2024, to around $2.2 billion.[1190]

In 2025, however, losses increased sharply, exceeding $3.4 billion, driven by a few mega-hacks.[1191] In February 2025, the centralized exchange *Bybit* suffered a loss by theft of approximately $1.4 billion to $1.5 billion —one of the largest exploits in cryptocurrency history.[1192]

Unofficial analytics databases such as Rekt estimate that *cumulative* exploit losses across all major on-chain thefts and hacks have exceeded $100 billion, with less than 10% recovered.[1193] Many high-impact incidents have been attributed to state-linked actors, such as North Korea's Lazarus Group. One report estimates that North Korean-backed hackers have amassed crypto thefts estimated to total as much as $6.75 billion, with over $2 billion stolen in 2025 alone. [1194] Other high-profile cases involve large-scale money-laundering activities linked to centralized intermediaries. These include Russia-linked platforms such as BTC-e,[1195] which U.S. authorities describe as having processed billions of dollars in illicit proceeds and, more recently, the A7A5 stablecoin and Cambodia-based Huione Group, alleged to have laundered funds for North Korea and criminal organizations in Southeast Asia.[1196] They also include major exchange hacks in which stolen assets were subsequently laundered through complex cross-platform schemes.[1197]

However, despite these vulnerabilities and the substantial losses from individual incidents, major blockchain networks have demonstrated considerable resilience at the foundational level. Attacks on the underlying

1188 Qihao Bao et al., *A Survey of Blockchain Consensus Safety and Security: State-of-the-Art, Challenges, and Future Work*, J. Syst. Softw., 196 (2023), 111555, https://www.sciencedirect.com/science/article/abs/pii/S016412122200231X; Collin Connors & Dilip Sarkar, *Survey of prominent blockchain development platforms,* J. Netw. Comput. Appl. (2023)103650: https://ouci.dntb.gov.ua/en/works/4VZEJqe4/; Huaqun Guo & Xingjie Yu, *A survey on blockchain technology and its security* Blockchain: Res. Appl., 3 (2) (2022) 100067 https://www.sciencedirect.com/science/article/pii/S2096720922000070; Mohammad Dalvi Esfahani et al., *Blockchain Features for Facilitating Circular Economy Adoption in the Palm Oil Industry: A DEMATEL Approach,* 11 J. Soft Computing & Decision Support Syss. 1, 1 (2024), https://jscdss.com/index.php/files/article/view/271; Xiaoqi Li et al., *A survey on the security of blockchain systems*, Future Gener. Comput. Syst.(2020), 841-853, https://arxiv.org/abs/1802.06993.

1189 U.S. Dep't of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, supra note 1022, 18-19, 29.

1190 TRM Labs, *supra* note 1118.

1191 Chainalysis, *2025 Crypto Theft Reaches $3.4 Billion* (Jan. 4, 2026), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/.

1192 *Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft,* Chainanalysis (Feb. 24, 2025), https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/.

1193 De.Fi Rekt Database, DE.FI, https://de.fi/rekt-database; *Comprehensive List of DeFi Hacks & Exploits*, Chainsec, https://chainsec.io/defi-hacks/ (last visited Jan. 15, 2026).

1194 *North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion*, Chainanalysis (Dec. 18, 2025), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/; Ines Kagubare, *Crypto Hack Alarms Ramp Up As Authorities Crack Down After $3.7 Billion Stolen*, The Hill (June 20, 2023), https://thehill.com/policy/cybersecurity/4050333-crypto-hack-alarms-ramp-up-as-authorities-crack-down-after-3-7-billion-stolen/.

1195 Press Release, U.S. Dept. of Justice, *Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another*, (June 9, 2023), https://www.justice.gov/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another.

1196 *Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale*, (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/; Press Release, U.S. Dept of the Treasury, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Nov. 4, 2025), https://home.treasury.gov/news/press-releases/sb0278.

1197 Tom Carreras, *How North Korea Launders Billions in Stolen Crypto*, CoinDesk (Mar. 13, 2025), https://www.coindesk.com/policy/2025/03/07/here-s-how-north-korea-launders-billions-of-stolen-crypto.

blockchain consensus layer are theoretically possible. They can happen, for instance, through "51% attacks," in which an adversary controlling a majority of a network's mining or validation power can reorganize the ledger or execute double-spend attacks *(See Figure 21)*.[1198] But such incidents remain rare on major networks due to the substantial computational or economic resources required. Bitcoin, for instance, has never suffered a successful consensus-layer compromise since its launch in 2009.[1199] The vast majority of security incidents occur at higher levels of the technology stack —in smart contracts, centralized intermediaries, and through exploitation of individual users rather than attacks on the underlying blockchain protocol itself.

This section therefore focuses on three predominant categories of incidents: attacks on the application layer, attacks on centralized intermediaries, and attacks targeting individual users. A distinct category of risk arises when blockchain infrastructure is used not as the target of an attack but as a component of malware delivery systems; this case is discussed in Appendix 16.

5.3.1. Hacks on the Application Layer

Most security breaches in the crypto ecosystem occur not at the level of the underlying blockchain but at the application layer, where smart contracts, decentralized applications (dApps), and protocol integrations often contain exploitable vulnerabilities. These weaknesses usually stem from coding errors, which can occur for a panoply of reasons –including system design flaws or an inability to anticipate and stress-test for every possible extreme scenario.[1200]

These risks are amplified by the fact that crypto-assets can be drained instantaneously and irreversibly, and by the ease with which malicious actors can create, promote, and distribute fraudulent or scam tokens.[1201] Importantly, several high-profile protocols have been exploited despite undergoing multiple audits, underscoring both the limits of current audit practices and the inherent challenges of securing large-scale smart-contract environments.[1202]

Application-layer attacks fall into several major categories, including protocol exploits, flash-loan attacks, bridge hacks, software backdoors, and undocumented functions.

5.3.1.A. Protocol Exploits

Protocol exploits occur when attackers take advantage of vulnerabilities in smart-contract code or exploit weaknesses in a protocol's economic design or oracle mechanisms.[1203] Attackers may leverage poorly constructed incentive structures, manipulate market prices (e.g., via oracle manipulation), or exploit asymmetries in how liquidity pools or lending mechanisms operate. These attacks often occur without violating the protocol's explicit rules, yet they nonetheless result in substantial losses for users or for the protocol itself. Protocol exploits, whether stemming from logic errors or oracle manipulation, remain among the most common and costly forms of DeFi attacks.

1198 Zack Voell, *Ethereum Classic Hit by Third 51% Attack in a Month*, CoinDesk (Aug. 29, 2020), https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month

1199 *How Much Would it Cost to 51% Attack Bitcoin?*, Braiins (Nov. 1, 2021), https://braiins.com/blog/how-much-would-it-cost-to-51-attack-bitcoin. However, there were other types of incidents on Bitcoin. For instance, in 2010, a bug briefly produced 184 billion bitcoins before being patched. See Alex Min, *How to Hack Bitcoin: A History of Bitcoin Hacks,* BitcoinBriefly (Dec. 5, 2020), https://bitcoinbriefly.com/hacking-bitcoin-history-of-bitcoin-hacks/.

1200 *See Understanding Crypto Hacks and Exploits*, DLNews (Sept. 28, 2023), https://www.dlnews.com/articles/llama-u/understanding-crypto-hacks-and-exploits-with-defillama/.

1201 *See The Importance of Blockchain Security and How to Prevent Threats Before They Strike*, Chainalysis (Apr. 30, 2025), https://www.chainalysis.com/blog/blockchain-security/.

1202 Ciaran Lyons, *Euler Finance Hacked Despite 10 Audits in 2 Years, Says CEO,* Cointelegraph (Mar. 17, 2023), https://cointelegraph.com/news/euler-finance-hacked-despite-10-audits-in-2-years-says-ceo.

1203 U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses, supra* note 1022, 26-27.

1. Code-Execution Vulnerabilities

Code-related attacks arise from bugs in the smart-contract code itself. The most famous example is The DAO exploit *(See section 6.2.1.A.)*, in which the attacker exploited a flaw in the smart contract's withdrawal system. The attacker used a malicious program that could trigger repeated withdrawals before the smart contract was able to update the attacker's account balance. This loophole allowed the attacker to withdraw the same funds multiple times in a single transaction. Approximately $60 million worth of ETH was drained over several hours and transferred into a newly created, attacker-controlled smart contract, where it remained inaccessible for weeks due to the contract's time-lock mechanism.

Other major incidents have similarly resulted from technical flaws in the underlying code or system architecture. For example, the Poly Network exploit (2021) remains one of the largest in DeFi history, because of the scale of the funds involved and the attack's unconventional resolution. It underscored the urgent need for rigorous smart-contract audits and more robust security practices across the DeFi sector.

FIGURE 42.

Poly Network (2021)

On August 10, 2021, Poly Network, a decentralized finance (DeFi) protocol facilitating cross-chain asset transfers, suffered a major security breach.[1204] An attacker exploited a vulnerability in the platform's smart contracts, enabling the unauthorized transfer of more than $600 million worth of cryptocurrencies across Ethereum, Binance Smart Chain, and Polygon networks.[1205] The hack prompted an immediate and coordinated response from the broader cryptocurrency ecosystem.[1206] In an unexpected development, the individual responsible for the attack —later referring to themselves as "Mr. White Hat"— began communicating directly with Poly Network through on-chain messages embedded in Ethereum transactions.[1207] The attacker claimed that the exploit was conducted "for fun" and as a means to expose critical security flaws in the protocol. Over the following days, the attacker voluntarily began returning the stolen assets.

By August 12, 2021, the hacker had returned the vast majority of the funds to Poly Network. For the final tranche, valued at $235 million, the hacker transferred the funds to a "shared multisig" Ethereum account that required keys from both Poly Network and the hacker to authorize any movement. According to the hacker, Poly Network offered a $500,000 "bug bounty" in recognition of the returned funds and the hacker's stated motivation: to highlight blockchain vulnerabilities, not cause lasting harm. The hacker initially declined this offer. Then he created an account to solicit an ex-post "bug bounty" via donations from those who support the hacker's "decision" to return the money. Poly Network reportedly transferred approximately $525,000 in Ether to the account. About two weeks after the initial hack, the hacker shared the key required to move the remaining funds in the shared wallet. The hacker also sent the entire contents of the donation account back to Poly Network and asked that it be distributed among the "survivors," the victims of his hack.

1204 *See* Gertrude Chavez-Dreyfuss et al., *How Hackers Stole $613 Million in Crypto Tokens From Poly Network*, Reuters (Aug. 12, 2021) https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/.

1205 *Id.*; see *also $600 Million in Crypto Stolen and Returned in 24 Hours*, Elliptic Blog (Aug. 12, 2021), https://www.elliptic.co/blog/the-poly-network-hack-600-million-in-crypto-stolen-and-returned-in-24-hours.

1206 Elliptic *supra* note 1205; *see also Poly Network Attacker Returning Funds After Pulling Off Biggest DeFi Theft Ever*, Chainalysis (Aug. 12, 2021), https://www.chainalysis.com/blog/poly-network-hack-august-2021/.

1207 Elliptic *supra* note 1205.

2. Oracle-Manipulation Vulnerabilities

Other exploits arise from flaws in a protocol's economic assumptions. These attacks often involve distorting price oracles or liquidity conditions. In such cases, the attacker technically operates "within the rules" of the protocol but exploits unintended weaknesses in its design. A widely cited example is the Mango Markets exploit (2022), where the attacker artificially pumped up the market price of the MNGO token (On the legal consequences, *See section 6.2.2.*)[1208] This incident shows that oracles can introduce points of failure, not because the oracle malfunctions but because they may rely on data from markets that are easy to manipulate.[1209]

FIGURE 43.

The Mango Markets price manipulation (2022)

The Mango Markets DeFi protocol on Solana suffered a major manipulation event in October 2022, costing approximately $116 million.[1210] According to the U.S. Securities and Exchange Commission's complaint, the attacker, who later identified himself as Avraham Eisenberg, manipulated the price of the MNGO token by executing large spot trades on external exchanges whose prices were referenced by Mango Markets' oracle. Exploiting the low liquidity of the MNGO market, he carried out a sophisticated price manipulation scheme.

Eisenberg created two accounts on Mango Markets, with approximately 5 million USDC in each.[1211] He then acquired millions of MNGO tokens on external exchanges and established "perpetual futures" —with one of his accounts holding a long position and the other holding a short position in MNGO.[1212] The Mango Markets' system relied on price feeds from external exchanges (via oracles) to determine its internal pricing.[1213]

Since Eisenberg's transactions were substantial, they drove up the external price of MNGO, which increased the value of his long "perpetual futures" by 1,300%. Eisenberg then used that inflated value as collateral to borrow and withdraw assets from Mango. He withdrew much more than he would have been able to borrow otherwise —a total of approximately $116 million worth of crypto.[1214] After the withdrawal, the price of MNGO collapsed back to near its original levels, leaving Mango Markets at a deficit.

1208 Chainalysis Team, *Oracle Manipulation Attacks Rising: A Unique Concern for DeFi,* Chainalysis (2023), https://www.chainalysis.com/blog/oracle-manipulation-attacks-rising/ (last visited Jan. 15, 2026).

1209 Amirmohammad Pasdar, Young Choon Lee & Zhongli Dong, *Connect API with Blockchain: A survey on Blockchain Oracle Implementation*, 55 ACM Computing Surveys 2-4 (2023), https://dl.acm.org/doi/10.1145/3567582.

1210 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Avraham Eisenberg with Manipulating Mango Markets' "Governance Token" to Steal $116 Million of Crypto Assets* (Jan. 20, 2023), https://www.sec.gov/newsroom/press-releases/2023-13; Chainalysis Team, *Oracle Manipulation Attacks Are Rising, Creating a Unique Concern for DeFi*, Chainalysis (Mar. 7, 2023), https://www.chainalysis.com/blog/oracle-manipulation-attacks-rising/.

1211 Complaint at para 72, *U.S. Sec. & Exch. Comm'n v. Eisenberg*, No. 1:23-cv-00503-LGS (S.D.N.Y. Jan. 20, 2023), ECF No. 1 https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-13.pdf [hereinafter SEC Eisenberg Complaint]. USDC is a cryptocurrency with value pegged to the U.S. dollar. Therefore, one can assume that both Eisenberg's accounts each had approximately $5 million worth of coins.

1212 *Id.* at 6. "Perpetual futures" is a term in the blockchain community that refers to transactions that operate similar to real-world future contracts, in which "one party agrees to pay another party a return based on the performance of another asset." A long position contract profits when the price of the underlying asset goes up; a short position contract profits when it goes down. Here, since Eisenberg entered into transactions with himself and they were "offsetting," meaning they were mutually exclusive, barring any other changes he would have no true market risk resulting here from fluctuations in the underlying asset, the MNGO token.

1213 *Id.* at 14 (Mango oracle was "a computer program that calculated the relative value of crypto asset pairings by looking at the exchange rate of those crypto assets on three other crypto asset trading platforms").

1214 *Id.* at 15.

Other historically significant incidents include Harvest Finance and Cheese Bank in 2020. Cheese Bank,[1215] a decentralized autonomous banking protocol on Ethereum, suffered a major exploit resulting in the loss of approximately $3.3 million in stablecoins (USDC, USDT, and DAI). The attacker exploited a weakness in the protocol's price-measurement mechanism, which relied on Uniswap as its oracle. By executing a flash-loan-enabled price manipulation on Uniswap, the attacker artificially distorted the collateral value and was able to carry out a sequence of illegitimate borrowing transactions from Cheese Bank. In the case of Harvest Finance,[1216] the attacker manipulated the prices of stablecoins within the smart contracts that the Harvest protocol relied on. By pushing these prices to artificially favorable levels, the attacker was able to drain the protocol's liquidity pools and steal over $24 million.

5.3.1.B. Flash Loan Attacks

Flash loans are a DeFi innovation that allows users to borrow large amounts of cryptocurrency instantly and without collateral, provided the loan is repaid within the same blockchain transaction.[1217] Flash loan attacks involve a malicious actor exploiting a protocol by taking out an uncollateralized flash loan, typically a large sum of cryptocurrency.[1218] The attacker then uses the borrowed funds to manipulate market conditions or exploit specific vulnerabilities in the targeted protocol.

In a typical flash-loan attack, the attacker uses the borrowed funds to distort collateral values, manipulate price oracles, or induce extreme slippage in liquidity pools. Once the exploit has generated a profit or drained assets from the protocol, the attacker repays the flash loan within the same transaction, leaving no initial capital at risk. Since the entire process occurs atomically (within one transaction), if any step fails, the transaction is reversed, making it a low-risk, high-reward method for attackers.

One of the first major flash-loan exploits occurred in 2020 against the bZx lending protocol.[1219] Through its newly introduced margin-trading platform Fulcrum, an attacker used a flash loan to create a large, under-collateralized short position by exploiting a flaw in bZx's smart-contract logic. The attacker ultimately profited approximately $370,000, while bZx incurred losses of roughly $620,000. This attack was followed by a series of similar incidents across the DeFi ecosystem, illustrating both the power and the dangers of flash-loan-enabled manipulation.

5.3.1.C. Bridge Hacks

Bridge hacks target cross-chain bridges —protocols that enable the transfer of digital assets between different blockchains, for example between Ethereum and Binance Smart Chain.[1220] These bridges are particularly vulnerable as they hold large reserves of tokens, making them especially attractive targets.[1221] Over the past several years, bridges have accounted for some of the largest and most damaging exploits in the crypto ecosystem.

- **Wormhole bridge**. In February 2022, attackers exploited a vulnerability in the Wormhole bridge, which connects the Solana and Ethereum

1215 *Strengthening DeFi Security: A Static Analysis Approach to Flash Loan Vulnerabilities*, arXiv, https://arxiv.org/html/2411.01230v1

1216 *DeFi Project Harvest Exploited for Over $24 Million,* CoinGeek (Nov. 25, 2020), https://coingeek.com/defi-project-harvest-exploited-for-over-24-million/

1217 *What is a Flash Loan?*, OSL (Feb. 12, 2025), https://www.osl.com/hk-en/academy/article/what-is-a-flash-loan?utm_source.

1218 *What is a Flash Loan Attack? How It Works & Examples,* Twingate Blog (Aug. 1, 2024), https://www.twingate.com/blog/glossary/flash%20loan%20attack.

1219 Eric Rafaloff, *Flash Loan Attacks: A Case Study*, Aon (Oct. 13, 2023), https://www.aon.com/en/insights/cyber-labs/flash-loan-attacks-a-case-study.

1220 *Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk*, Chainalysis (Aug. 2, 2022), https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/.

1221 *See* Guneet Kaur, *The Risks of Using Cross-Chain Bridges*, Cointelegraph (Apr. 3, 2024), https://cointelegraph.com/learn/articles/risks-of-using-cross-chain-bridges.

blockchains.[1222] By bypassing signature verification in the contract responsible for validating cross-chain messages,[1223] the attacker was able to mint 120,000 wrapped Ether (wETH) on Solana without corresponding deposits on Ethereum —a theft of approximately $324 million.[1224] The incident exposed significant deficiencies in the bridge's validation logic and highlighted the systemic risks inherent in flawed interoperability protocols.

- **Harmony Horizon bridge**. In June 2022, attackers breached the Horizon bridge, which supported transfers across Ethereum, Binance Smart Chain, and Harmony's native network.[1225] The attackers exploited compromised private keys to make unauthorized withdrawals totaling roughly $100 million. Subsequent investigations attributed the attack to the Lazarus Group, a cybercriminal organization linked to the North Korean government.[1226] The incident demonstrated the risks associated with inadequate key management and the geopolitical dimensions of certain cyberattacks on blockchain infrastructure.
- **Nomad bridge**. In August 2022, a critical misconfiguration in the Nomad bridge enabled an attacker to drain an estimated $190 million.[1227] This exploit was particularly notable because it was not confined to a single actor.[1228] After the initial vulnerability was exposed, hundreds of users replicated the original malicious transaction by replacing the recipient address with their own. This effectively turned the incident into a decentralized looting of the protocol, facilitated by the deterministic and predictable nature of the exploit.
- **Ronin bridge**. The largest bridge hack to date is the hack of Axie Infinity's bridge Ronin, in 2022. The attacker compromised bridge funds by using hacked private keys to gain control of a majority of bridge validators. The attacker then forged fake withdrawals and drained over $600 million. The hack punished the Axie token price and left users of the bridge facing an uncertain recovery.[1229]

Several additional bridge hacks occurred in 2023,[1230] further illustrating the persistent weaknesses in bridge design and operation. To date, there are no industry-wide standards governing bridge security, validator management, or operational resilience. As a result, cross-chain bridges continue to present significant vulnerabilities, undermining confidence in interoperability and posing a major systemic risk to the broader blockchain ecosystem.

5.3.1.D. Software Backdoors or Undocumented Functions

Software backdoors create serious vulnerabilities in

1222 *Lessons from the Wormhole Exploit: Smart Contract Vulnerabilities Introduce Risk; Blockchains' Transparency Makes It Hard for Bad Actors to Cash Out*, Chainalysis (Feb. 3, 2022), https://www.chainalysis.com/blog/wormhole-hack-february-2022/.

1223 *The Dark Side of DeFi: Cross-Chain Bridge Hacks,* Quanstamp Labs (May 11, 2022), https://quantstamp.com/blog/the-dark-side-of-defi-cross-chain-bridge-hacks.

1224 *Solana Wormhole Compromise, 120K Wrapped ETH Stolen,* TRM Blog (Feb. 3, 2022), https://www.trmlabs.com/resources/blog/solana-wormhole-compromise-120k-stolen-eth

1225 Ryan Browne, *$100 Million Worth of Crypto Has Been Stolen in Another Major Hack*, CNBC (June 24, 2022), https://www.cnbc.com/2022/06/24/hackers-steal-100-million-in-crypto-from-harmonys-horizon-bridge.html

1226 *See The Harmony Horizon Bridge Hack*, Elliptic, https://www.elliptic.co/resources/harmony-horizon-bridge-hack (last visited Jan. 15, 2026); Press Release, Fed. Bureau of Investigation, *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft*, (Jan. 23, 2023), https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft

1227 Aaron Gregg, *Crypto 'Bridge' Nomad Offers 10 Percent Bounty in $190 Million Hack*, Wash. Post (Aug. 5, 2022), https://www.washingtonpost.com/business/2022/08/05/nomad-crypto-bounty/.

1228 *See* Osato Avan-Nomayo, *Hacker Behind $190M DeFi Exploit From 2022 Arrested in Israel*, DLNews (May 5, 2025), https://www.dlnews.com/articles/defi/hacker-behind-190m-nomad-bridge-exploit-arrested-in-israel/.

1229 *Behind Axie Infinity's $625M Hack,* Coinbase Bytes (Apr. 7, 2022), https://www.coinbase.com/bytes/archive/axie-infinity-625-million-dollar-hack-explained.

1230 Nikita Belenkov et al., *SoK: A Review of Cross-Chain Bridge Hacks in 2023* (Dec. 19, 2023), arXiv https://arxiv.org/html/2501.03423v1.

blockchain-based systems because they may allow unauthorized or unilateral access to user funds. In some cases, developers intentionally insert harmful or deceptive code into the smart contracts that support decentralized applications. These hidden mechanisms may take the form of backdoors or undocumented privileged functions that give developers disproportionate control over user assets or the protocol's governance. For example, such code may enable the developer to modify essential parameters, withdraw user deposits, or trigger a self-destruct sequence after certain conditions are met.

These elements are often embedded within otherwise functional smart contracts, allowing the project to appear legitimate and attract substantial deposits. Once sufficient value is locked in, the developers may exploit these hidden mechanisms to extract funds and abandon the project.

FIGURE 44.

Munchables (2024)

The Munchables exploit occurred in March 2024 and was carried out by a developer who had legitimate access to the project's codebase.[1231] The developer manipulated a smart contract to transfer stored user funds and steal approximately $62.5 million in cryptocurrency. Remarkably, the attacker, who was allegedly linked to North Korea, later returned the entire sum voluntarily, without imposing any conditions or demanding ransom.[1232] The Munchables incident thus stands as a rare case in which a major insider-led exploit resulted in the full restitution of stolen assets.

5.3.2. Attacks on Centralized Intermediaries

In addition to application-layer vulnerabilities, a substantial share of losses in the crypto asset ecosystem stems from attacks on centralized intermediaries, particularly cryptocurrency exchanges that hold customer assets in custodial wallets. These platforms constitute highly attractive targets: Compromising a single system can provide access to large concentrations of digital assets. Unlike attacks on decentralized protocols, which typically require exploiting smart-contract flaws, attacks on centralized exchanges generally succeed through operational failures, such as the compromise of private keys, inadequate internal controls, or poor cybersecurity practices. One of the most notorious examples is the Mt. Gox hack *(See Figure 45)*, widely regarded as a defining incident in the history of cryptocurrency security failures.

1231 Shaurya Malwa, *Munchables Exploited for $62M, North Korea-Linked Exploiter Returns Private Keys to Web3 Firm*, CoinDesk (Mar. 27, 2024), https://www.coindesk.com/tech/2024/03/27/munchables-exploited-for-62m-ether-linked-to-rogue-north-korean-team-member.

1232 Arjit Sarkar, *Munchables Hacker Returns $62.8M Ether Without Ransom*, CoinTelegraph (Mar. 27, 2024), https://cointelegraph.com/news/munchables-hacker-returns-ether-without-ransom.

FIGURE 45.

Mt. Gox (2014)

Mt. Gox was a centralized Bitcoin exchange based in Tokyo which, at its peak in 2013, processed roughly 70% of global Bitcoin transactions.[1233] The collapse began in February 2014, when Mt. Gox abruptly suspended trading, took its website offline, and filed for bankruptcy. The company announced that it had lost access to approximately 850,000 bitcoins —valued at around $450 million at the time— of which 750,000 belonged to customers.[1234]

Mt. Gox initially attributed the losses to a flaw in the Bitcoin protocol known as transaction malleability,[1235] which allows modification of transaction identifiers after a withdrawal request is submitted.[1236] However, a subsequent study showed that transaction malleability could explain only a portion of the missing funds: Only 302,000 bitcoins were ever involved in malleability-related attacks.[1237]

Later investigations revealed a far more troubling reality: Mt. Gox had been subject to years-long theft, enabled by extremely weak internal controls, outdated wallet-management procedures, and the absence of proper accounting.[1238] The exchange failed to detect ongoing unauthorized withdrawals for an extended period. Roughly 200,000 bitcoins were later recovered. A creditor compensation framework was ultimately established in 2024 to distribute recovered assets to creditors, nearly a decade after the initial incident.[1239] Mt. Gox represents the first large-scale exchange hack.

Other attacks against centralized intermediaries took place over the past few years:

- **Binance**. In May 2019, Binance suffered a major security breach, when attackers targeted one of its "hot wallets," containing about 2% of Binance's total cryptocurrency assets.[1240] A hot wallet is a cryptocurrency wallet connected to the internet for operational purposes, making it more vulnerable than "cold storage" wallets that are kept offline. Attackers obtained a large volume of Application Programming Interface (API) keys, two-factor authentication (2FA) credentials, and other user information that allowed them to withdraw 7,000 BTC —worth about $40 million at the time— in a single transaction. Binance absorbed the losses through its Secure Asset Fund for Users (SAFU), and no customers ultimately bore financial harm.

1233 Guneet Kaur, *The Mt. Gox Bitcoin Heist, and Why It Still Matters*, Cointelegraph (June 26, 2024), https://cointelegraph.com/learn/articles/the-mt-gox-bitcoin-heist.

1234 Chris O'Brien, *Mt. Gox Files for Bankruptcy as 850,000 Bitcoins Go Missing,* L.A. Times (Feb. 28, 2014), https://www.latimes.com/business/technology/la-fi-tn-mt-gox-bankruptcy-bitcoins-20140228-story.html.

1235 Christian Decker et al., *Bitcoin Transaction Malleability and MtGox*, in Computer Security – ESORICS 2014, 314, (Marek Kutyłowski et al., eds., 2014), https://web.cs.miami.edu/home/burt/learning/csc597.251/docs/978-3-319-11212-1_18.pdf.

1236 *Id.* at 5.

1237 *Id.* at 325.

1238 Kim Nilsson, *The Missing MTGox Bitcoins*, WizSec Blog (Apr. 19, 2015), https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.

1239 *The Story of Mt. Gox: Explained*, Trust Blog (July 17, 2024), https://trustwallet.com/blog/mt-gox-explained.

1240 *Binance Exchange Hackers Steal Bitcoins Worth $41m,* BBC News (May 8, 2019), https://www.bbc.com/news/technology-48199375.

- **DMM Bitcoin**. In May 2024, DMM Bitcoin, a centralized Japanese cryptocurrency exchange, experienced a major hack, resulting in a loss of $305 million. While the exchange has not disclosed the root cause of the breach, the attack likely stemmed from the compromise of a private key, enabling the attacker to initiate unauthorized transfers.[1241]
- **Bybit**. In February 2025, attackers carried out the largest cryptocurrency theft ever recorded, targeting Bybit, one of the world's largest cryptocurrency exchanges.[1242] The attack was attributed by the FBI to the Lazarus Group, a state-sponsored hacking collective linked to the Democratic People's Republic of Korea (DPRK).[1243] Rather than directly breaching Bybit's own systems, the attackers injected malicious code into the web interface of a third-party multisignature wallet platform used by Bybit. This caused Bybit to unknowingly approve a malicious transaction that appeared legitimate, resulting in the unauthorized transfer of funds from Bybit's multisignature cold-wallet system. The attack resulted in losses estimated at approximately $1.5 billion in Ethereum. Despite the unprecedented scale of the theft, Bybit continued operating and stated that customer funds were covered by drawing on reserves and liquidity-management mechanisms.[1244]
- **Upbit**. In November 2025, Upbit, South Korea's largest cryptocurrency exchange operated by Dunamu, suffered a breach resulting in the unauthorized transfer of approximately $30 million worth of Solana-affiliated digital assets to an unidentified wallet.[1245] South Korean authorities subsequently launched an on-site investigation, with government and business sources indicating that the Lazarus Group (the same DPRK-linked hacking collective responsible for the Bybit attack) was suspected of being behind the incident. Upbit stated that it would cover the full amount of the losses with its own holdings and announced a series of remedial measures, including the transfer of all assets to cold-wallet storage, efforts to freeze the relevant on-chain transactions, and a comprehensive security review of its deposit and withdrawal systems.[1246]

5.3.3. Individual User Targeting

Individual users remain a primary point of failure in blockchain systems, as attackers increasingly exploit human behavior rather than technical vulnerabilities to gain control over digital assets. Many of the most effective intrusions ultimately depend on deceiving individual users into taking actions that compromise their own security: whether by revealing private keys, signing malicious transactions, or executing code that installs malware on their devices.

1241 *2024 Exploits Recap: Top 10 Most Exploited DeFi Vulnerabilities and How to Prevent Them,* Three Sigma (Jan. 1, 2025), https://threesigma.xyz/blog/exploit/2024-defi-exploits-top-vulnerabilities. U.S. authorities, including the FBI and the Department of Defense Cyber Crime Center, publicly attributed the DMM Bitcoin hack to North Korea's Lazarus Group; FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com (Dec. 24, 2024), https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom.

1242 *The largest theft in history - following the money trail from the Bybit Hack*, Elliptic Research (Feb. 23, 2025), https://www.elliptic.co/blog/bybit-hack-largest-in-history.

1243 Press Release, Fed. Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack* (Feb. 26, 2025), https://www.fbi.gov/investigate/cyber/alerts/2025/north-korea-responsible-for-1-5-billion-bybit-hack

1244 Rosalia Mazza, *Bybit's $1.4 Billion Hack: The Race to Recover Stolen Crypto from Lazarus Group,* Fintech Weekly (Mar. 20, 2025), https://www.fintechweekly.com/magazine/articles/bybit-ceo-ben-zhou-says-most-funds-are-still-traceable.

1245 James Field, *N. Korea's Lazarus Group Suspected to Be Behind $30M Upbit Hack*, CoinGeek (Dec. 4, 2025), https://coingeek.com/north-korea-lazarus-group-suspected-to-be-behind-30m-upbit-hack/.

1246 *Id*.

5.3.3.A. Private Key Loss

Attackers use various methods to obtain the private keys that control access to cryptocurrency. Fraudulent emails or websites that trick users into revealing their private keys are extremely common. Attackers also try phishing campaigns that mimic legitimate services, key-logging malware that records keystrokes, and tactics that manipulate victims into revealing sensitive information. Malicious applications, including fraudulent or compromised wallet applications, can secretly transmit private keys to attackers.[1247]

Disputes about private-key loss arise in litigation. In the Tulip Trading case *(See section 6.3.2.A.)*, Craig Wright asserted that he had been the victim of a computer hack that deprived him of access to private keys controlling bitcoin then valued at approximately £3 billion (about $4 billion). Courts have not accepted these claims as proven, but the case highlights the challenges associated with alleged private-key theft.

Another well-known incident occurred in January 2023, when entrepreneur Kevin Rose lost roughly $1 million worth of NFTs after signing a malicious transaction generated on a fraudulent website.[1248] Importantly, Rose's private key was not "stolen;" rather, the attacker induced him to sign a valid on-chain authorization. The incident illustrates that even informed users who safeguard private keys may unintentionally authorize malicious transactions.

5.3.3.B. Wrench Attack

A "wrench attack" is an informal term used to describe the use of physical coercion, threats, or violence to compel an individual to surrender sensitive information, such as passwords, private cryptographic keys, or seed phrases.[1249] Unlike cyberattacks that exploit technical vulnerabilities in software or networks, a wrench attack targets the person directly. Because crypto can be self-custodied and transfers are irreversible, obtaining a victim's credentials or forcing them to initiate a transaction can be far easier than breaking encryption. Breaking strong encryptions could take years or prove computationally infeasible, while attackers can simply physically threaten and coerce a wealthy victim into disclosing their credentials or transferring their funds directly. In short, a wrench attack highlights the human vulnerability in otherwise secure cryptographic systems: what security experts often call the "human layer" of risk.

Several high-profile incidents reported in 2024 and 2025 illustrate the severity of this risk, including kidnappings, home invasions, and violent extortion attempts directed at individuals known to hold substantial crypto-assets.[1250] These cases, reported in jurisdictions ranging from France to the United States, have prompted many users to adopt more resilient security architectures. In response, users are resorting to more secure solutions, such as multi-signature (multisig) wallets or distributed key management schemes, to make it impossible for a single individual to access funds without the cooperation of others. Other users store keys in multiple locations, use secure hardware devices, or employ trusted third-party custodians.

1247 ESET Research, *Crypto Malware in Patched Wallets Targeting Android and iOS Devices,* (Mar. 24, 2022), https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/.

1248 Andrew Hayward, *Proof Founder Kevin Rose Just Had Over $1M Worth of NFTs Stolen From His Wallet*, Decrypt (Jan. 25, 2023), https://decrypt.co/119981/proof-founder-kevin-rose-nfts-stolen-wallet.

1249 Alan Suderman, *Why 'Wrench Attacks' on Wealthy Crypto Holders Are on the Rise*, APNews (May 28, 2025), https://apnews.com/article/crypto-bitcoin-kidnapping-wrench-attack-ddc7263c25ba590f85648e1682576971. The term itself originates with an online comic that mocked how easily high-tech security can be undone by hitting someone with a wrench until they give up their passwords.

1250 Sam Schechner, Robert McMillan & Angus Berwick, *Severed Fingers and 'Wrench Attacks' Rattle the Crypto Elite*, Wall St. J. (May 17, 2025), https://www.wsj.com/finance/currencies/crypto-industry-robberies-attacks-32c2867a?mod=hp_lead_pos7.

5.4. ENVIRONMENTAL IMPACT

Concerns about the environmental impact of digital technologies —particularly their energy consumption— extend far beyond blockchain. However, these issues warrant specific attention in the blockchain context because proof-of-work protocols have sparked extensive debate and are frequently criticized for their high energy consumption.

5.4.1. Electricity Consumption

Debates about the environmental impact of blockchain technologies have centered largely on the electricity consumption associated with proof-of-work[1251] consensus mechanisms *(See section 2.3.1.)* and the specialized hardware —application-specific integrated circuits (ASICs)[1252]— used to secure these networks.

5.4.1.A. Level of Electricity Usage

Electricity usage varies significantly across crypto-assets and depends primarily on the underlying consensus mechanism, principally proof of work or proof of stake. Proof of work requires miners to solve cryptographic puzzles by repeatedly hashing blocks of transactions. This process is intentionally computationally intensive: It requires trillions of guesses within mere minutes, with vast amounts of electricity needed to power those efforts. Miners who solve these puzzles are rewarded with new coins.[1253] In this context, the energy debate focuses primarily on Bitcoin, which remains the largest consumer by far of electricity. As of 2024, Bitcoin's electricity consumption was estimated to be 120 trillion to 170 trillion watt-hours (terawatt hours or TWh) per year,[1254] compared to total worldwide electricity consumption, which was estimated to be about 30,000 TWh for 2024.[1255] As of January 2026, Bitcoin's annual electricity consumption is estimated to range between 160 and 175 TWh,[1256] a significant increase from 2024 levels that now places its demand above the national electricity use of countries like Switzerland.[1257]

Ethereum relied on proof of work until 2022, and its annual electricity demand was estimated at 21.42 terawatt-hours.[1258] In September 2022, Ethereum changed its consensus mechanism from one of proof of work to proof of stake, an event the industry called "The Merge" *(See section 2.3.2.B.)*. After adopting proof of stake, Ethereum's energy demand dropped by more than 99%[1259] —from 21.42 *trillion* watt-hours (terawatt-hours or TWh) to about 5.36 *billion* watt-hours (gigawatt-hours or GWh) per year. The drop put Ethereum's consumption at slightly

1251 Nathan Reiff, *What is the Environmental Impact of Cryptocurrency?*, INVESTOPEDIA (Aug. 2024), https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/; Scott Nevil, *Understanding Proof of Work (PoW) in Blockchain: Key Mechanism Explained*, (Aug. 23, 2025), INVESTOPEDIA, https://www.investopedia.com/terms/p/proof-work.asp (last accessed Dec 28, 2025).

1252 An ASIC is a type of specialized hardware, a computer chip, that is designed and optimized for completing a specific task. In this case, this is a custom-built mining ASIC that has been tailored for one purpose only: mining cryptocurrency. *See* The Investopedia Team, *Discover Consensus Mechanisms: Blockchain and Cryptocurrency Essentials,* INVESTOPEDIA (Aug. 20, 2025), https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp; Carla Tardi, *What is an ASIC Miner? How it Works and Why It Matters,* INVESTOPEDIA, (Sep 12, 2025), https://www.investopedia.com/terms/a/asic.asp (last accessed Dec 28, 2025).

1253 Alireza Jafari, Taher Niknam, Ali Taghavi, Sadreddin Saleh, *Energy, Economic and Environmental Impacts of Cryptocurrency Mining: A Review of Sustainable Integration Pathways in Power Systems,* 29 Energy Conversion and Management: X art. 101413, (2026), https://doi.org/10.1016/j.ecmx.2025.101413; *see also*: Mohamd Laimon, , Almadadha Rula, and Steven Goh, *Energy Consumption of Crypto Mining: Consequences and Sustainable Solutions Using Systems Thinking and System Dynamics Analysis*, 17 Sustainability, 3522 (2025). https://doi.org/10.3390/su17083522.

1254 CAMBRIDGE CENTER FOR ALTERNATIVE FINANCE, *Cambridge Bitcoin Electricity Consumption Index (CBECI)* https://ccaf.io/cbnsi/cbeci (last visited Jan. 15, 2026).

1255Euan Graham, Nicolas Fulghum, and Katye Altieri, *Global Electricity Review 2025,* EMBER, (Apr. 8, 2025), https://ember-energy.org/latest-insights/global-electricity-review-2025/2024-in-review/

1256 CAMBRIDGE CENTER FOR ALTERNATIVE FINANCE, *supra* note 1254.

1257 Bitcoin Energy Consumption Index, DIGICONOMIST, https://digiconomist.net/bitcoin-energy-consumption (last visited Jan. 15, 2026).

1258 Ethereum relied on proof of work until 2022, and its annual electricity demand was estimated at 21.42 terawatt-hours. CAMBRIDGE CTR. FOR ALTERNATIVE FIN., *Cambridge Blockchain Network Sustainability Index: Ethereum 1.0*, https://ccaf.io/cbnsi/ethereum/1 (last visited Jan. 15, 2026).

1259 Katie Clinebell, *How Green is Ethereum?* INVESTOPEDIA, (May 27, 2024), https://www.investopedia.com/how-green-is-ethereum-2-0-6666266.

below the annual electricity demand of the Eiffel Tower or a large business building.[1260] There have been calls for Bitcoin to change its consensus mechanism to proof of stake,[1261] as Greenpeace USA[1262] and other environmental groups have advocated against the continued use of proof of work.[1263] Such major changes would require the overwhelming support of Bitcoin's entire stakeholder base[1264] but, as of yet, such broad consensus for this significant change seems unlikely.[1265]

In this context, Bitcoin advocates have highlighted various arguments to nuance the critique related to the high electricity consumption by Bitcoin. They note that estimates of Bitcoin's annual electricity use are significantly *less* than that of the global banking industry's annual demand of about 263.72 TWh.[1266] They also point to Bitcoin's relative flexibility compared with other industries and technologies using large amounts of energy. Bitcoin mining can be turned off with relative ease and speed, which makes it ideal for grid stabilization. In Texas, for instance, the state's electric grid operator, the Electric Reliability Council of Texas (ERCOT), created a large flexible load curtailment program. The program would pay large Bitcoin miners to shut down their operations when the demand for electricity exceeds the capacity of the grid.[1267] The program received praise during Texas' winter storm Elliott in 2022. On December 24, 2022, in the midst of Elliott, ERCOT paid Bitcoin miners to curtail their use to ease the stress on grids. Texas Bitcoin miners were able to quickly curtail their use by 91.5%.[1268] The program has come under pressure, however. In August 2023, during a record-breaking heat wave, ERCOT paid Riot Platforms, a large Bitcoin mining company, $31.7 million in energy credits to curtail its energy use. To many, this amount was excessive —it was roughly $22 million more than the amount Bitcoin Riot Platforms mined that same month.[1269]

5.4.1.B. Policy Initiatives to Curb Electricity Consumption

A growing number of jurisdictions have taken note of the substantial energy consumption associated with proof-of-work consensus mechanisms and have adopted measures aimed at regulating or constraining domestic cryptocurrency-mining activities.

China provides the most prominent example of large-scale intervention. At its peak in 2021, an estimated 60-70% of global Bitcoin mining capacity was located

1260 Cambridge Ctr. for Alternative Fin., *Cambridge Blockchain Network Sustainability Index: Ethereum Comparisons*, https://ccaf.io/cbnsi/ethereum/comparisons, (last visited Jan. 15, 2026)

1261 Amy Castor, *Ethereum moved to proof of stake. Why can't Bitcoin*? MIT TECHNOLOGY REVIEW, (Feb. 28, 2023), https://www.technologyreview.com/2023/02/28/1069190/ethereum-moved-to-proof-of-stake-why-cant-bitcoin/.

1262 Tyler Kruse, *Climate Groups to Bitcoin: Cut the Pollution, and the B.S.*, GREENPEACE USA, (Sep. 15, 2022) https://www.greenpeace.org/usa/climate-groups-to-bitcoin-cut-the-pollution-and-the-b-s/.

1263 Eliza Gkritsi, *Environmental Groups Call on US Government to Implement Stringent Bitcoin Mining Regulations,* COINDESK (April 9, 2024), https://www.coindesk.com/policy/2022/05/10/environmental-groups-call-on-us-government-to-implement-stringent-bitcoin-mining-regulations.

1264 There is no foundation or core group of developers that can, at their own discretion, implement this hard fork. Such a major change would necessarily require the majority of users and developers to agree to follow. Scott Sullivan, *A Bitcoiner's Guide to Proof of Stake*, Bitcoin Mag. (Sep. 26, 2022), https://bitcoinmagazine.com/technical/bitcoiners-guide-to-proof-of-stake.

1265 Castor, *supra* note 1261.

1266 Namcios, *Research: Bitcoin Consumes Less Than Half the Energy of the Banking or Gold Industries*, NASDAQ, (May, 17, 2021), https://www.nasdaq.com/articles/research:-bitcoin-consumes-less-than-half-the-energy-of-the-banking-or-gold-industries

1267 Xinyi Luo, *Bitcoin Miners Offered Way to Cut Texas Electricity Usage to Help the Grid*, COINDESK, (May 8, 2023), https://www.coindesk.com/business/2022/12/06/texas-bitcoin-miners-are-offered-to-cut-electricity-usage-to-help-the-grid.

1268ERCOT, *December 2022 Cold-Weather Operations Public Report* (Winter Storm Elliott), (Mar. 27, 2023), https://www.ercot.com/files/docs/2023/03/27/December-2022-Cold-Weather-Operations-Public-Report.pdf.

1269 Elizabeth Napolitano, *Texas Paid Bitcoin Miner More Than $31Million to Cut Energy Usage During Heat Wave*, CBS NEWS, (Sep 7, 2023), https://www.cbsnews.com/news/bitcoin-mining-cryptocurrency-riot-texas-power-grid/

within China's borders. Beginning that year, Chinese authorities implemented a comprehensive crackdown on cryptocurrency activities, including the explicit prohibition of mining operations *(See section 7.4.1.)*.[1270] These measures were justified by a combination of concerns, including financial stability, capital-control enforcement, fraud prevention, and broader energy-consumption and carbon-reduction objectives.[1271] As a result, a substantial share of mining activity migrated abroad, particularly to Kazakhstan[1272] and the United States,[1273] with the latter subsequently becoming the world's largest Bitcoin-mining hub.[1274] A study has alleged that this geographic shift increased the carbon intensity of Bitcoin mining, on the grounds that certain Chinese mining operations relied on seasonal hydroelectric power, whereas relocated miners have more often drawn on fossil-fuel-based electricity.[1275]

Kazakhstan illustrates how rapid inflows of mining activity can strain domestic energy systems. By 2021–2022, crypto-mining operations were estimated to account for approximately 7% of the country's total electricity consumption.[1276] Citing energy security and grid-reliability concerns as primary justifications, Kazakh authorities introduced a range of restrictive measures, including higher electricity tariffs for miners, licensing requirements, and usage caps.

In the United States, policy responses at the federal level have, thus far, focused on transparency and potential fiscal disincentives, rather than outright prohibitions. In 2023, Senator Ed Markey and Representative Jared Huffman introduced the Crypto-Asset Environmental Transparency Act,[1277] which would require large digital-asset mining facilities to disclose their energy consumption and greenhouse-gas emissions. The proposal has not advanced beyond early legislative stages. The Biden Administration also proposed a 30% excise tax on the cost of electricity used for digital-asset mining —the so-called Digital Asset Mining Energy (DAME) tax.[1278] But Congress did not enact the initiative, and the legislation was subsequently abandoned amid the start of a new congressional session and a new president's priorities.[1279]

Several U.S. states have pursued more targeted or divergent approaches. In 2022, New York enacted a temporary "moratorium on cryptocurrency mining operations that use proof-of-work authentication

1270 Taylor Dorrell, *United States of Bitcoin: Crypto Miners Got Kicked Out of China. Now They're Sucking America Dry*, BUSINESS INSIDER (Sep. 10, 2024), https://www.businessinsider.com/china-bitcoin-mines-american-electricity-china-crypto-ban-energy-crisis-2024-9

1271 Francis Shin,*What's Behind China's Cryptocurrency Ban?* WEF (Jan. 31, 2022), https://www.weforum.org/stories/2022/01/what-s-behind-china-s-cryptocurrency-ban/

1272 MacKenzie Sigalos, *Kazakhstan's Deadly Protests Hit Bitcoin, as the World's Second-Biggest Mining Hub Shuts Down*, CNBC, (Jan. 7, 2022), https://www.cnbc.com/2022/01/06/kazakhstan-bitcoin-mining-shuts-down-amid-fatal-protests.html

1273 Hiroko Tabuchi, *China Banished Cryptocurrencies. Now, 'Mining' is Even Dirtier,* NY TIMES (Feb. 25, 2022), https://www.nytimes.com/2022/02/25/climate/bitcoin-china-energy-pollution.html.

1274 Taylor Dorrell, *United States of Bitcoin: Crypto Miners Got Kicked Out of China. Now They're Sucking America Dry*, BUSINESS INSIDER, (Sep 10, 2024), https://www.businessinsider.com/china-bitcoin-mines-american-electricity-china-crypto-ban-energy-crisis-2024-9

1275 Alex de Vries, et al., *Revisiting Bitcoin's carbon footprint,* 6 Joule, Issue 3, 498 - 502 (2022), https://www-cell-com.stanford.idm.oclc.org/joule/fulltext/S2542-4351(22)00086-1; Hiroko Tabuchi, *China Banished Cryptocurrencies. Now, 'Mining' is Even Dirtier*, NY TIMES (Feb. 25, 2022), https://www.nytimes.com/2022/02/25/climate/bitcoin-china-energy-pollution.html

1276 Peter Guest, *After China's Crackdown, Bitcoin Mining Boom Moves to Kazakhstan*," MIT TECHNOLOGY REVIEW, (Jan. 12, 2023), https://www.technologyreview.com/2023/01/12/1066589/bitcoin-mining-boom-kazakhstan/

1277 Crypto-Asset Environmental Transparency Act of 2023, H.R. 1460, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/1460.

1278 Council of Economic Advisors, *The DAME Tax: Making Cryptominers Pay for the Costs They Impose on Others*, (May 2, 2023), THE WHITE HOUSE, https://bidenwhitehouse.archives.gov/cea/written-materials/2023/05/02/cost-of-cryptomining-dame-tax/.

1279 Scott Patterson and Amrith Ramkumar, *How Trump's AI, Crypto Push Would Spur Clean Energy*, THE WALL STREET JOURNAL, (Dec. 25, 2024), https://www.wsj.com/business/energy-oil/trump-clean-energy-ai-crypto-fe0f5bcf; THE WHITE HOUSE, *Strengthening American Leadership in Digital Financial Technology*, (Jan. 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

methods."[1280] New York legislation[1281] has also required state authorities to study the potential for powering digital-asset mining operations with renewable energy sources.[1282] Other states have taken a more permissive stance. Kentucky, for example, has enacted tax exemptions and incentives designed to attract Bitcoin-mining operations to the state.[1283] Texas, which hosts a significant share of U.S. mining capacity, has generally adopted an accommodative regulatory posture. But, to mitigate stress on the state's electricity network, it has also required large mining facilities to report electricity usage and participate in grid-management and demand-response programs.[1284]

Taken together, these initiatives illustrate the fragmented and evolving nature of public policy responses to the energy demands of proof-of-work mining. Regulatory approaches vary widely across jurisdictions, reflecting differing priorities related to climate policy.

5.4.1.C. Towards Renewable Energy Sources

The energy profile of major blockchain networks has increasingly shifted toward low-carbon and renewable energy sources. Researchers affiliated with the University of Cambridge's Centre for Alternative Finance examined the energy consumption of Ethereum following The Merge.[1285] The Centre's analysis suggests that approximately 48% of the electricity used by the network is derived from low-carbon sources, including renewable energy, such as wind and hydroelectric power, as well as nuclear energy. The remaining share is estimated to come from fossil fuels, primarily natural gas (around 30%), coal (19%), and oil (3%).[1286] While these figures remain estimates and depend on methodological assumptions, they indicate a meaningful shift toward lower-carbon energy sources, coupled with a drastic reduction in Ethereum's overall energy consumption following its adoption of proof-of-stake.

A parallel debate has emerged with respect to Bitcoin. Some Bitcoin-mining advocates argue that a substantial share of Bitcoin's electricity consumption is supplied by renewable or low-carbon energy sources, including solar, wind, and hydropower.[1287] According to the Bitcoin Mining Council (BMC)[1288] —an industry association whose participating members collectively represent approximately 43% of the global Bitcoin network— about 59.9% of Bitcoin's mining energy usage is "sustainable," a category that includes both renewable and other low-carbon sources.[1289] Independent estimates from the Cambridge Centre for Alternative Finance suggest a broadly comparable order of magnitude. It estimates that approximately 52.4% of Bitcoin's electricity use is derived from low-carbon sources, with about 42.6% attributable

1280 A. 7389C, 2021–2022 Reg. Sess. (N.Y. 2021) https://www.nysenate.gov/legislation/bills/2021/A7389.

1281 A.7866, 2021–2022 Reg. Sess. (N.Y. Assembly). https://www.assembly.state.ny.us/leg/?bn=A07866&term=2021

1282 S. 6486, 2021–2022 Reg. Sess. (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/S6486.

1283 *An Act Relating to Commercial Mining of Cryptocurrency,* S.B. 255, 2021 Reg. Sess. (Ky. 2021), (enacted as Ch. 141) https://legiscan.com/KY/text/SB255/id/2321901; *An Act Relating to the Taxation of the Commercial Mining of Cryptocurrency*, H.B. 230, 2021 Reg. Sess. (Ky. 2021) (enacted as Ch. 122), https://legiscan.com/KY/text/HB230/id/2321983.

1284 Public Utility Commission of Texas, Press Release, *PUCT Approves Rule Requiring Registration of Virtual Currency Mining Facilities*, (Nov 21, 2024), https://ftp.puc.texas.gov/public/puct-info/agency/resources/pubs/news/2024/PUCT_Approves_Rule_Requiring_Registration_of_Virtual_Currency_Mining_Facilities.pdf; *see also*, ERCOT, *Demand Response*, https://www.ercot.com/services/programs/load (last visited Jan. 15, 2026).

1285 Alexander Neumüller, *Ethereum's Climate Impact: A Contemporary and Historical Perspective*, Cambridge Ctr. for Alternative Fin., https://www.jbs.cam.ac.uk/2023/ethereums-climate-impact-a-contemporary-and-historical-perspective/, (last visited Jan. 15, 2026).

1286 *Id*.

1287 *Id*.

1288 Liam 'Akiba' Wright, *63% Renewable Energy Used by Bitcoin Mining Council Making up 43% of Global Mining Network,* CryptoSlate (Aug. 10, 2023) https://cryptoslate.com/63-renewable-energy-used-by-bitcoin-mining-council-making-up-43-of-global-mining-network/.

1289 *Id.*

specifically to renewable energy.[1290] Based on these estimates, Bitcoin's annual greenhouse-gas emissions have been estimated at roughly 95 million metric tons of carbon-dioxide equivalent ($MtCO_2e$), a figure often compared to the approximately 100 $MtCO_2e$ attributed annually by the global gold-mining industry, though such comparisons depend on contested methodological choices.[1291]

Advocates of Bitcoin mining also argue that, because mining operations are geographically flexible, they can be powered by energy resources that would otherwise be wasted. In particular, they point to methane produced at sites such as oil extraction fields or waste-management facilities, where it cannot easily be brought to market.[1292]

In oil production, natural gas is often released as a byproduct.[1293] Where pipeline or processing infrastructure is lacking, operators typically dispose of this gas on site through venting or flaring.[1294] Venting (the direct release of methane into the atmosphere) is prohibited or tightly restricted in many jurisdictions due to methane's extremely high global warming impact. Flaring (which involves combusting the gas) is generally permitted but still results in substantial greenhouse-gas emissions and other pollutants,[1295] and it is often imperfect in practice. Some Bitcoin-mining proponents contend that this stranded gas could instead be captured and combusted in electrical generators that power on-site mining operations.[1296] In theory, this approach could reduce uncontrolled methane emissions while producing economic value from gas that would otherwise be wasted. Projects of this kind already exist at a limited scale near active oil fields, though their overall environmental and systemic impact remains contested.

Proposals have also extended this logic to abandoned oil and gas wells, including "orphaned wells."[1297] In the United States, estimates suggest that approximately 3.7 million inactive wells remain,[1298] more than half of which are unplugged and continue to leak methane.[1299] Some advocates suggest that methane emissions from these sites could, in principle, be captured and used to power Bitcoin mining operations.[1300] In practice, however, such applications remain largely speculative and far less developed than projects involving active extraction sites.[1301]

1290 *Cambridge Study: sustainable energy rising in Bitcoin mining*, UNIVERSITY OF CAMBRIDGE: JUDGE BUSINESS SCHOOL, (April 28, 2025), https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/

1291 Cambridge Center for Alternative Finance, *supra* note 1254.

1292 Christian Stoll et al., *Climate Impacts of Bitcoin Mining in the U.S.*, MIT Ctr. for Energy & Env't Pol'y Rsh. Working Paper 2023-11, at 3 (2023), https://ceepr.mit.edu/wp-content/uploads/2023/06/MIT-CEEPR-WP-2023-11.pdf.

1293 World Bank Group, *Global Flaring and Methane Reduction Partnership (GFMR)*, https://www.worldbank.org/en/programs/gasflaringreduction/gas-flaring-explained (last accessed Dec 28, 2025).

1294 To use the gas, Bitcoin miners will still need to build a generation infrastructure on-site to clean and rechannel the expended gas into gas engines that can then power on-site computer infrastructure. This can be done entirely without access to a main power grid. See Stoll et al., *supra* note 1292, at 3.

1295IEA, *Gas Flaring*, https://www.iea.org/energy-system/fossil-fuels/gas-flaring (last accessed Dec 28, 2025); flaring is a controlled burn, but the method is not perfect: Residual methane emissions are common. Combusting the gas in an engine is not only a more productive use for the gas but a better methane-removal process. See Alexander Neumueller, et al., *Cambridge Digital Mining Industry Report,* Cambridge Center for Alternative Finance, (April 23, 2025), https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf.

1296 See Stoll et al., *supra* note 1292.

1297 According to the U.S. Environmental Protection Agency, there are an estimated 3.7 million abandoned oil and gas wells in the United States. This category encompasses both plugged (approximately 42%) and unplugged (approximately 58%) inactive wells, including orphaned wells. However, the available inventory does not disaggregate orphaned wells as a distinct category, as comprehensive data on orphaned wells remain unavailable. U.S. Department of the Interior, Orphaned Wells Program Office, *Assessing Methane Emissions from Orphaned Wells to Meet Reporting Requirements of the 2021 Infrastructure Investment and Jobs Act: Methane Measurement Guidelines* 5 (July 2023), https://www.doi.gov/sites/doi.gov/files/orphaned-wells-methane-measurement-guidelines-july-2023-version.pdf

1298 *Id.*

1299 See Stoll et al., *supra* note 1292 at 3.

1300 See Stoll et al., *supra* note 1292 at 3-4.

1301 See, e.g., Stoll et al., supra note 1292 at 1-3, discussing Bitcoin mining at orphaned wells as a potential benefit that "warrants closer attention" but emphasizes the need for "further research".

Oil fields are not the only source of under-utilized methane. Landfills generate methane through the decomposition of organic waste and account for a substantial share of human-caused methane emissions.[1302] This methane can be captured and repurposed for on-site electricity generation, including to power Bitcoin mining operations, a practice that already exists, albeit at a limited scale. In the United States, captured landfill gas is also commonly processed into renewable natural gas.[1303] Relative to uncontrolled venting or release, such uses can significantly reduce CO_2-equivalent emissions.

Critics, however, may argue that the broader relevance of these approaches is constrained.[1304] Only a small fraction of Bitcoin's total energy demand can realistically be met through flared gas or landfill methane, and mobile mining installations may divert gas that could otherwise be used for grid-connected electricity generation or more socially productive purposes. Moreover, imperfect combustion, generator inefficiencies, and upstream methane leakage can substantially erode claimed emissions benefits, particularly when projects are not subject to rigorous monitoring, reporting, and verification requirements.

5.4.2. Water Consumption

Electricity is not the only resource consumed by blockchain infrastructure. While mining and validation activities do not inherently require water, water may be consumed upstream through electricity generation, particularly where thermoelectric power plants rely on water-intensive cooling systems and, in some cases, through on-site cooling of data-center equipment. One estimate suggests that Bitcoin mining operations in the United States may have a cumulative water footprint comparable to that of approximately 300,000 U.S. households.[1305] Such figures, however, remain estimates and are highly sensitive to methodological choices.

Concerns about water consumption have been invoked to support arguments that Bitcoin should transition away from energy-intensive proof of work and toward less resource-intensive consensus mechanisms. Critics of this position counter that water consumption is not intrinsic to proof-of-work mining itself but, instead, largely reflects the characteristics of the underlying energy infrastructure. From this perspective, water impacts vary widely depending on the energy sources used to power mining operations rather than on the consensus mechanism as such. Others have, therefore, emphasized alternative mitigation strategies, including the use of low-water or non-freshwater energy sources and more water-efficient cooling technologies.

Experimental efforts are underway: Microsoft has been working on a water-free cooling system,[1306] and others are trying to develop seawater cooling systems.[1307] To date, however, the effectiveness, scalability, and environmental trade-offs of these approaches remain uncertain.

1302 In general, methane emissions are 86 times more potent than carbon dioxide emissions over a 20-year horizon. *See* Climate Trace Labs, *Accelerating Global Decarbonization Through Emissionality,* U.S. CLIM. TRACE, https://labs.climatetrace.org/landfill/https://labs.climatetrace.org/landfill/ (last visited Jan. 15, 2026).

1303 See, e.g.,U.S. Env't Prot. Agency, *Landfill Methane Outreach Program (LMOP): Project and Landfill Data* (2025), https://www.epa.gov/lmop (documenting the prevalence of RNG conversion projects).

1304 See, e.g., Earthjustice, *The Environmental Impacts of Cryptomining*, https://earthjustice.org/feature/cryptocurrency-mining-environmental-impacts (last updated Jan. 30, 2025).

1305 Alex de Vries, *Bitcoin's Growing Water Footprint*, 1 CELL REPS. SUSTAINABILITY 100004 (2024), https://doi.org/10.1016/j.crsus.2023.100004

1306 James Darley, *Microsoft's Zero-Water Solution for Data Centre Cooling*, SUSTAINABILITY MAGAZINE, (Dec 11, 2024), https://sustainabilitymag.com/articles/microsoft-unveils-zero-water-cooling-for-ai-data-centres.

1307 Reza Mokhtari and Ahmad Arabkoohsar, *Feasibility Study and Multi-Objective Optimization of Seawater Cooling Systems for Data Centers: A Case Study of Caspian Sea*, 47 SUSTAINABLE ENERGY TECHNOLOGIES & ASSESSMENTS 101528 (Oct. 2021), https://doi.org/10.1016/j.seta.2021.101528/

5.5. PRIVACY CHALLENGES

Most public blockchains make transaction data visible to anyone.[1308] In permissionless systems such as Bitcoin, transactions are recorded on an open ledger that can be freely accessed and verified by both network participants and external observers. Although users are identified only through cryptographic addresses rather than real-world identities, the full transaction history associated with an address is publicly visible and permanently recorded. This transparency can raise significant privacy concerns, particularly when blockchain data is combined with external information that enables the reidentification of users.

Permissioned or private blockchains generally pose a somewhat lower privacy risk because access to the ledger is restricted to authorized participants.[1309] However, participants within the network are typically able to view transaction data unless additional confidentiality mechanisms are implemented.

Historically, blockchain proponents have claimed that, despite the full transparency of transactions, pseudonymity can safeguard privacy.[1310] The Bitcoin white paper *(See Figure 1)* argued that privacy could be preserved "by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else but without information linking the transaction to anyone."[1311] However, this pseudonymity is not sufficient, as there are various means available to de-anonymize users and obtain personal information. This section will focus on that issue, while compliance with data protection frameworks is examined in section 6.7.[1312]

5.5.1. User Identification Using Transaction Histories and On-Chain Communications

Although blockchain transactions are pseudonymous and authenticated through cryptographic signatures, they are typically publicly visible, transparent, and trackable. The data that is stored on the blockchain cannot be altered or deleted.[1313] Coupled with transparency, this immutability facilitates a high degree of user profiling. Specifically, by observing and analyzing a blockchain user's transaction history and interactions, it is possible to build detailed user profiles that reveal insights into the user's financial status, habits, transaction patterns, affiliations, and, potentially, their real-world identity.[1314]

For example, time-stamp data —like the timestamps associated with social-media activity— can significantly compromise an individual's privacy by enabling

1308 European Data Protection Board, *Guidelines 02/2025 on Processing of Personal Data Through Blockchain Technologies, Version 1.1*, Adopted on Apr. 8, 2025 (public consultation version), https://edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf, [hereinafter EDPB Guidelines 02/2025]; Vitalik Buterin et al., *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium,* 5 Blockchain: Research and Applications, 100176 (2024), https://doi.org/10.1016/j.bcra.2023.100176*;* Oluwafemi Akanfe, Diane Lawong & H. Raghav Rao, *Blockchain Technology and Privacy Regulation: Reviewing Frictions and Synthesizing Opportunities,* 76 Int'l J. Info. Mgmt. 102753 (2024) https://www.sciencedirect.com/science/article/abs/pii/S026840122400001X?via%3Dihub*;* Muhammad Al-Abdullah et al., *Designing privacy-friendly data repositories: A framework for a blockchain that follows the GDPR,* 22 Digital Pol'y, Reg. & Governance 393 (2020) https://www.emerald.com/dprg/article-abstract/22/5-6/389/38471/Designing-privacy-friendly-data-repositories-a?redirectedFrom=fulltext.

1309 Francisco José de Haro-Olmo, Ángel Jesús Varela-Vaca & José Antonio Álvarez-Bermejo, *Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review*, 20 Sensors 7171 (2020) https://www.mdpi.com/1424-8220/20/24/7171.

1310 Buterin, *supra* note 1308.

1311 Satoshi Nakamoto, *Bitcoin: a Peer-to-Peer Electronic Cash System*, 6 (2008), https://bitcoin.org/bitcoin.pdf.

1312 The notion of privacy has a broader scope than personal data protection. The right to privacy encompasses an individual's autonomy in making decisions about their identity, relationships, and personal interactions without undue interference or control. Personal data protection specifically concerns safeguarding information that can identify an individual, such as their name, birthdate, phone numbers, email addresses, or IP addresses.

1313 Claudio Lima, *Blockchain-GDPR Privacy by Design: How Decentralized Blockchain Internet Will Comply with GDPR Data Privacy*, at 2-3 (2018), https://attachment.victorlampcdn.com/article/content/20230315/blockchain-gdpr-privacy-by-design.pdf (last visited Jan. 15, 2026); Pascal Ugochukwu Ojukwu et al., *Exploring Theoretical Constructs of Blockchain Technology in Banking: Applications in African and U. S. Financial Institutions*, 4 Int'l J. Frontline Res. Sci. & Tech. 36 (2024), https://frontlinejournals.com/ijfrst/sites/default/files/IJFRST-2024-0051.pdf.

1314 Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments: Characterizing Payments Among Men with No Names*, in Proc. Internet Measurement Conf. at 127, 131-140, (2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

behavioral inference. If analysis of aggregate time-stamp data reveals occasional activity between 7:00–9:00 a.m. Eastern Standard Time, followed by inactivity from 9:00 a.m. to 12:00 p.m., increased activity during a lunch break (12:00–1:00 p.m.), inactivity until 5:00 p.m., and sustained activity between 5:00–10:00 p.m. —and this pattern holds primarily on weekdays, with irregular activity on weekends and U.S. federal holidays— one could reasonably infer that the account holder resides in the Eastern Time Zone of the United States. This conclusion alone would exclude approximately 98% of the global population as potential candidates. Similar inference techniques apply to blockchain data, where transaction timing, frequency, and coordination across addresses are observable on a public ledger.

Such analyses become even more effective when additional data points are triangulated. For example, observing memecoin trading accounts can reveal usage patterns that are far more predictive than random chance with respect to a user's geographical location or behavioral profile. This privacy risk escalates further when diverse forms of blockchain-related data are aggregated, including which specific memecoins a user purchases, the blockchain addresses they interact with, the chains they use and at what times, etc.[1315] When combined, these data points enable blockchain analytics providers, such as Chainalysis, often in cooperation with exchanges or law-enforcement authorities, to de-anonymize users and, in many cases, attribute on-chain activity to specific individuals.

Today, many private companies and state authorities use advanced blockchain analytic techniques to link pseudonymous blockchain addresses to real-world identities. By clustering and connecting transactions, these techniques reveal patterns, spending behaviors, and relationships among different addresses. Even in the absence of direct personal identifiers, transaction metadata —such as timing, frequency, and size— can expose sensitive information about users. Additionally, the reuse of blockchain addresses increases the number of data points available for correlation, thereby amplifying the risk of de-anonymization.

The analysis of on-chain communications further increases risks to privacy. While blockchain activity primarily involves the transfer of digital assets or the execution of smart contracts, on-chain communications include additional data that may expose a user's identity. These communications encompass transaction metadata —such as wallet addresses, transaction amounts, time-stamps, and hashes— as well as messages embedded within transactions or data exchanged through smart contract interactions.[1316] Because this information is generally accessible to anyone with the ability to view the blockchain,[1317] it can be analyzed and correlated with transaction histories, thereby increasing the likelihood of identifying users or inferring sensitive aspects of their activities.

Various examples illustrate the ability to identify blockchain users:

- **"Individual X"[1318] and James Zhong**. The U.S. Internal Revenue Service's Criminal Investigation (IRS-CI) unit in 2020[1319] and 2021[1320] used

1315 *See* Jiajun Zhou et al., *Behavior-aware Account De-anonymization on Ethereum Interaction Graph*, arXiv (Sept. 13, 2022), https://arxiv.org/abs/2203.09360.

1316 EDPB Guidelines, *supra* note 1308, at 8; Yeolib Kim et al., *Privacy Concern and Its Consequences: A Meta-Analysis*, 196 Tech. Forecasting and Soc. Change 122789 (2023) https://www.sciencedirect.com/science/article/abs/pii/S0040162523004742?via%3Dihub.

1317 EDPB Guidelines, *supra* note 1308 at 8.

1318 Chainalysis Team, *Chainalysis in Action: U.S. Government Agencies Seize More Than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road,* Chainalysis (Nov. 5, 2020), https://www.chainalysis.com/blog/silk-road-doj-seizure-november-2020/.

1319 *Id*.

1320 Chainalysis Team, *How IRS-CI Seized Billions from Silk Road Hacker James Zhong,* Chainalysis (Sept. 13, 2023), https://www.chainalysis.com/blog/james-zhong-silk-road-hack-seizure/.

blockchain analytics tools, in combination with other investigative techniques, to track and seize approximately 69,370[1321] bitcoin and 50,676[1322] bitcoin from the anonymous hacker known as "Individual X"[1323] and James Zhong,[1324] respectively, both of whom are believed to have stolen bitcoin from wallets associated with the Silk Road darknet marketplace.

- **Colonial Pipeline**. In 2021, the FBI used blockchain analytics tools to trace multiple Bitcoin transfers paid as ransom to the DarkSide ransomware group following the Colonial Pipeline attack.[1325] The FBI ultimately seized approximately 63.7 bitcoins from wallet addresses associated with the group, after obtaining access to the private key controlling the relevant wallet.[1326]
- **Operation Token Mirrors**. In October 2024, the FBI conducted "Operation Token Mirrors," an undercover operation in which agents created a fictitious cryptocurrency company and token (NexFundAI) to detect and expose large-scale market-manipulation schemes. The operation led to the indictment of 18 individuals, the seizure of more than $25 million in cryptocurrency, and the shutdown of numerous market-manipulation bots. The investigation relied on the analysis of smart-contract interactions, transaction metadata, and patterns of wash trading across multiple tokens.[1327]
- **Hamas terrorist financing scheme**. In March 2025, the U.S. Department of Justice announced the disruption of a Hamas terrorist-financing scheme involving a network of cryptocurrency addresses used to funnel funds to the organization. Investigators relied on blockchain analytics tools to trace donation flows, identify operational wallets, and seize assets, with key support from exchanges and stablecoin issuers that froze funds under their control.[1328]

The inherent traceability of blockchain transactions, together with the ability to construct detailed user profiles, raises significant concerns about large-scale surveillance. Governments and private organizations can deploy transaction-graph analysis tools to aggregate blockchain data and monitor user activity at scale. Similarly, corporations may exploit blockchain-derived user profiles to refine targeted advertising strategies,

1321 Chainalysis Team, *Chainalysis in Action: U.S. Government Agencies Seize More Than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road,* Chainalysis (Nov 5, 2020), https://www.chainalysis.com/blog/silk-road-doj-seizure-november-2020/.

1322 *How IRS-CI Seized Billions from Silk Road Hacker James Zhong, supra* note 1320.

1323 *Chainalysis in Action, supra* note 1321.

1324 *How IRS-CI Seized Billions from Silk Road Hacker James Zhong, supra* note 1320.

1325 Colonial Pipeline Company, a major fuel supplier for the U.S. East Coast, fell victim to a ransomware attack by a group known as DarkSide. The cyberattack severely disrupted pipeline operations, cutting off nearly half of the region's gasoline, diesel, and jet fuel supply. This cyberattack led to widespread fuel shortages, panic buying, and price hikes across multiple states. Jen Easterly, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*, Cybersecurity & Infrastructure Security Agency (2024), https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (last visited Jan. 15, 2026). U.S. Dep't of Just., *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to Ransomware Extortionists DarkSide* (June 7, 2021) https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (stating that the FBI "tracked multiple transfers of bitcoin" paid as ransom following the Colonial Pipeline attack); Affidavit in Support of Seizure Warrant paras. 10–12, *In re Search of Info. Associated with Specific Bitcoin Address* (N.D. Cal. June 7, 2021) https://www.justice.gov/archives/opa/press-release/file/1402056/dl. (describing FBI's review of Bitcoin public ledger to trace ransom payments).

1326 Press Release, Office of Pub. Affairs, U.S. Dep't of Just., *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide* (2024), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (last visited Jan. 15, 2026), *see also*, Affidavit in Support of Seizure Warrant, *supra* note 1325.

1327 Chainalysis, *The 2022 Crypto Crime Report* 30–36 (2022), https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf; TRM Labs, *FBI Creates Token Project in Trojan Horse Crypto Operation That Seizes $25 Million*, TRM Insights (Oct. 18, 2024), https://www.trmlabs.com/post/fbi-creates-token-project-in-trojan-horse-crypto-operation-that-seizes-25-million.

1328 Press Release, U.S. Dept. of Justice, *Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure of Cryptocurrency* (Mar. 27, 2025), https://www.justice.gov/opa/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure-cryptocurrency; Chainalysis Team, *United States DOJ and FBI Seize Cryptocurrency in Major Disruption of Hamas Terrorist Financing Scheme*, Chainalysis Blog (Mar. 28, 2025), https://www.chainalysis.com/blog/doj-fbi-seize-cryptocurrency-disrupt-hamas-terrorist-financing-scheme-march-2025/.

tailoring content based on users' transaction patterns, interests, and financial behaviors. The permanence of blockchain records exacerbates these risks, as past activity remains accessible indefinitely, allowing behavior to be tracked, aggregated, and analyzed over long periods of time. These concerns become more pronounced as blockchain platforms scale or achieve mainstream adoption, dramatically increasing the volume of available data.

Overall, one may wonder whether blockchain systems offer less effective privacy protection than bank-based systems, despite their initial promise to circumvent centralized surveillance. In conventional banking systems, transaction data is held by regulated intermediaries and is subject to legal constraints, including limits on access and retention that vary by jurisdiction (often several years). By contrast, public blockchains make transaction data openly accessible to anyone and preserve it indefinitely, thereby enabling continuous and cumulative analysis by both state and private actors. In this respect, blockchain systems may, paradoxically, reduce certain forms of institutional opacity while simultaneously expanding the scope for broader, and potentially less constrained, forms of surveillance —a trade-off that existing data protection frameworks were not designed to address.

5.5.2. Analysis of Information Included in Off-Chain Communications

Off-chain communication refers to interactions that occur outside the blockchain but are connected to on-chain decisions or activities. These communications include direct messaging between users via non-blockchain channels, community discussions on forums or social media, and email exchanges between parties. When they are public, such communications can be exploited. For example, discussions on public platforms, such as governance forums and social media, create off-chain records that can be correlated with users' on-chain activity.

Unless conducted on public platforms, off-chain interactions are generally not publicly accessible. However, when data from off-chain communications are linked to transparent on-chain activities, they significantly amplify privacy risks by increasing the potential for linking pseudonymous blockchain activity to real-world identities and behaviors. For instance, governance votes conducted off-chain —through platforms like Snapshot,[1329] where voting power is tied to on-chain token holdings— can be cross-referenced with publicly visible wallets.

5.5.3. The Disclosure of Personal Information to Administrators and Service Providers

In private and permissioned blockchains, where access is restricted, the identities of users are usually known to the platform administrators. In contrast, on public blockchains, users can create blockchain addresses cryptographically without providing personal information. These addresses operate solely through public-private key pairs and are not inherently connected to real-world identities.[1330] However, to store and transfer crypto-assets, users typically create a digital wallet. The most common approach involves using an online service provider, such as Coinbase or Binance.

These custodial service providers hold users' private keys and often offer both cryptocurrency storage and

1329 Snapshot's users sign messages with their wallet to vote, and voting power is determined by their on-chain token holdings. The votes themselves are not submitted as blockchain transactions but are instead stored off-chain, typically via decentralized file storage systems Arweave. Snapshot Labs, *Introducing Snapshot's Onchain Voting Protocol: Snapshot X, Mirror* (Sept. 9, 2024), https://snapshot.mirror.xyz/F0wSmh8LROHhLYGQ7VG6VEG1_L8_IQk8eC9U7gFwep0.

1330 CoinGeek, *Blockchain Networks: Private, Public, & Permissioned*, (Sept. 8, 2024), https://coingeek.com/blockchain101/private-vs-public-vs-permissioned-blockchain-a-comparative-guide/; Investopedia, *Public, Private, and Permissioned Blockchains Compared*, (Nov. 2, 2024), https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/ .

exchange services.[1331] KYC/AML regulations often require these service providers to collect identifying information. For instance, in the United States, most crypto exchanges are classified as money service businesses (MSBs) under federal law and must comply with the Bank Secrecy Act (BSA). This requires them to register with FinCEN and implement KYC/AML programs, including customer identification, verification, and ongoing monitoring.[1332] Similarly, in the European Union, crypto exchanges and custodial wallet providers must register with local regulators and follow KYC/AML procedures, including collecting and verifying customer identity documents.[1333] They usually require customers to undergo identity verification, particularly those offering fiat currency conversion services, as part of their KYC/AML compliance. A user is typically required to provide identification documents, such as a driver's license, passport, or utility bill.[1334] In practice, many custodial wallets are also linked to real-world bank accounts or credit/debit cards.[1335]

The only way to avoid disclosing personal information is to create a non-custodial wallet. This is a cryptocurrency wallet where the user has complete control over their private keys and digital assets, rather than entrusting them to a third party. In this case, there is no need to register with personal information or undergo KYC verification. Transactions are submitted directly to the blockchain network. Popular non-custodial wallets include MetaMask, Trust Wallet, Ledger, and Trezor. They come in various forms, including hardware wallets (physical devices), software wallets (desktop/mobile apps), and paper wallets (physical documents).[1336]

Finally, some applications require users to publish information about themselves on-chain. For example, registering a name on decentralized domain name services, such as the Ethereum Name Service (ENS), involves making a transaction on the Ethereum blockchain and creating a public link between transactions and the users' ENS name.[1337]

1331 FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. Coinbase, *What Does Coinbase Do With My Digital Assets?*, (June 6, 2022), https://help.coinbase.com/en/coinbase/other-topics/legal-policies/what-does-coinbase-do-with-my-digital-assets; Binance, *Everything You Need to Know About Our Self-Custody Web3 Wallet*, (Feb. 24, 2025), https://www.binance.com/en/blog/ecosystem/binance-wallet-everything-you-need-to-know-about-our-selfcustody-web3-wallet-7898832595548730429.

1332 31 U.S.C. § 5311 et seq. (2022); 31 C.F.R. § 1010.100(ff) (2022); Dep't of the Treasury, Fin. Crimes Enf't Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* FIN-2013-G001 (Mar. 18, 2013) https://www.fincen.gov/system/files/shared/FIN-2013-G001.pdf; Dep't of the Treasury, Fin. Crimes Enf't Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

1333Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "AML Regulation").

1334 Trulioo, *Understanding KYC Crypto Requirements* (Oct. 26, 2023), https://www.trulioo.com/industries/crypto-identity-verification/kyc; Plaid, *KYC for Crypto: Ensuring Crypto Security and Compliance* (Oct. 21, 2024), https://plaid.com/resources/compliance/kyc-crypto/.

1335 Institutional Real Estate Inc., *The Era of Digital Wallets,* (Sept. 1, 2022) https://irei.com/publications/article/era-digital-wallets/; ID.me Network, *Digital Wallets – Beyond Payments,* (June 16, 2020) https://network.id.me/article/digital-wallets-beyond-payments/.

1336 Education for Consumers, *The Best Non-Custodial Wallets for Storing Your Cryptocurrency Safely,* CoinPayments (Mar. 28, 2024), https://media.coinpayments.net/consumer-education/best-non-custodial-wallets/.

1337 Ethereum Name Service, *How to Register a .eth Name* (2025), https://support.ens.domains/en/articles/7882582-how-to-register-a-eth-name.

FIGURE 46.

United States v Gratkowski

In the U.S. case *United States v. Gratkowski*,[1338] law enforcement used blockchain analysis tools to identify individuals who purchased child pornography using bitcoins.[1339] Authorities traced bitcoin wallet addresses and subpoenaed Coinbase for records of users who had transacted with these addresses.[1340] By correlating on-chain wallet data with Coinbase's information, they were able to identify Richard Gratkowski, leading to his arrest[1341] and indictment on child pornography charges. Gratkowski entered a conditional guilty plea[1342] and appealed the denial of his motion to suppress the evidence obtained from a search warrant executed at his home.[1343]

Interestingly, Gratkowski argued on appeal that his on-chain Bitcoin transaction records and the personal information held by Coinbase were private and protected under the Fourth Amendment[1344] of the U.S. Constitution.[1345] He claimed that the seizure of this data by law enforcement without a warrant amounted to an unlawful search, violating his constitutional right to privacy.[1346]

However, the Fifth Circuit U.S. Court of Appeals rejected this argument.[1347] It ruled that Bitcoin transaction records are not protected by the Fourth Amendment, as they are publicly recorded on the Bitcoin ledger, which is intentionally designed to be transparent.[1348] The court compared the records held by Coinbase to that of traditional bank records, which are subject to the third-party doctrine because they are voluntarily provided to financial institutions. Consequently, the Fifth Circuit affirmed the District Court's denial of Gratkowski's motion to suppress, concluding that Bitcoin users have no reasonable expectation of privacy regarding their transaction records on the public Bitcoin blockchain or their personal information held by exchanges such as Coinbase.[1349]

1338 *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020) https://law.justia.com/cases/federal/appellate-courts/ca5/19-50492/19-50492-2020-06-30.html.

1339 *Id*. at 307.

1340 *Id*. at 308.

1341 *Id*. at 307.

1342 *Id*. at 308.

1343 Daniel Penn, *The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy,* 24 SMU Sci. & Tech. L. Rev. 125, 125–34 (2021), https://scholar.smu.edu/scitech/vol24/iss1/6/.

1344 "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; U.S. Constitution - Fourth Amendment, Constitution Annotated, Congress.gov, https://constitution.congress.gov/constitution/amendment-4/ (last visited Jan. 15, 2026).

1345 *United States v. Gratkowski*, 964 F.3d 307 at 309, https://law.justia.com/cases/federal/appellate-courts/ca5/19-50492/19-50492-2020-06-30.html.

1346 *Id.* at 310.

1347 *Id.* at 309.

1348 *Id.* at 310–11.

1349 *Id*., Penn, *The Fifth Circuit and Bitcoin Privacy,* 24 SMU Sci. & Tech. L. Rev. 127 (2021).

5.5.4. Limitations of Privacy Tools

Various techniques have been developed to reinforce pseudonymity on blockchain networks *(See above section 2.6.1.)*.[1350] Some blockchain platforms —most notably privacy-focused cryptocurrencies such as Monero and, in certain configurations, Zcash— are specifically designed to limit the traceability of transactions by concealing transaction amounts, counterparties, or address linkages. In these systems, on-chain analysis is significantly constrained, making it extremely difficult, though not categorically impossible, to trace transactions or link them to identifiable individuals, particularly when attribution relies solely on publicly available blockchain data. While privacy advocates view these features as a benefit, emphasizing that an electronic equivalent to cash is essential to maintaining a free and open society, government authorities often perceive such systems as posing heightened risks for law enforcement and regulatory oversight.

Tornado Cash, one of the most prominent privacy-enhancing protocols *(See section 2.6.2.)*, was designed to address privacy concerns by severing the on-chain link between deposit and withdrawal addresses. However, it was also exploited by malicious actors. Deposit records and subsequent investigations indicated that hacker groups used the protocol to launder funds derived from illicit activities.[1351] Notably, evidence linking Tornado Cash to transactions associated with a North Korean state-sponsored hacking group led to the inclusion of Tornado Cash's smart-contract addresses on the Specially Designated Nationals and Blocked Persons (SDN) list maintained by the U.S. Office of Foreign Assets Control (OFAC)[1352] (On the Tornado Cash case, *see section 6.5.3.*). A core issue with Tornado Cash was that legitimate users had limited means to credibly dissociate themselves from criminal activity linked to the protocol. Although Tornado Cash offered a compliance tool that enabled users to demonstrate that a given withdrawal corresponded to a specific prior deposit, the practical use of such tools often depended on trusted relayers or verification mechanisms, thereby introducing forms of reliance on intermediaries and creating information asymmetries.[1353]

In this context, a persistent tension exists between cryptocurrency privacy and regulatory oversight, as law-enforcement agencies explore methods for tracing transactions on privacy-focused systems. In practice, identifying users in such systems frequently depends on obtaining information from exchanges, custodial wallet providers, or other service intermediaries that maintain customer records. Access to this information generally requires legal authorization, such as a search warrant, court order, or subpoena. The issuance of such instruments typically presupposes that authorities can present sufficient grounds to a judicial body to establish a reasonable suspicion or likelihood that criminal conduct has occurred.

Governments have also promoted research aimed at improving the traceability of privacy-enhancing cryptocurrencies.[1354] In 2020, the U.S. Internal Revenue Service (IRS) Criminal Investigation (CI) division

1350 Vitalik Buterin et al., *supra* note 1308.; Johannes Heurix et al., *A Taxonomy for Privacy Enhancing Technologies,* 53 Comput. & Sec. 2 (2015), https://www.sciencedirect.com/science/article/abs/pii/S0167404815000668.

1351 Z. Wang et al., *On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy,* arXiv preprint, arXiv:2201.09035 (2022), https://doi.org/10.48550/arXiv.2201.09035.

1352 Office of Foreign Assets Control, *Cyber-related Designation*, U.S. Dep't Of The Treasury (Aug. 8, 2022), https://ofac.treasury.gov/recent-actions/20220808.

1353 M. Nadler & F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* 105 Fed. Res. Bank St. Louis Rev. 122, 122–36 (2023), https://doi.org/10.20955/r.105.122-136.

1354 Andrew Hayward, *US Homeland Security Can Now Track Privacy Crypto Monero*, Decrypt (Aug. 31, 2020), https://decrypt.co/40284/us-homeland-security-can-now-track-privacy-crypto-monero.

offered two bounties[1355] to support the development of blockchain-analysis tools capable of generating investigative leads related to transactions on privacy-focused cryptocurrencies, particularly Monero (XMR) and Zcash (ZEC).[1356] These contracts,[1357] awarded to Chainalysis[1358] and Integra FEC,[1359] sought to enhance law-enforcement capabilities in detecting and investigating illicit activity involving such assets. Although the technical details and effectiveness of the resulting tools were not publicly disclosed, the initiative illustrates the ongoing contest between developers seeking to preserve strong privacy protections and authorities attempting to expand investigative reach.[1360]

In addition to initiatives undertaken by public authorities, users' identities may also be disclosed through actions by private actors. In July 2023, Arkham Intelligence, a company specializing in blockchain attribution and analytics,[1361] sparked controversy by launching a bounty-based program that incentivized participants to submit information linking blockchain addresses to real-world identities. Participants could report personally identifiable information in exchange for monetary rewards. This so-called "dox-to-earn" model was widely criticized within the cryptocurrency community, on ethical and privacy grounds.[1362] Arkham was also the subject of public allegations made by the whistleblower platform Crypto Leaks, which claimed that the company had obtained user-identifying information by exploiting vulnerabilities or privileged access points at major cryptocurrency exchanges.[1363] According to these allegations, Arkham may have leveraged exchange-related transaction data, including deposit and withdrawal address linkages, to enhance its attribution capabilities. While these claims have not been judicially established, the controversy highlights broader concerns about the role of private analytics firms in eroding privacy protections through data aggregation and attribution practices.

1355 Kollen Post, *Chainalysis and Texas Firm Win Million-Dollar IRS Contract to Crack Monero,* Cointelegraph (Sept. 30, 2020), https://cointelegraph.com/news/chainalysis-and-texas-firm-win-million-dollar-irs-contract-to-crack-monero.

1356 Joshua Mapperson, *The IRS Offers a $625,000 Bounty to Anyone Who Can Break Monero and Lightning,* Fed. Cointelegraph (Sept. 11, 2020), https://cointelegraph.com/news/the-irs-offers-a-625-000-bounty-to-anyone-who-can-break-monero-and-lightning.

1357 *Pilot IRS Cryptocurrency Tracing Award Notice,* Sam.gov (2020), https://sam.gov/opp/5ab94eae1a8d422e88945b64181c6018/view (last visited Jan. 15, 2026).

1358 *The Blockchain Data Platform,* Chainanalysis (2024), https://www.chainalysis.com/ (last visited Jan. 15, 2026).

1359 IntegraFEC, IntegraFEC, https://www.integrafec.com/ (last visited Jan. 15, 2026).

1360 See *US Homeland Security Can Now Track Privacy Crypto Monero*, Decrypt (Aug. 31, 2020), https://decrypt.co/40284/us-homeland-security-can-now-track-privacy-crypto-monero; *The IRS Is Offering You $625,000 to Crack Monero*, Decrypt (Sept. 10, 2020), https://decrypt.co/41411/the-irs-is-offering-you-625000-to-crack-monero.

1361 Arkham Intelligence Platform, https://platform.arkhamintelligence.com/ (last visited Jan. 15, 2026).

1362 *See* James Cirone, *Crypto sleuths have a new way to get paid: Arkham's on-chain intelligence platform*, Blockworks (Jul. 10, 2023 https://blockworks.co/news/arkham-on-chain-intelligence-platform; *See also* Sam Kessler, *Arkham CEO Defends 'DOX-to-Earn' Program, Says Public Blockchains 'Worst' for Privacy*, CoinDesk (Jul. 11, 2023), https://www.coindesk.com/tech/2023/07/11/arkham-ceo-defends-dox-to-earn-program-says-public-blockchains-worst-for-privacy;

1363 Liam Wright, *Whistleblower Accuses Arkham Intelligence of Exploiting Crypto Exchange Backdoors to Dox Users,* CryptoSlate (Oct. 6, 2023), https://cryptoslate.com/whistleblower-accuses-arkham-intelligence-of-exploiting-crypto-exchange-backdoors-to-dox-users/; Digital Assets Team, *Here's Why Anonymous NFT and Crypto Founders Continue to Gain Popularity,* Forbes (Sept. 1, 2023), https://www.forbes.com/sites/digital-assets/2023/09/01/heres-why-anonymous-nft-and-crypto-founders-continue-to-gain-popularity/.

KEY TAKEAWAYS

■ Crypto-assets exhibit high and persistent **price volatility,** making the blockchain ecosystem highly vulnerable to sudden shocks. Although some recent analyses suggest that Bitcoin's volatility has declined as crypto markets mature, significant price swings remain a defining and persistent feature of the asset class. At the same time, there is deep disagreement over whether crypto-assets possess **fundamental value**, with critics arguing they lack intrinsic economic anchors and proponents claiming that utility, scarcity, network effects, and collective expectations can justify non-zero valuations.

■ **Stablecoins** have drawn intense scrutiny, as policymakers and central banks have warned that both asset-backed and algorithmic designs can generate risk, contagion, and systemic vulnerabilities. These concerns have been underscored by the collapse of algorithmic stablecoins, such as Terra/Luna, and by ongoing transparency and reserve-adequacy issues affecting some asset-backed models, including Tether.

■ **Non-fungible tokens (NFTs)** pose significant speculative and consumer risks, having experienced a sharp boom-and-bust cycle marked by extreme price volatility and substantial losses for many investors. Beyond these market risks, NFTs raise complex legal issues, as ownership of a token does not necessarily confer rights in the underlying asset. Legal uncertainty remains a defining feature of the NFT ecosystem.

■ Crypto-asset markets remain highly susceptible to **manipulation** because they often lack the disclosure requirements, market-surveillance mechanisms, and conflict-of-interest safeguards that govern traditional financial markets. This situation creates structural opacity and enables such practices as wash trading, pump-and-dump schemes, insider trading, and coordinated price manipulation.

■ Crypto markets have experienced repeated high-profile bankruptcies, from Mt. Gox to the Terra/Luna collapse and the 2022 collapse of FTX, exposing deep structural weaknesses in the ecosystem. These failures were driven by excessive leverage, opaque governance, concentrated counterparty exposure, misuse of customer funds, and fragile business models lacking effective risk management and supervision.

■ Blockchain's pseudonymity, permissionless access, and lack of centralized control can facilitate **illicit uses** —such as fraud, money laundering, ransomware, sanctions evasion, and scams— by enabling transactions outside traditional regulatory and enforcement frameworks. Yet available data indicates that illicit transactions constitute only a small fraction of total on-chain activity. Moreover, the transparency of public blockchains increasingly enables effective forensic tracing and law-enforcement investigations.

■ Decentralization can reduce single points of failure compared to centralized systems, but blockchain ecosystems continue to face significant and evolving **security vulnerabilities.** Most successful exploits occur at the application layer, where bugs or design flaws in smart contracts —such as oracle manipulation, flash-loan abuse, bridge failures, and hidden backdoors— are particularly prevalent in DeFi. Centralized intermediaries, especially custodial exchanges, remain highly attractive targets, as illustrated by incidents like Mt. Gox. Finally, individual users are often the weakest link: Phishing, malicious transaction approvals, private-key compromise, and even physical coercion ("wrench attacks") frequently enable attackers to seize assets.

■ **Environmental concerns** surrounding blockchain focus primarily on the high consumption of electricity for proof-of-work systems. Governments have responded with a fragmented array of measures —from outright bans and moratoria to disclosure obligations and grid-management requirements. Meanwhile, debate continues over the extent to which mining relies on renewable or low-carbon energy sources. Beyond electricity, blockchain activity may also involve significant water consumption linked to power generation and data-center cooling.

■ Public blockchains provide radical transparency, rendering transactions permanently visible and enabling extensive user profiling despite claims that pseudonymity alone protects **privacy.** Analysis of transaction histories, on-chain metadata, and related off-chain communications increasingly allow private firms and law-enforcement authorities to link blockchain addresses to real-world identities, raising concerns about large-scale surveillance. Privacy-enhancing tools, such as privacy coins and mixers, seek to mitigate traceability but create persistent tensions with regulatory and law-enforcement objectives.

CHAPTER 6

Legal Challenges

CHAPTER 6 TABLE OF CONTENTS

CHAPTER 6. LEGAL CHALLENGES 232
6.1. Is Blockchain Beyond the Reach of Law? 235
6.1.1. Code is Law 235
6.1.2 The "Lex Cryptographica" 238
6.1.3. The "Alegality" of Blockchain 238
6.2. The Uncertain Legal Significance of Blockchain Code 240
6.2.1. The DAO Case 241
6.2.1.A. The DAO hack 241
6.2.1.B. A Governance Decision 241
6.2.1.C. Doctrinal Significance 242
6.2.2. The Mango Markets Case 243
6.2.2.A. Legal Proceedings 244
6.2.2.B. Doctrinal Significance 246
6.2.3. Platypus 247
6.2.3.A. The Attack 247
6.2.3.B. Legal Proceedings 248
6.2.3.C. Doctrinal Significance 248
6.2.4. MEV and the Peraire-Bueno Case 249
6.2.4.A. What is MEV? 249
6.2.4.B. The Controversy About the Legality of MEV 250
6.2.4.C. The Peraire-Bueno Prosecution 252
6.3. The Debate on Developers' Liability 254
6.3.1. Rationale and Limits of Developers' Liability 254
6.3.2. Case Studies 256
6.3.2.A. Tulip Trading Case 256
6.3.2.B. The Uniswap Case (2023) 258
6.4. The Uncertain Legal Status of DAOs 259
6.4.1. Legal Classification Challenges for DAOs 260
6.4.2. Case Studies 261
6.4.2.A. DAOs as Incorporated Associations: The Ooki DAO case (2022) 261
1. Can a DAO Be Sued? 262
2. Are Governance Token Holders Liable for a DAO's Activities? 262
6.4.2.B. DAOs as General Partnerships 263
1. Sarcuni v. bZx DAO (2023) 263
2. Samuels v. Lido DAO (2024) 263
3. Houghton v Leshner (2023) 263
6.4.2.C. Conclusion 265
6.5. Legal Ambiguity Surrounding the Status of Smart Contracts 266
6.5.1. Conceptualizing Smart Contracts in Law 266
6.5.1.A. Smart Contracts and Smart Legal Contracts 267
6.5.1.B. Typology of Smart Contracts 269
6.5.2. The Legal Significance of Smart Contracts 271
6.5.2.A. Can Smart Contracts Be Legally Binding Agreements? 271
1. In the United States 271
a. Core Elements Required for Contract Formation 271
b. Formal Requirements 273
c. The UCC Amendments 273
2. In European Countries 276
3. The United Kingdom 277
6.5.2.B. Limitations of Smart Contracts 278
6.5.3. Case Study: Tornado Cash 280
6.5.3.A. What Is Tornado Cash? 280
6.5.3.B. Legal Proceedings 280
1. The Bar on Using Tornado Cash 280
2. The Trial Court's Decision 281
3. The Appeal 281
6.5.3.C. Doctrinal Significance 283
6.6. Indeterminacy in Jurisdiction, Forum, and Applicable Law for Blockchain Transactions 284

CHAPTER 6
TABLE OF CONTENTS (CONT'D)

6.6.1. Conflict-of-Laws and Jurisdictional Challenges in Blockchain Systems 284
6.6.2. Examples from U.S. Case Law 286
6.7. Compliance with Data Protection Frameworks 289
6.7.1. The Presence of Protected Personal Data on Blockchain Networks 289
6.7.2. Who Is the "Data Controller" on Blockchain Systems? 291
6.7.3. Can Data Subjects' Rights Effectively Be Guaranteed on Blockchain Systems? 293
KEY TAKEAWAYS 296

CHAPTER 6
Legal Challenges

The decentralized architecture of blockchain-based systems is often presented as a means to mitigating the risks of surveillance and control associated with centralized power structures. Yet this apparent freedom from control coexists with a paradox: Blockchain systems simultaneously function as code-based systems in which software defines what can and cannot be done within a given network. They are operationally autonomous vis-à-vis traditional forms of authority. As a result, some blockchain theorists argue that such systems may, in certain contexts, resist the application of legal norms altogether, a characteristic some scholars describe as "alegality." In practice, blockchain features raise complex and unprecedented legal questions that create persistent uncertainty.

This chapter examines these issues. It begins with an analysis of the scholarship addressing the claim that legal ordering is being displaced by blockchain code. It then turns to the principal legal challenges that contemporary legal systems encounter in responding to blockchain-related phenomena. These challenges include the legal status of blockchain code, questions of conflict of laws, the legal nature of smart contracts and decentralized organizations, and compliance with privacy requirements.

6.1. IS BLOCKCHAIN BEYOND THE REACH OF LAW?

Blockchain technology appears to embody the well-known principle that "code is law." In doing so, it gives rise to a new system of rules and governance —often referred to as *lex cryptographica*— which operates in a sphere that many describe as "alegal."

6.1.1. Code is Law

The debate concerning the regulation of blockchain technologies must be understood in continuity with the discourse on internet regulation in the 1990s.[1364] In his *Declaration of the Independence of Cyberspace*, John Perry Barlow articulated a vision of cyberspace as fundamentally resistant to conventional forms of state governance. Addressing governments directly, the *Declaration* famously asserted: "You have no sovereignty where we gather."[1365] At about the same time, David Post wrote that cyberspace is "unregulatable" to describe the inherent difficulties of governing the decentralized and transnational networks that compose the internet.[1366] Likewise, in their seminal 1996 article *Law and Borders: The Rise of Law in Cyberspace*, Post and David Johnson contended that cyberspace constituted a distinct jurisdictional space in which traditional, territorially

1364 *See generally* Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 Chi. Kent L. Rev. 1119 (1998), https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3143&context=cklawreview.

1365 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Elec. Frontier Found. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence. Barlow argued that cyberspace governed itself through its own "culture, ethics, or the unwritten codes" and envisioned the creation of "a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."

1366 David G. Post, *Anarchy, State, and the Internet: An Essay on Lawmaking in Cyberspace*, *in* Crypto Anarchy, Cyberstates, and Pirate Utopias, 207-08 (Peter Ludlow ed., 2001), https://monoskop.org/images/4/42/Ludlow_Peter_Crypto_Anarchy_Cyberstates_and_Pirate_Utopias.pdf ("[T]he aggregated choices of individual users seeking particular network rule sets most to their liking—will therefore, to a significant extent, determine the contours of the 'law of cyberspace.'").

based regulation was inadequate.[1367] They posited that new, non-territorial governance structures would emerge organically from within online communities. At the time, commentators emphasized several characteristics of cyberspace that challenged established regulatory mechanisms —its global and borderless nature, the pseudonymity it affords users, its distributed network architecture, and the rapid pace of technological change that continually outstrips legislative and regulatory developments.[1368]

In *Code and Other Laws of Cyberspace*, Lawrence Lessig famously advanced the view that in cyberspace "effective regulatory power [shifts] from law to code"[1369] and that "code is law."[1370] Lessig argued that the architecture of software functions as a regulatory modality alongside law, markets, and social norms, shaping and constraining individual behavior. In this sense, "code is law" because it performs normative and behavioral functions analogous to legal rules: computer code structures what users can and cannot do, much as physical architecture directs movement in the offline world. Lessig's argument was primarily descriptive: software architecture regulates behavior by embedding technical constraints.[1371] At the same time, he emphasized that the technical infrastructure of the internet is never neutral. Because someone always writes the code, it inevitably reflects particular values and design choices.[1372] This insight raised broader governance questions. If designing code is a form of governance, then architectural decisions may themselves carry political significance. Who designs the architecture of digital environments, under what institutional constraints, and according to which values?

Lessig further observed that the regulability of cyberspace depends on its architecture. Technical design choices —such as whether systems permit anonymity, require authentication, or allow the monitoring and traceability of user activity— determine the extent to which behavior online can be effectively regulated. Code can be modified to make cyberspace either "more regulable" or "less regulable," depending on the design choices of those who write it.[1373] Even if the decentralized and ostensibly "free" nature of the internet limits direct state control, governments and private actors may nonetheless exercise regulatory influence indirectly by shaping the architecture of digital systems.[1374] These ideas drew criticism from Robert C. Post. Post did not dispute that code embeds values and structures behavior. However, he rejected the conclusion that architectural choices should therefore be treated as political decisions requiring collective governance. In his view, the coexistence of multiple cyber-places, each structured by its own technical architecture and values, allows different normative environments to emerge without necessarily requiring collective decision making.[1375]

1367 David R. Johnson & David G. Post, *Law and Borders - the Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1378 (1996), https://yalelawtech.org/wp-content/uploads/2011/08/riseofcyberlaw.pdf.

1368 *See, e.g.*, *id.* at 1370-76; Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. Colo. L. Rev. 1203 (2000), https://ssrn.com/abstract=223462.

1369 Lawrence Lessig, Code And Other Laws of Cyberspace 206 (1999), https://lessig.org/product/code/.

1370 *Id.* at 6. *See also* Lawrence Lessig, *Lawrence Lessig on the Increasing Regulation of Cyberspace*, Harv. Mag. (Jan. 1, 2000), https://www.harvardmagazine.com/2000/01/code-is-law-html; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach,* Harv. L. Rev. 501-549 (1999), https://cyber.harvard.edu/works/lessig/LNC_Q_D2.PDF.

1371 Carla Reyes, Andrea Tosato & Andrew Hinkes, *Code is not Law*, SMU Dedman School of Law (2026), https://ssrn.com/abstract=6179104 (invoking H.L.A. Hart's positivist framework to show that code gains legal force only through recognition by positive law).

1372 "A code of cyberspace, defining the freedoms and controls of cyberspace, will be built. About that there can be no debate. But by whom, and with what values?", Lawrence Lessig, Code And Other Laws of Cyberspace, Version 2.0, 6 (2006), https://lessig.org/product/codev2/.

1373 Lessig, Code And Other Laws of Cyberspace, *supra* note 1369, at 109.

1374 *See Id.* at 43-44.

1375 Post argued that fundamental values could best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and their embodiments in code. In this view, what was needed was not a collective "plan" for cyberspace but a multitude of competing architectures from which individuals could freely choose —a diversity that the market was best placed to deliver. See objections to Lessig's ideas in David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, 52 Stan. L. Rev. 1439, 1441-43, 1454-58 (2000), https://doi.org/10.2307/1229518.

Several years later, in *Who Controls the Internet? Illusions of a Borderless World* (2006), Jack Goldsmith and Tim Wu challenged the thesis that cyberspace lies beyond the reach of state regulation. They showed that, by the early 2000s, territorial states had reasserted authority online by directing regulation toward intermediaries, such as "ISPs (Internet Service Providers), search engines, browsers, the physical network, and financial intermediaries."[1376] These actors, strategically situated at critical nodes of online infrastructure, provide effective points of control because they maintain a physical or economic presence within national jurisdictions.[1377] In practice, since the early 2000s, the Internet has evolved from a decentralized network of networks into a more centralized system that has increasingly been brought within the reach of law.[1378]

Much like in the early days of the internet, the rise of blockchain technology challenges both the effectiveness and the applicability of existing legal frameworks. However, the debate surrounding blockchain has taken a distinctive turn from earlier debates on internet governance: It is characterized by a discourse that frequently invokes the "supremacy of code."[1379] Commentators note that blockchain applications rely on specific technical and organizational architectures that place software protocols at the center of governance, even though human actors remain responsible for designing and updating the code *(See above section 3.1.1)*. Some blockchain advocates even declare that they place their "full faith in programming," investing their trust in transparent, auditable code rather than in long-standing legal, financial, or political institutions.[1380]

Within this context, blockchain scholarship has largely focused on distinguishing regulation *by law* from regulation *by blockchain code*. As a private regulatory framework, blockchain code —through the underlying protocol and smart contracts— defines what can and cannot be done within a given network, operating autonomously from traditional legal systems and institutional governance structures. Building on Lessig's principle that "code is law," some blockchain theorists argue that protocol rules and smart contracts constitute self-sufficient sources of normativity, often superseding legal institutions and discretionary human judgment.[1381] Some scholars, therefore, distinguish Lessig's "code is law" from the more blockchain-specific idea that "law is code",[1382] suggesting that legal rules may be drafted or implemented directly in computational form. Karen Yeung contrasts the traditional "code of law," enacted and enforced through national legal systems, with the emergent "code as law," embodied in the internal rules of blockchain architectures.[1383] Others have examined the self-executing quality of these systems, characterized by their capacity for the "code to run itself."[1384]

1376 *See* Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 69-74 (2006) https://scholarship.law.columbia.edu/books/175/.

1377 *Id*. at 68. *See also id.* at 81-82 (pointing out that the United States and France are more powerful controllers of intermediaries than Fiji and Ghana, for example, because they have more intermediaries within their borders to go after).

1378 *Id.* at 93-95 (using some of China's practices as an example of using national laws to target domestic intermediaries to implement the government's filtering).

1379 Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance*, 92 Geo. Wash. L. Rev. 1229, 1237 (2024), https://www.gwlr.org/wp-content/uploads/2024/12/92-Geo.-Wash.-L.-Rev.-1229.pdf; *see also* Kelvin F.K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 Int'l & Comp. L.Q. 135, 137–40 (2020) (calling "code is law" a "dangerous fallacy"), https://doi.org/10.1017/S0020589319000502.

1380 Ephrat Livni, *For Rules in Technology, the Challenge is to Balance Code and Law*, N.Y. Times (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/business/dealbook/cryptocurrency-code-law-technology.html

1381 Carla L. Reyes et al., view computer code as a form of "soft law." *See* Reyes et al., *Code is not Law, supra* note 1371, at 8.

1382 Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code*, 21 First Monday (2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

1383 Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code* of *Law and Code* as *Law*, 82 Mod. L. Rev. 207 (2019), https://www.jstor.org/stable/45220933.

1384 Wessel Reijers et al., *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, 40 Topoi 821 (2018), https://scispace.com/pdf/now-the-code-runs-itself-on-chain-and-off-chain-governance-g3a3xt7abo.pdf.

Some even believe that software could become "the sole determinant of enforceability."[1385]

6.1.2 The "Lex Cryptographica"

In 1998, Joel Reidenberg's influential article, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, introduced a foundational framework for understanding technology as a modality of regulation.[1386] Reidenberg argued that the architecture and design of technological systems embed rules that structure online behavior, thereby generating a quasi-legal order he termed "Lex Informatica."[1387] This regulatory layer operates alongside, and at times independently of, traditional legal frameworks.

Building on this insight, Aaron Wright and Primavera De Filippi introduced the concept of *lex cryptographia* to describe the governance structures emerging within blockchain networks, where participants are bound by "a set of rules administered through self-executing smart contracts and decentralized (and potentially autonomous) organizations."[1388] They conceptualized this regime as a form of technologically mediated private ordering, implemented through cryptographic protocols and enforced through technical execution rather than conventional legal instruments. They suggested that over time, "law and code may merge, so that the only way for people to infringe the law is to effectively break the code," [1389] implying that code might operate as a source of normative authority in its own right.

More recent scholarship by De Filippi and other blockchain theorists reinforces this account. They argue that "the technological design of blockchain technology —as a decentralized, transnational, and autonomous infrastructure— enables the emergence of a new autonomous legal order (so-called *lex cryptographica*)."[1390] On this view, *Lex cryptographica* represents a shift from traditional legal systems, which primarily regulate intermediaries, toward a model of governance that is autonomous, self-executing, and operates independently of established legal frameworks and institutional hierarchies.[1391]

6.1.3. The "Alegality" of Blockchain

At the same time, blockchain theorists also argue that blockchain systems, given their features, may be considered "alegal."[1392] "Alegality" is broadly understood among blockchain legal experts as the "capacity to be neither legal or illegal, the ability to exist and act in the

1385 Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 26 (Mar. 12, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

1386 *See generally* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553 (1998), https://ir.lawnet.fordham.edu/faculty_scholarship/42 (arguing that, "for network environments and the Information Society, however, law and government regulation are not the only source of rule making. Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations.")

1387 *Id.* at 568-76. "Lex Informatica" comes from a medieval merchant-created legal regime called "Lex Mercatoria."

1388 Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia,* 48 (Mar. 12, 2015) (unpublished manuscript), https://ssrn.com/abstract=2580664.

1389 *Id.* at 26

1390 Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 Pol'y & Soc'y 358, 363 (2022), https://academic.oup.com/policyandsociety/article/41/3/358/6529327 [hereinafter *Alegality*]. For a more skeptical view of *lex cryptographica* —that it displaces symbolic and imaginary basis of law with purely technical enforcement— See Katrin Becker, *Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, 33 Law & Critique 113, 118 (2022), https://pmc.ncbi.nlm.nih.gov/articles/PMC8733918/ ("[*lex cryptographia* initiates] a profound displacement of the traditional imagery and symbolic basis of law: not only does the coded lex cryptographia initiate a detachment from the traditional symbolic referent as its legal legitimacy").

1391 *See* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia, supra* note 1388, at 48-49.

1392 *See generally* De Filippi et al., *Alegality*, *supra* note 1390. *See also*, Primavera De Filippi, Morshed Mannan & Wessel Reijers, Blockchain Governance 127-133 (2024) [hereinafter *Blockchain Governance*].

interstices, or perhaps beyond or outside, the dominant . . . modes of legal production."[1393] In this perspective, blockchain systems are "neither legal nor illegal; they merely subsist outside of the legal realm."[1394]

Blockchain-based systems are autonomous vis-à-vis traditional forms of authority. Once deployed on a blockchain, the underlying protocol and the smart contract code operate independently of their original developers and may, as a result, evade the reach of legal norms. Transactions and agreements are enforced through the automatic and, in principle, immutable execution of code, without recourse to courts, lawyers, or other intermediaries. Because governance is embedded directly into the technical infrastructure, legal frameworks appear to be redundant. Blockchain governance constitutes a distinct, transnational legal order that operates independently from any single state's legal system, while remaining shaped by "*exogenous regulatory forces,*" such as market pressures and, indirectly, national legal frameworks.[1395]

Primavera De Filippi and her co-authors have identified seven key features of blockchain technology that render it particularly resistant to legal regulation: (1) decentralization, (2) transnationality, (3) tamper resistance, (4) pseudonymity, (5) absence of coercive enforcement mechanisms, (6) trustlessness, and (7) operational autonomy.[1396] Due to these characteristics, they write, "blockchain technologies can be said to challenge the *boundaries* of the legal order(s) in which they operate."[1397] Traditional legal systems, they contend, often lack the conceptual categories necessary to recognize, classify, or adequately describe blockchain-based activities. Blockchain systems exist outside the traditional legal categories to which regulation typically applies.[1398] In this sense, blockchain operations may be "invisible" to conventional legal analysis or may resist categorization within established legal taxonomies.

For example, Bitcoin disrupts the conventional distinction between legality and illegality within the domain of monetary and financial regulation. It introduces an alternative monetary system that may undermine the exclusive authority of legally recognized financial institutions that have existed for centuries. Bitcoin creates the possibility of becoming "another legality," a normative framework in which Bitcoin could be recognized as legal tender by a sovereign state —which El Salvador has already attempted, for example—[1399] despite it not being issued by a central bank. Another example is the legal concept of ownership. Blockchain systems rely on a technical idea of ownership that does not always align

1393 Vanja Hamzić, *Alegality: Outside and Beyond the Legal Logic of Late Capitalism*, *in* NEOLIBERAL LEGALITY 191 (Honor Brabazon ed., 2017) https://www.academia.edu/38575515/Alegality_Outside_and_Beyond_the_Legal_Logic_of_Late_Capitalism.

1394 De Filippi, Mannan & Reijers, *Blockchain Governance*, *supra* note 1392, at 125. Additional note: Because *alegal* and *alegality* lack dictionary recognition, we initially used quotation marks to signal their novelty, then omitted them.

1395 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance*, *supra* note 1379. The authors largely build on Lawrence Lessig's four modalities of regulation: code/architecture, market, social norms and, finally, law. See: Lawrence Lessig, *The Laws of Cyberspace*, (Taiwan Net conference, 1998); LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (1999) https://lessig.org/product/code/; CODE: AND OTHER LAWS OF CYBERSPACE VERSION 2.0 (2006), Chapter 7 (What Things Regulate), https://lessig.org/product/codev2/.

1396 De Filippi et al., *Alegality*, *supra* note 1390, at 359.

1397 *Id.*

1398 But note that self-governing blockchain systems using smart contracts "alone cannot govern communities; traditional constitutions and declarations of rights are still crucial for good governance." Joshua Tan et al., *Constitutions* of *Web3*, METAGOV, https://constitutions.metagov.org/article (last visited Jan. 15, 2026).

1399 De Filippi et al., *Alegality*, *supra* note 1390, at 364. *See* the Salvadoran law that established Bitcoin as a legal tender in the country in 2021, L. 57, June 9, 2021, [431] DIARIO OFICIAL [D.O.] 13-15 (El Sal.). However, in 2025, El Salvador agreed to abolish Bitcoin as legal tender partly because of pressure from the International Monetary Fund and because it had never become popular among the public. *See Bitcoin Is No Longer Legal Tender in El Salvador*, THE DIGIT. WATCH (Feb. 7, 2025), https://dig.watch/updates/bitcoin-is-no-longer-legal-tender-in-el-salvador; Rebecca Beyer, *El Salvador Adopted Bitcoin as an Official Currency; Salvadorans Mostly Shrugged*, YALE INSIGHTS (Jan. 29, 2024), https://insights.som.yale.edu/insights/el-salvador-adopted-bitcoin-as-an-official-currency-salvadorans-mostly-shrugged (describing research by David Argente and Diana Van Patten showing that Bitcoin never really took off among Salvadorans); *see also* Kara Bruce, Christopher K. Odinet & Andrea Tosato, *The Private Law of Stablecoins* (2023), https://ssrn.com/abstract=4191646.

with legally recognized forms of ownership. In practice, whoever holds the private cryptographic key to a Bitcoin wallet can fully control the assets inside it, even if that person is not the wallet's legal owner under applicable law. This gap between technical and legal possession can lead to a fundamental misalignment between how blockchain-based systems work and how the legal system defines property rights.[1400]

Blockchain systems may also facilitate conduct that violates the normative boundaries established by the legal systems in which they are deployed. The pseudonymity of blockchain users complicates regulatory enforcement by making it difficult to identify the individuals or entities subject to orders or sanctions arising from unlawful transactions.[1401] More critically, blockchain records' immutability and tamper-resistant nature mean that governments cannot easily police blockchain networks. Instead, enforcement happens outside the blockchain, through legal actions against individuals or entities who control the relevant assets or provide access to them. Authorities can seize private keys, freeze assets on regulated exchanges, or block access to these platforms. Regulators may disable centralized interfaces or front-end platforms that provide access to blockchain networks. But even then, the decentralized applications that run on blockchains and enable some of this illicit activity usually remain functional and can be re-accessed once new access points are created. Overall, the alegal nature of blockchain systems and the primacy of code raise the risk that these systems could evolve into hazardous environments.[1402]

These theoretical debates over whether blockchain systems are truly beyond law's reach are more than academic exercises. As the following sections demonstrate, courts and regulators worldwide are grappling with concrete legal questions arising from blockchain exploits, developer responsibilities, organizational structures, contractual relationships, jurisdictional boundaries, and privacy compliance. The remainder of this chapter examines how legal systems are responding to these challenges in practice.

6.2. THE UNCERTAIN LEGAL SIGNIFICANCE OF BLOCKCHAIN CODE

How have courts addressed the legal significance of blockchain code when vulnerabilities are exploited? The following four cases —*The DAO, Mango Markets, Platypus,* and *Peraire-Bueno*— illustrate the central tension between the "code is law" approach and traditional legal concepts of fraud, market manipulation, theft, and liability. In these cases, users exploited weaknesses in the underlying code to extract substantial funds, thereby raising the question of whether conduct that complies with a protocol's technical rules can nonetheless be deemed unlawful. However, these cases have not provided a definitive answer to whether the exploitation of such flaws constitutes an unlawful act under existing legal frameworks and what standards of conduct apply to blockchain participants.

1400 De Filippi et al., *Alegality*, *supra* note 1390, at 364-66; Andrea Tosato & Christopher K. Odinet, *Digital Assets and the Property Question*, 78 FLA. L. REV. (forthcoming 2026), https://ssrn.com/abstract=5151907*; see also* Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607 (2022), https://scholarship.law.ufl.edu/flr/vol74/iss4/2.

1401 Georgios Dimitropoulos, *The Law of Blockchain*, 85 WASH. L. REV. 1117, 1182 (2020), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=5129&context=wlr.

1402 For example, see the effort to protect Ethereum's transactions from "predator" bots that invisibly monitor and exploit pending transactions outside of traditional legal oversight. Dan Robinson & Georgios Konstantopoulos, *Ethereum Is a Dark Forest*, PARADIGM (Aug. 28, 2020), https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest.

6.2.1. The DAO Case

6.2.1.A. The DAO Hack

The DAO was established in April 2016 as a decentralized investment vehicle implemented through a smart contract on the Ethereum blockchain. At the time, Ethereum was only one year old. Its primary objective was to raise cryptocurrency to finance blockchain-based projects and to distribute any resulting profits to its investors. When token holders voted in favor of a project, the smart contract was programmed to automatically transfer funds to the project initiator. In the absence of a centralized authority, The DAO operated through a technical infrastructure composed entirely of Ethereum smart contracts. Its operational rules were encoded, automated, and enforced exclusively by software. The terms of The DAO explicitly stated that "by creating DAO tokens through interaction with The DAO's smart contract code, you expressly agree to all of the terms and conditions set forth in that code."[1403] The underlying code was published openly on GitHub.

The DAO represented an early experiment in collective, automated governance.[1404] The protocol allocated governance rights in proportion to each investor's financial contribution, allowing token holders to participate directly in decision-making processes. *Contractors,* either individuals or organizations, sought funding for proposed projects. They submitted detailed proposals to The DAO, outlining a project plan and requesting funds. Slock.it, the German startup that created The DAO, pre-selected a group of individuals called *curators.* Appointed before The DAO's launch, the curators included several prominent members of the Ethereum community, including Vitalik Buterin and Gavin Wood. This group of trusted community members was responsible for maintaining a white list of addresses eligible to receive funds and for verifying the integrity of proposals before these were submitted to a vote by all DAO token holders. Once a proposal obtained the requisite majority and quorum, the associated smart contract automatically transferred funds to the approved project.

Within weeks of its launch, The DAO attracted more than $150 million in ETH from over 11,000 investors.[1405] However, a vulnerability in its smart contracts quickly became a point of concern. Before corrective measures could be taken, an attacker exploited the flaw and siphoned one-third of The DAO's holdings of ETH –worth approximately $50-60 million– into a segregated account under the attacker's control.[1406] Given that The DAO held about 14% of all circulating ETH at the time, the very foundation of the fledgling Ethereum platform was threatened.[1407]

6.2.1.B. A Governance Decision

The Ethereum community had a brief window to act, as the stolen funds were locked in a separate, attacker-controlled child DAO, subject to a 28-day waiting period imposed by The DAO's own split mechanism, during which the attacker could not withdraw them. Rather than seek judicial intervention, the Ethereum community made a collective decision: A majority of participants in the Ethereum network, not just The DAO's members, voted to implement a hard fork (a protocol update that created a new blockchain with an

1403 *The DAO*, Explanation of Terms and Disclaimer (2016), https://web.archive.org/web/20160513073743/https://daohub.org/explainer.html.

1404 As the founders put it, their goal was to "blaze a new path in business for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of unstoppable code." Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 34-81207, 117 SEC Docket 745 (July 25, 2017) [hereinafter SEC Investigative Report: The DAO], https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

1405 *Ethereum DAO Hack*, Bitstamp Learn (July 17, 2023), https://www.bitstamp.net/learn/crypto-101/ethereum-dao-hack/. Robert Morrison, Natasha C. H. L. Mazey & Stephen C. Wingreen, *The DAO Controversy: The Case for a New Species of Corporate Governance*, 2 Frontiers Blockchain 1, 6 (2020), https://doi.org/10.3389/fbloc.2020.00025

1406 Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 34-81207, 117 SEC Docket 745 (July 25, 2017). https://www.sec.gov/files/litigation/investreport/34-81207.pdf

1407 Bitstamp Learn, *supra* note 1405.

altered transaction history), reversing the hack and returning funds to investors. A majority of miners and node operators adopted this forked chain, which retained the name "Ethereum" and successfully reversed the theft. A minority refused the fork and continued operating the original, unaltered blockchain, which became known as "Ethereum Classic." On Ethereum Classic, the attacker retained control of the diverted funds, though the overwhelming majority of community value and network activity migrated to the forked Ethereum chain where investors were made whole. As a result, the attacker preserved nominal control over the assets but could only extract value gradually, under scrutiny, and at a likely discount.[1408]

The fork was controversial within the blockchain community. It blurred the line between project-level governance (The DAO) and protocol-level governance (Ethereum itself). Moreover, it undermined the fundamental principle of blockchain immutability which provides that, once recorded, transactions should be irreversible.[1409] Adhering strictly to the "code is law" ethos would have left investors with no effective remedy and could have irreparably damaged Ethereum's credibility. Abandoning the core precepts of irreversibility and an immutable ledger violated one of the animating purposes of blockchain in the first place. While the hard fork successfully reversed the financial losses resulting from the attack, it also revealed that the security and governance of blockchain systems ultimately depend on collective, extra-code decision making.[1410]

6.2.1.C. Doctrinal Significance

Without the technical possibility of modifying the blockchain through the hard fork, investors in The DAO would likely have lost approximately $60 million, with no effective legal recourse. The fork, however, left unresolved the broader legal questions raised by the incident. The DAO had no formal legal status: It was not incorporated as a company, a partnership, or any other legally recognized entity in any jurisdiction. Consequently, the rights and obligations of its participants were not defined under any established legal framework. The absence of a centralized authority, combined with the pseudonymity of participants, made it virtually impossible to identify any person or entity that could be held legally liable.

More fundamentally, the episode raised the question of the legal implications of code-based governance. The DAO's documentation explicitly stated that its terms were defined by the smart contract code,[1411] and participants had agreed that this code would govern their rights and obligations. Yet, it remained unclear whether they had implicitly accepted the risk of vulnerabilities in the open-source software, including the possibility that their tokens might be misappropriated.[1412]

The attacker publicly argued that the diversion of funds was not wrongful or classifiable as theft, since the hacker had exploited only the code as written.[1413] The attacker claimed that these actions were permissible under the rules of the smart contract and even warned of legal

1408 See, e.g., Cryptopedia, *The DAO Hack Explained*, Gemini (Dec. 4, 2025) https://www.gemini.com/cryptopedia/the-dao-hack-makerdao (noting that although the funds were restored on the forked Ethereum chain, the attacker "did not lose out entirely," as the stolen tokens "remained in their possession on the Ethereum Classic chain" and were valued at approximately $8.5 million in ETC in the months following the attack).

1409 Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. Times (June 17, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html.

1410 While "the idea of a perfectly neutral, self-patrolling system is appealing, high-profile mishaps have cast doubt on the idea that code is a sufficient form of regulation on its own—or that it is immune to human mistakes and manipulation." Ephrat Livni, *For Rules in Technology, the Challenge is to Balance Code and Law*, N.Y. Times (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/business/dealbook/cryptocurrency-code-law-technology.html.

1411 Matt Levine, *Blockchain Company's Smart Contracts Were Dumb*, Bloomberg View (June 17, 2016), https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb.

1412 Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 Stan. Tech. L. Rev. 198, 218-19 (2018) (considering the "code is the contract" approach in the context of The DAO controversy), https://law.stanford.edu/wp-content/uploads/2018/09/Kolber_LL_20180910.pdf.

1413 The attacker published an anonymous note to the DAO and the Ethereum community, see "The Attacker," *An Open Letter*, Pastebin (June 18, 2016), https://pastebin.com/CcGUBgDG.

action against any attempt at retaliation. Nonetheless, the diversion of funds contradicted the spirit in which The DAO had been established —to finance blockchain-based projects— and amounted to a misappropriation of participants' assets.[1414] This dispute triggered intense debate within the Ethereum community over whether the incident constituted theft —because it subverted the parties' shared expectations— or was a legitimate, even if ethically questionable, application of the maxim that "code is law."[1415] Had the attacker been identified, any criminal prosecution would have depended on whether exploiting a flaw in a smart contract could constitute a prosecutable offense under existing law.

To further complicate matters, no jurisdiction had clear legal authority over the dispute. The DAO existed as a decentralized software protocol, replicated across thousands of nodes on the Ethereum network. It was not registered in any jurisdiction and lacked a physical presence for several reasons: the absence of a centralized operator, the pseudonymity of most participants, the autonomous nature of its transaction mechanisms, and the lack of any tangible assets being exchanged. Even if a court had asserted jurisdiction and found that the diversion of ETH constituted theft, a judgment ordering the return of funds would have been nearly impossible to enforce. The attacker's identity was unknown and, even if identified, the decentralized architecture of blockchain offered no mechanism for court-ordered seizure of cryptocurrency.[1416]

Finally, it remained uncertain whether The DAO's developers could have been held legally responsible for defects in the code[1417] or whether token holders themselves might bear liability as participants in a collective arrangement.[1418] If The DAO were considered a partnership or a contractual arrangement, it is unclear whether liability would be collectively borne by all token holders or limited to certain individuals. The pseudonymity of The DAO's participants further complicated these legal questions by making the identification of responsible parties particularly difficult.

6.2.2. The Mango Markets Case

In 2022, a decentralized exchange called Mango Markets, operating on the Solana blockchain, was targeted by a trader who manipulated the price of its native token through a series of coordinated actions *(See Figure 43)*. The loss was approximately $116 million, according to the SEC.[1419] The attacker, who later identified himself as Avraham Eisenberg, manipulated the price of the MNGO token by executing large spot trades on a set of external exchanges, whose prices were incorporated into Mango Markets' oracle to determine the value of MNGO perpetuals and related collateral. What made this manipulation particularly notable was Eisenberg's public statement afterward, claiming his actions were a "highly profitable trading strategy."[1420] He publicly justified his actions as "legal open market actions, using the protocol as designed, even if the development team did not fully

1414 *See* Morrison, Mazey & Wingreen, *supra* note 1405, at 6, 7.

1415 *Id*. (many people thought that it was not a "hack"—"[r]ather, one member [merely] found a loophole in the rules that, ethics aside, he was entitled to exploit").

1416 Andrew W. Balthazor, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. Rev. 1207, 1209 (2019), https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1410&context=lawreview (explaining that because no central authority can revoke a transaction and assets are controlled solely by private keys, a court judgment is often unenforceable against a thief who refuses to—or cannot be found to—transfer the funds).

1417 Laila Metjahic, *Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*, 39 Cardozo L. Rev. 1533, 1536 (2018), https://cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf.

1418 *See* Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4 Stan. J. Blockchain L. & Pol'y 1, 14-18 (2021), https://stanford-jblp.pubpub.org/pub/rise-of-daos.

1419 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Avraham Eisenberg with Manipulating Mango Markets' "Governance Token" to Steal $116 Million of Crypto Assets (Jan. 20, 2023), https://www.sec.gov/newsroom/press-releases/2023-13; *Oracle Manipulation Attacks Are Rising, Creating a Unique Concern for DeFi*, Chainalysis (Mar. 7, 2023), https://www.chainalysis.com/blog/oracle-manipulation-attacks-rising/.

1420 Avraham Eisenberg (@avi_eisen), X.com (Oct. 15, 2022, 12:48 PM), https://x.com/avi_eisen/status/1581326197241180160.

anticipate all the consequences of setting parameters the way they are."[1421]

Following the exploit, Eisenberg entered negotiations with the Mango DAO, the protocol's decentralized governance body. As part of the "settlement" with the Mango DAO, he agreed to return approximately $67 million, while retaining $47 million as a retroactive "bug bounty,"[1422] pursuant to a governance vote approving the arrangement.[1423] As stated in a complaint in one of the legal actions against Eisenberg, Mango Markets was able to reimburse its users affected by Eisenberg's actions using its treasury funds and the funds that he returned.

6.2.2.A. Legal Proceedings

Several legal actions against Eisenberg ensued:

- The U.S. Department of Justice (DOJ), in a criminal case, charged Eisenberg with commodities fraud, commodities manipulation, and wire fraud, alleging that he withdrew money with no intention of repaying.[1424]
- A few weeks later, the Commodity Futures Trading Commission (CFTC) also sued Eisenberg for the same conduct, alleging that his "manipulative and deceptive scheme" inflated the price of "perpetual futures," violating the Commodity Exchange Act.[1425]
- Meanwhile, the U.S. Securities and Exchange Commission (SEC) brought an enforcement action under the Exchange Act, alleging fraud and market manipulation.[1426]
- Finally, Mango Labs LLC, the company behind Mango Markets, sued Eisenberg for conversion of property, fraud, and unjust enrichment. It argued that Eisenberg misrepresented to Mango Markets that "he was a legitimate market participant." It said he unjustly took over millions in cryptocurrency, causing Mango Labs damages.[1427]

The criminal case brought by the DOJ went forward, while the remaining legal actions were stayed ("paused") pending the resolution of the criminal case. In December 2022, Eisenberg was indicted by a grand jury and arrested in Puerto Rico; he was subsequently tried in the federal court for the Southern District of New York.[1428] During the proceedings, Eisenberg invoked traditional defenses, including the suppression of evidence, exclusion of expert

---

1421 *Id.*

1422 Press Release, U.S. Commodity Futures Trading Comm'n, *CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 Million from Mango Markets, a Digital Asset Exchange* (Jan. 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8647-23.

1423 Anthony Cuthbertson, *Crypto exchange hacker nets $114m but returns $67m to pay back customers*, The Independent (Oct. 17, 2022), https://www.the-independent.com/tech/crypto-exchange-hack-mango-markets-cyber-security-b2204210.html.

1424 Interestingly, the DOJ alleged that "virtual currencies, such as USDC, are 'commodities' under the Commodity Exchange Act." Sealed Complaint at 6, United States v. Eisenberg, No. 1:23-cr-00010-RMB (S.D.N.Y. Dec. 23, 2022), ECF No. 1 [hereinafter DOJ Eisenberg Complaint].

1425 *See* Complaint at 8-13, U.S. Commodity Futures Trading Comm'n v. Eisenberg, No. 1:23-cv-00173-LGS (S.D.N.Y. Jan. 9, 2023), ECF No. 1 [hereinafter CFTC Eisenberg Complaint], https://www.cftc.gov/media/8046/enfeisenbergcomplaint010923/download. This action is notable because the CFTC argued that Eisenberg's conduct fell within the scope of the Commodity Exchange Act as conduct involving "swaps," a statutorily defined category of derivatives transactions involving the exchange of financial exposures linked to commodities (See Press Release, U.S. Commodity Futures Trading Comm'n, *CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate over $110 Million from Mango Markets, a Digital Asset Exchange* (Jan. 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8647-23). The government further alleged that Eisenberg defrauded Mango Markets by concealing "the fact that he was on both sides of this transaction" and conducting a manipulative wash transaction—i.e., a transaction with the goal not to gain or lose economically from the trade itself, but rather to create a false or misleading appearance of market activity or demand. CFTC Eisenberg Complaint, at 9.

1426 To show that the Exchange Act applied, the SEC argued that MNGO tokens were securities under the so-called *Howey* test (See below Figure 55) because Mango Market users invested money in a common enterprise with a reasonable expectation of profits. *See* SEC Eisenberg Complaint, paras. 43-44, 66, U.S. Sec. & Exch. Comm'n v. Eisenberg, No. 1:23-cv-00503-LGS (S.D.N.Y. Jan. 20, 2023), ECF No. 1, https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-13.pdf [hereinafter SEC Eisenberg Complaint].

1427 *See* Complaint at paras. 41-43, 83-87, Mango Labs, LLC v. Eisenberg, No. 1:23-cv-00665-LJL (S.D.N.Y Jan. 25, 2023), ECF No. 1, https://www.courtlistener.com/docket/66760250/1/mango-labs-llc-v-eisenberg/ [hereinafter Mango Eisenberg Complaint]. Even though the Mango DAO technically agreed not to pursue any legal action against Eisenberg, the complaint alleged that Eisenberg's "settlement" to return only part of the money he took and keep the rest as "bug bounty" was unenforceable because it was offered to the Mango DAO under duress. *See* Cuthbertson, *supra* note 1423.

1428 Press Release, U.S. Att'y's Off., S.D.N.Y., Alleged Perpetrator of $100 Million Crypto Market Manipulation Scheme to Make Initial Appearance in the Southern District of New York (Feb. 2, 2023), https://www.justice.gov/usao-sdny/pr/alleged-perpetrator-100-million-crypto-market-manipulation-scheme-make-initial.

testimony, and due process.[1429] Eisenberg unsuccessfully argued that "perpetual futures" are not "swap" transactions covered by the Commodity Exchange Act.[1430] He also raised a few defenses that could be interpreted as the "code is law" defenses: He said his actions were within Mango's smart contract's terms and that he did not manipulate the system beyond its coded design. In other words, Eisenberg claimed that "his 'alleged conduct was fully permitted on the Mango Markets platform, and he deceived no one.'"[1431]

Despite Eisenberg's best efforts, the judge was not convinced and found the government's allegations sufficient. The judge treated transactions involving cryptocurrency similarly to regular financial transactions on the market, finding that the MNGO Perpetuals constituted "mixed swaps" subject to the Commodity Exchange Act. The judge noted that Eisenberg failed to disclose to Mango Markets important information about his plans, that his actions artificially increased the "perpetual futures" price, and that he withdrew the cryptocurrency with no intention of repaying it.[1432] In April 2024, the jury convicted Eisenberg on all three counts, finding him guilty of commodities fraud, commodities manipulation, and wire fraud.[1433]

However, Eisenberg moved for a post-trial acquittal. He successfully argued that the Southern District of New York was not a proper venue for the commodities charges — commodities fraud and commodities manipulation.[1434] The judge agreed. Although financial crimes often have connections to multiple jurisdictions, federal venue rules require that prosecution be brought where the offense was committed or had its effects. Here, Eisenberg resided in Puerto Rico, and his limited contacts with New York were insufficient to establish venue in that district.[1435] As a result, the court vacated his convictions on the first two counts on procedural grounds.[1436] At the same time, the court indicated that the evidence was sufficient to support findings of commodities fraud and manipulation, noting that Eisenberg had artificially inflated the price of MNGO perpetual futures to inflate the value of his collateral position and extract funds from the protocol's treasury. This leaves open the possibility that the government could pursue these charges in a proper venue.[1437]

On the wire fraud count, Eisenberg also moved for acquittal on the ground of insufficient evidence. In a post-trial ruling, the court agreed that the government had failed to establish a material misrepresentation. Eisenberg argued that his conduct was not prohibited by Mango Markets, which operated as a "permissionless and automatic" protocol. The court emphasized that the platform had no "rules, instructions, or prohibitions about borrowing," no prohibition on manipulation, no formal repayment obligation, and no requirement to maintain sufficient collateral.[1438] The terms to which users agreed — to use the platform at their own risk— were just too vague

1429 *See* United States v. Eisenberg, No. 23-cr-10 (AS), 2023 U.S. Dist. LEXIS 225952, at 19-21 (S.D.N.Y. Dec. 18, 2023). *See generally* United States v. Eisenberg, 707 F. Supp. 3d 406 (S.D.N.Y. Dec. 18, 2023).

1430 *See* Eisenberg, 2023 U.S. Dist. LEXIS 225952, at 35-48.

1431 *Id.* at 17.

1432 *Id.* at 15-18.

1433 Press Release, U.S. Department of Justice, Man Convicted for $110M Cryptocurrency Scheme (April 18, 2024), https://www.justice.gov/archives/opa/pr/man-convicted-110m-cryptocurrency-scheme; Matthew Beville & Alexandrea L. Rahill, *Reversals of Fraud Charges Highlight Difficulties in Bringing Market Manipulation Cases*, WilmerHale (Aug. 4, 2025), https://www.wilmerhale.com/en/insights/client-alerts/20250804-reversals-of-fraud-charges-highlight-difficulties-in-bringing-market-manipulation-cases.

1434 *See* United States v. Eisenberg, No. 23-cr-10 (AS), 2025 U.S. Dist. LEXIS 98813, at 7 (S.D.N.Y. May 23, 2025).

1435 *See id.* at 10.

1436 *Id.* at 82-83. Because these two convictions were vacated on procedural grounds, the government could technically re-indict and bring the case against Eisenberg in a proper venue. *See generally* Ball v. United States, 163 U.S. 662 (1896); Smith v. United States, 599 U.S. 236 (2023).

1437 *See id.* at 39-48 for the court's justification.

1438 The court said, "On a platform with no rules, instructions, or prohibitions about borrowing, the government needed more to show that Eisenberg made an implicit misrepresentation by allowing the algorithm to measure the actual value of his collateral." *Id.* at 77-78.

to give rise to enforceable obligations.[1439] In this context, the court rejected the government's argument that Eisenberg had implicitly represented that his collateral had not been manipulated and was genuinely valuable. This distinction reflects the different elements required for each offense: commodities manipulation turns on the artificial distortion of prices, whereas wire fraud requires an affirmative misrepresentation directed at a victim — a threshold the court found unmet on these facts. Although the court found that Eisenberg had engaged in market manipulation, it concluded that he had not made a material misrepresentation sufficient to sustain a wire fraud conviction. The combined effect of these post-trial rulings was the vacatur of all three of Eisenberg's convictions, leaving the criminal case against him, as it relates to the Mango Markets exploit, without any surviving conviction as of May 2025. However, the government has since appealed the wire fraud acquittal on July 23, 2025, and the commodities charges are not, as a matter of law, beyond the reach of re-prosecution in a proper venue.

6.2.2.B. Doctrinal Significance

The *Mango Markets v. Eisenberg* litigation exposed a deep divide between two opposing perspectives on code execution and legal responsibility. On one side, regulators and part of the blockchain community reject the notion that "code is law:" The mere fact that a protocol permits a transaction does not render it lawful or legitimate. Even actions that are technically feasible within a protocol's rules may give rise to civil or criminal liability when they involve deception, market manipulation, or the strategic exploitation of design vulnerabilities.[1440]

On the other side, proponents of the "code is law" position maintain that conduct complying with a protocol's own rules should not give rise to liability: users who interact with a system as designed are entitled to rely on the code as the governing framework, without exposure to legal standards imported from regulated markets. The normative and legal boundaries of blockchain-based financial activity nonetheless remain deeply unsettled. Courts are, therefore, compelled to bridge this gap by applying traditional doctrines of fraud and market manipulation —originally developed for conventional markets— to decentralized environments in which conduct is mediated by code rather than by intermediaries. This process is inherently difficult. A central question remains unresolved: Where should the line be drawn between legitimate strategic behavior on the blockchain that "outsmarts" a system and unlawful deception or misrepresentation, particularly when the code and the platform's internal rules serve as the primary reference points for assessing conduct?

The Eisenberg proceedings, inconclusive as of the time of writing, offered limited and mixed doctrinal guidance: while the court preserved factual findings that artificial price inflation constituted unlawful market manipulation, it simultaneously rejected the proposition that protocol-based trading without explicit misrepresentation could sustain a wire fraud conviction — leaving the normative boundaries of permissible conduct on decentralized platforms substantially unresolved. The government's appeal of the wire fraud acquittal signals that this doctrinal tension is far from settled, and that the question will receive further judicial consideration.

1439 "There was no evidence . . . that Mango Markets required any user to promise that they would repay funds as a condition of borrowing against their assets." *Id.* at 71.

1440 The Mango Markets controversy exemplifies market manipulation. An example of exploitation of smart-contract vulnerabilities is the case of Shakeeb Ahmed, who pled guilty to computer fraud for reverse-engineering and then hacking two cryptocurrency exchanges and stealing $12 million worth of cryptocurrency. *See* Press Release, U.S. Att'y's Off., S.D.N.Y., *Former Security Engineer Sentenced to Three Years in Prison for Hacking Two Decentralized Cryptocurrency Exchanges* (Apr. 12, 2024), https://www.justice.gov/usao-sdny/pr/former-security-engineer-sentenced-three-years-prison-hacking-two-decentralized.

Finally, the case highlights a broader dilemma for decentralized platforms such as *Mango Markets*: They must either accept the risks inherent in blockchain's alegal autonomy or mitigate them by reinforcing code-based governance with contractual and compliance mechanisms rooted in legal norms.

6.2.3. Platypus

6.2.3.A. The Attack

In February 2023, a young French developer, assisted by his brother, exploited a design flaw in the decentralized finance (DeFi) platform Platypus Finance, built on the Avalanche blockchain. The flaw concerned the collateral verification logic of Platypus's smart contract, which momentarily recognized deposits as valid collateral *before* updating the user's debt position.

FIGURE 47.

The Platypus exploit (2023)

The Platypus exploit began when the attacker used a "flash loan" —an instant loan that does not require collateral and must be repaid within a single blockchain transaction— to borrow approximately 44 million USDC through the Aave protocol.[1441] The borrowed funds were temporarily deposited into Platypus' liquidity pool to appear as collateral for generating the platform's stablecoin, USP. However, due to an implementation error in the collateral verification logic, the system validated the deposit *before* updating the user's debt position. This sequencing error —commonly known as a "check-before-effect" bug— created a brief but exploitable state in which the attacker's position appeared fully collateralized even though no actual collateralization had occurred.

The attacker then invoked the platform's "emergency withdraw" function, extracting approximately $9 million in crypto-assets from Platypus without proper collateralization. Once the $9 million in crypto-assets had been withdrawn, the attacker released the initial 44 million USDC deposit from Platypus and immediately repaid the Aave flash loan, thereby closing the debt. In a second phase, the funds were transferred to multiple wallets to launder the proceeds. The attacker was able to obscure the trail of transactions by switching between blockchains and by using a crypto mixer to mask the origin of the assets.[1442]

1441 *See* Louis Adam, *Piratage de la plate-forme de cryptomonnaies Platypus : les deux accusés relaxés par la justice [Hacking of the Platypus Cryptocurrency Platform: The Two Accused Acquitted by the Courts]*, Le Monde (Dec. 1, 2023), https://www.lemonde.fr/pixels/article/2023/12/01/piratage-de-la-plate-forme-de-cryptomonnaies-platypus-les-deux-accuses-relaxes-par-la-justice_6203417_4408996.html.

1442 Maximilien Prué, *Pourquoi 2 hackers français ont été relaxés pour l'attaque à 9,5 millions de dollars sur le protocole Platypus ? [Why Were Two French Hackers Acquitted for the $9.5 Million Attack on the Platypus Protocol?]*, Cryptoast (Dec. 5, 2023), https://cryptoast.fr/hack-crypto-2-francais-relaxes-attaque-9-5-millions-dollars-sur-protocole-platypus.

6.2.3.B. Legal Proceedings

The attacker was prosecuted for fraudulent access to and continued use of an automated information system, as well as fraud and money laundering. (His brother was tried as an accomplice for receiving stolen property.) At trial, the attacker did not dispute the facts but claimed to have acted in good faith as an "ethical hacker."[1443] He asserted that his intention was to safeguard "endangered funds" and return them to the protocol in exchange for a "white hat" bonus of around 10%. Similar to the defendant in the Mango case *(See Section 6.2.2.)*, the attacker in the Platypus case argued that he had not "hacked" an internal system but merely interacted with the publicly accessible smart contract interface —exploiting a design flaw rather than surreptitiously infiltrating a protected system.

On December 1, 2023, the Paris trial court (*Tribunal judiciaire de Paris,* 13^{e} *chambre correctionnelle*) acquitted the defendants of all charges under French criminal law.[1444] The court characterized the exploit as "unethical behavior" that took advantage of a coding error in Platypus' smart contract to withdraw funds. However, it held that, despite the actions being harmful, they did not give rise to criminal liability under existing statutory provisions but, instead, created a civil debt owed to Platypus in connection with the flash loan. The court observed that the flaw lay in the design of the contract code itself, rather than in any concealed intrusion or breach. It further found that the attackers' use of Platypus' "emergency withdrawal" function —the smart contract containing the exploited vulnerability— did not constitute fraud. Because the fraud charges could not be sustained, the tribunal also dismissed the related counts of money laundering and receiving stolen property.

On appeal, the Paris Court of Appeal upheld the acquittal.[1445] The court found that the defendant had merely interacted with the Platypus smart contract as an ordinary user, according to Platypus's terms of service. The judges further noted that the defendant had identified a flaw in the Platypus script —a flaw which performed the necessary verifications for fund withdrawals in an incorrect sequence— thus verifying collateral only after approving the withdrawal.[1446] The judges also found that Platypus (the company) was not the direct victim. They said the funds taken were that of the users who deposited them on the platform, so there was no fraudulent taking of property belonging to Platypus. They concluded that the existence of an error in the code of the smart contract, coupled with the "emergency withdrawal" function, made the "attack" possible.[1447]

6.2.3.C. Doctrinal Significance

In the *Platypus* case, the French court held that the defendant had merely exploited pre-existing vulnerabilities within the system. The court noted that the attacker had not breached Platypus' internal infrastructure but had interacted solely with the project's publicly accessible smart contract. Consequently, his conduct was not classified as hacking or criminal activity, and all charges were dismissed.

1443 Camomile Shumba, *Duo Behind $9M Platypus Exploit Acquitted by Paris Court: Report*, CoinDesk (Dec. 4, 2023), https://www.coindesk.com/policy/2023/12/04/duo-behind-9m-platypus-exploit-acquitted-by-paris-court-report (last visited Jan. 15, 2026).

1444 Eur. Union Agency for Crim. Just. Coop., Cybercrime Judicial Monitor Issue 9 – July 2024, at 14 (2024); Zack Abrams, *Platypus Finance Hackers Cleared of Criminal Charges: Le Monde*, THE BLOCK (Dec. 3, 2023), https://www.theblock.co/post/265797/platypus-finance-hackers-cleared-of-criminal-charges-le-monde.

1445 Gabriel Thierry, *Finance décentralisée : la Cour d'appel de Paris confirme le jugement de première instance dans l'affaire* Platypus *[Decentralized Finance: Paris Court of Appeals Upholds First Instance Judgment in* Platypus Case*]*, Dalloz Actualité (Dec. 6, 2024), https://www.dalloz-actualite.fr/flash/finance-decentralisee-cour-d-appel-de-paris-confirme-jugement-de-premiere-instance-dans-l-affa.

1446 *Id.*

1447 Thierry, *supra* note 1445.

The decision has provoked considerable controversy within the cryptocurrency community.[1448] Many observers have expressed concern that the Paris court's refusal to impose criminal liability for the *Platypus* exploit sets a troubling precedent for how protocol vulnerabilities are addressed under French criminal law.

Like the *Mango* case in the United States, *Platypus* illustrates the fundamental difficulty of applying existing legal concepts and criminal provisions to blockchain-based transactions and behaviors. Existing legal frameworks conceived for traditional forms of conduct fail to account for the distinctive features of blockchain-based activities. This mismatch creates considerable legal uncertainty. However, the French courts in this case seemed to consider the exploitation of a protocol's vulnerability as merely a lawful interaction under the terms of a flawed smart contract. This position, coupled with the legal uncertainty surrounding the treatment of conduct on the blockchain, imposes on users the risk of losing funds to a "hack" and puts the burden of protecting users' funds on blockchain platforms.

6.2.4. MEV and the Peraire-Bueno Case

6.2.4.A. What is MEV?

Maximal Extractable Value (MEV) refers to the maximum amount of economic value that can be extracted from the production of a block —beyond the protocol-defined block rewards and transaction fees— by strategically ordering the transactions and including or excluding them in a blockchain network.[1449] In practical terms, MEV arises when validators are able to influence transaction ordering or execution in ways that generate additional profit.

MEV was first observed in the context of transactions on decentralized exchanges (DEXs) running on the Ethereum blockchain.[1450] However, the MEV phenomenon extends to any public, permissionless blockchain where block space is scarce and where the ordering or inclusion of transactions is at least partially discretionary for miners or validators who determine the contents of blocks.[1451]

MEV arises when miners or validators exploit their control over the ordering of blockchain transactions to extract value. Block updates occur through a competitive and probabilistic process. In proof-of-work protocols, such as Bitcoin, miners expend computational resources to solve a cryptographic puzzle, and only one miner can succeed in solving the puzzle and, thus, earn a reward for appending the next block *(See above section 2.3.1.)*. While transactions offering sufficiently high fees are more likely to be included promptly, low-fee transactions may remain pending for extended periods, reflecting the economic incentives motivating block producers.

Although miners or validators must comply with the protocol's validity and consensus rules, they generally retain significant discretion over the order in which pending transactions are included within a block. Public, permissionless blockchains typically impose no explicit protocol-level requirement that transactions be ordered fairly, processed strictly on a first-come-first-served basis,

1448 *See, e.g.*, Stanislas Pogorzelski, *Les hackers français du protocole DeFi Platypus relaxés [French Hackers of the DeFi Protocol Platypus Acquitted]*, COINS.FR (Dec. 5, 2023), https://coins.fr/hack-platypus-relaxes-pirates-justice/.

1449 PRIMAVERA DE FILIPPI, WESSEL REIJERS & MORSHED MANNAN, BLOCKCHAIN GOVERNANCE 152 (The MIT Press 2024), 152-153. https://mitpress.mit.edu/9780262379861/blockchain-governance/

1450 Philip Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, ARXIV 1–2 (Apr. 10, 2019), https://arxiv.org/pdf/1904.05234.

1451 Mikolaj Barczentewicz, Alex F. Sarch & Natasha Vasan, *Blockchain Transaction Ordering as Market Manipulation*, 20 OHIO ST. TECH. L.J. 1 (2023), https://ssrn.com/abstract=4187752;

or treated equally without discrimination.[1452] As a result, transaction ordering becomes an economically strategic decision: Miners or validators may organize pending transactions —commonly drawn from a memory pool (or "mempool")— to maximize value, and they often prioritize transactions that pay them higher fees (or "gas prices"). This discretion enables "front-running," whereby a miner or validator intentionally places one transaction ahead of another to capture an economic advantage. For instance, in some cases, users obtain this priority by including a higher-fee transaction ahead of a known pending transaction.

In this context, miners or validators may arrange, delay, or exclude transactions based on their expected profitability, the fees users are willing to pay, or the validator's own trading or strategic interests.[1453] Maximal Extractable Value thus consists of profits generated by strategic transaction sequencing or selective inclusion. It captures the maximum value that can be extracted by any actor with influence over transaction ordering, including miners or validators, block builders that assemble transaction sequences for inclusion in blocks, and "MEV searchers" who identify and exploit ordering opportunities.[1454] MEV searchers typically are automated trading bots that monitor pending transactions and submit bundles designed to profit from transaction sequencing opportunities such as arbitrage or liquidation.

Finally, MEV manifests differently across blockchain architectures. Some newer blockchains, such as Solana, do not rely on a traditional public mempool. On such networks, MEV does not disappear but emerges through alternative mechanisms.[1455]

6.2.4.B. The Controversy About the Legality of MEV

Without any formal requirement to process transactions in the order in which they are received and in the absence of explicit rules imposing a natural transaction sequence or prohibiting alternative ordering,[1456] MEV extraction based on transaction ordering is typically regarded as lawful, so long as it complies with applicable rules and protocols.[1457] However, MEV has created controversies and gained salience as a policy matter from financial regulators because a common MEV tactic —the frontrunning of transactions— would be illegal under market conduct rules in the regulated traditional financial markets.[1458] In the equities and commodities markets, regulated intermediaries hold a trusted fiduciary duty that requires fairness to all customers and even some affirmative duties, such as finding the "best" price execution for them.[1459]

On the other hand, some scholars have observed that MEV extraction is not always unethical or unlawful.[1460] For example, in some instances, MEV is no different than price arbitrage, an amoral and efficiency-enhancing activity

1452 Galaxy Research, *MEV - Part 1: How Flashboys Became Flashbots*, Galaxy (Jan. 6, 2022), https://www.galaxy.com/insights/research/mev-how-flashboys-became-flashbots/.

1453 Eur. Sec. & Mkts. Auth., Final Report on the Draft Technical Standards Specifying Certain Requirements in Relation to the Detection and Prevention of Market Abuse under the Markets in Crypto-Assets Regulation 9 (2024) [hereinafter ESMA Market Abuse Report], https://www.esma.europa.eu/document/final-report-draft-technical-standards-specifying-certain-requirements-relation-detection.

1454 *Maximal Extractable Value*, Ethereum.org, https://ethereum.org/en/developers/docs/mev/ (last updated May 24, 2024); CoinDesk Learn Team, *What Is MEV, aka Maximal Extractable Value?*, CoinDesk (Oct. 26, 2023), https://www.coindesk.com/learn/what-is-mev-aka-maximal-extractable-value/.

1455 *See* Helius, *Solana MEV: An Introduction*, Helius Blog (Jan. 26, 2024), https://www.helius.dev/blog/solana-mev-an-introduction. Solana validators apparently punish validators for facilitating MEV, though there is no explicit rule against it. *See* Sam Kessler, *Solana Heavyweights Wage War Against Private Mempool Operators*, CoinDesk (June 10, 2024), https://www.coindesk.com/business/2024/06/10/solana-heavyweights-wage-war-against-private-mempool-operators.

1456 *See* ESMA Market Abuse Report, *supra* note 1453, at 7.

1457 *See* Barczentewicz et al., *supra* note 1451, at 78–87; *see also What Is Maximal Extractable Value?*, Chainlink, https://chain.link/education-hub/maximal-extractable-value-mev (last updated May 24, 2023).

1458 Fin. Conduct Auth., Review of Maximal Extractable Value & Blockchain Oracles (2024), https://www.fca.org.uk/publication/research-notes/research-note-review-and-maximal-extractable-value-blockchain-oracles.pdf.

1459 Fin. Conduct Auth., *supra* note 1458, at 20; Barczentewicz et al., *supra* note 1451, at 63–65.

1460 *See* Philip Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, arXiv (2019), https://doi.org/10.48550/arXiv.1904.05234 (explaining that some MEV strategies are economically analogous to arbitrage and can contribute to market efficiency even as they raise fairness concerns).

that facilitates faster price discovery. Under this thinking, searching for and extracting MEV may even promote efficiency in crypto markets.[1461] In fact, some contend that MEV can contribute to greater levels of market participation, transparency, and efficiency.[1462]

Official bodies have expressed a more critical view. The Bank for International Settlements describes MEV as an "intrinsic shortcoming of pseudo-anonymous blockchains."[1463] The International Organization of Securities Commissions (IOSCO) notes that the exploitation of MEV enables conduct that, in traditional financial markets, may be considered manipulative and unlawful.[1464] MEV may adversely affect users, as they cannot reliably assume that their transactions will be executed neutrally or in the order anticipated.[1465] Validators may also engage in other anti-competitive behaviors —such as collusion or censorship of certain transactions— which at a minimum contravene the essence of the blockchain ethos and may be improper otherwise.[1466] Moreover, although the blockchain ledger is publicly observable, making these forms of extraction potentially detectable, the identities of the miners or validators often remain pseudonymous.

The European Securities and Markets Authority (ESMA) has similarly noted that MEV "creates detriment to DeFi users" and may "go against the principles of fairness and integrity that underpin orderly markets in traditional finance."[1467] From a regulatory perspective, this raises the question whether validators should, at least in certain contexts, be treated analogously to regulated intermediaries and be subject to duties not to trade against or exploit users. Permitting validators to extract value from other market participants would allow them to claim decentralization as a shield from liability.[1468]

A possible synthesis is that MEV is neither inherently beneficial nor inherently harmful, but rather an endogenous feature of permissionless blockchain design.[1469] Whether MEV is empirically more harmful than beneficial on balance has yet to be determined. The research firm Galaxy estimated in 2023 that the total amount of MEV extracted from Ethereum users was between $300 million to $900 million annually. That surplus went to block producers, searchers, and builders —presumably away from retail traders.[1470]

The industry has attempted to mitigate some of the negative effects of MEV through technical solutions designed to coordinate and make more transparent the process of MEV extraction. The most prominent are created by the research company Flashbots and include Flashbots Auction and MEV-Boost.[1471] Flashbots

1461 Mikołaj Barczentewicz, *MEV on Ethereum: A Policy Analysis*, L. & Econ. Ctr. (Jan. 23, 2023), https://laweconcenter.org/resources/mev-on-ethereum-a-policy-analysis; Barczentewicz et al., *supra* note 1451, at 58.

1462 Galaxy Research, *supra* note 1452.

1463 Raphael Auer, Jon Frost & Jose Maria Vidal Pastor, *Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi*, BIS Bulletin No. 58, 1 (June 16, 2022), https://www.bis.org/publ/bisbull58.pdf

1464 Int'l Org. of Sec. Comm'ns, Policy (IOSCO), Policy Recommendations for Decentralized Finance (DeFi), *Policy Recommendations for Decentralized Finance (DeFi)* Consultation Report (Sept. 2023) [hereinafter IOSCO Consultation Report 2023] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf; Final Report (Dec. 2023) [hereinafter IOSCO Final Report 2023], https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf.

1465 Auer, Frost & Vidal Pastor, *supra* note 1463, at, 4–5.

1466 IOSCO Consultation Report 2023, see *supra* note 1464, at 56-59.

1467 Eur. Sec. & Mkts. Auth., Maximal Extractable Value Implications for crypto markets 3 (July 1, 2025), https://www.esma.europa.eu/sites/default/files/2025-07/ESMA50-481369926-29744_Maximal_Extractable_Value_Implications_for_crypto_markets.pdf.

1468 *See* Auer, Frost & Vidal Pastor, *supra* note 1463, at 4-5. IOSCO recommends that countries evaluate the ability of a "Responsible Person" to identify, disclose, and even manage and mitigate the impact of MEV strategies. IOSCO Final Report 2023, see *supra* note 1464, at 35.

1469 Galaxy Research, *supra* note 1452.

1470 Galaxy Research, *Distribution of MEV Surplus*, GALAXY (June 5, 2023), https://www.galaxy.com/insights/perspectives/distribution-of-mev-surplus/.

1471 Galaxy Research, *supra* note 1470.

Auction enables validators to connect multiple off-chain marketplaces to transparently auction off block space to MEV searchers.[1472] MEV-Boost is used to separate block construction from block validation by introducing a neutral third party to build blocks from searchers and relay them to validators.[1473] MEV-Boost is nearly universally used; approximately 80 percent of all Ethereum validators earn MEV through MEV-Boost.[1474] These technical countermeasures alone, however, are, so far, insufficient to mitigate the negative externalities of MEV.[1475] New technical solutions continue to be explored by researchers.[1476]

6.2.4.C. The Peraire-Bueno Prosecution

In May 2024, the U.S. Department of Justice indicted the two brothers, James and Anton Peraire-Bueno, on charges of conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering. The alleged wire fraud arose from their use of infrastructure associated with MEV which allegedly threatened "the stability and integrity of the Ethereum blockchain for all network participants."[1477] The U.S. DOJ indictment alleged that the brothers, who operated their own Ethereum validators, deliberately targeted MEV searcher bots[1478] and exploited a vulnerability in MEV-Boost.[1479] According to prosecutors, the brothers exploited a flaw in this relay mechanism to disrupt the normal, non-discretionary ordering of transactions, allowing them to interfere with and rearrange transaction bundles for their personal benefit. Prosecutors also alleged that the brothers sent a false digital signature to the relay.[1480] According to them, this tactic tricked the relay into prematurely revealing the full contents of pending transaction bundles, giving the defendants advance visibility into transaction bundles before they were finalized and enabling them to manipulate the ordering of trades before resubmitting valid blocks.[1481] Through this conduct, defendants allegedly extracted approximately $25 million from victim traders.[1482]

To secure convictions for wire fraud, prosecutors were required to establish that the defendants intentionally made at least one material misrepresentation with the purpose of deceiving others to obtain money.[1483] But a federal judge in New York declared a mistrial November 7, 2025, after jurors reported that they were unable to reach a unanimous verdict.[1484] The jury explained that deliberations had become an emotional strain and that further discussion would not lead to consensus.

1472 *Id*.

1473 This advance is related to Ethereum's update to have block proposer-builder separation. Galaxy Research, *MEV: Part 2: The Rise of the Builders*, Galaxy (Feb. 2, 2023), https://www.galaxy.com/insights/research/mev-the-rise-of-the-builders.

1474 *Id.*

1475 Eur. Sec. & Mkts. Auth., Maximal Extractable Value Implications for crypto markets 3, 11-12 (2025), https://www.esma.europa.eu/sites/default/files/2025-07/ESMA50-481369926-29744_Maximal_Extractable_Value_Implications_for_crypto_markets.pdf.

1476 Pranav Garimidi & Joseph Bonneau, *MEV Explained*, a16z crypto (May 15, 2025),https://a16zcrypto.com/posts/article/mev-explained/.

1477 Indictment, *United States v. Peraire-Bueno*, No. 1:24-CR-00293 (S.D.N.Y. May 8, 2024) at 6, https://www.justice.gov/archives/opa/media/1351996/dl [hereinafter *Peraire-Bueno Indictment*].

1478 MEV is typically carried out by *MEV searchers* which are automated trading bots that monitor pending transactions and submit bundles designed to profit from transaction sequencing opportunities such as arbitrage or liquidation.

1479 MEV-Boost is designed to limit validators' discretion by requiring them to blindly accept transaction bundles assembled by independent block builders, thereby reducing the risk of selective transaction manipulation.

1480 *Peraire-Bueno Indictment*, *supra* note 1477, at 6–7.

1481 Id. at 7–8; Defendants' Joint Motion to Dismiss, *United States v. Peraire-Bueno*, No. 24-CR-293 (S.D.N.Y. Aug. 2024), https://www.steptoe.com/a/web/2eWMpC4eHfLD9ZFkgbNQxT/defendants-joint-mtd.pdf [hereinafter *Peraire-Bueno Motion to Dismiss*].

1482 *Peraire-Bueno Indictment*, *supra* note 1477, at 6-7.

1483 *Peraire-Bueno Indictment*, *supra* note 1477, at 3–4; *Peraire-Bueno Motion to Dismiss, supra* note 1481, at 4-6.

1484 Christopher Beam, *Crypto Mistrial Shows Difficulty in Applying Law to Blockchain Trades*, Bloomberg (Nov. 18, 2025), https://www.bloomberg.com/news/newsletters/2025-11-17/crypto-mistrial-shows-difficulty-in-applying-law-to-blockchain-trades.

Following the mistrial, U.S. Attorney Jay Clayton wrote to the court requesting a retrial scheduled for spring 2026, suggesting that the government intended to pursue the prosecution.[1485] The mistrial has left unresolved fundamental questions about validator conduct, MEV exploitation, and the boundaries of permissible strategic behavior on blockchain networks.

The Peraire-Bueno prosecution directly challenged the "code is law" thesis by asserting that conduct that is technically feasible within blockchain infrastructure may nonetheless constitute fraud under certain circumstances.[1486] In doing so, the prosecution appeared to import into the blockchain context the expectations of market integrity derived from regulated financial markets, despite the absence of an explicit legal or normative framework governing validator conduct. In an unsuccessful motion to have the charges against the brothers dismissed, their defense argued that the prosecution strategy amounted to "an audacious attempt by the United States government to regulate, for the first time and through criminal prosecution, the duties and interactions of the Ethereum Network —a decentralized, trustless system that uses economic incentives to drive behavior and relies on consensus to effect changes."[1487]

If successful, the prosecution of the Peraire-Bueno brothers could have effectively imposed unwritten standards of conduct on validators even though "there are many reasons and an inherent logic as to why Ethereum's protocol rules have been designed to allow for Defendants' conduct."[1488] However, industry observers have noted that the alleged behavior by the brothers violated what some describe as a "gentleman's agreement" within MEV communities.[1489]

At present, there is no clear agreed-upon compact defining validators' duties, nor any explicit legal framework establishing or delimiting their responsibility for harms occurring on-chain, whether directly or derivatively from user behavior. This unresolved allocation of responsibility leaves significant gaps in accountability. Where neither validators nor smart-contract developers are held responsible, users must ultimately bear the risk of participation in blockchain systems that continue to operate outside clearly articulated legal and normative boundaries. On the other hand, holding validators responsible for MEV or for other misconduct on blockchains (like sanctions violations)[1490] may be infeasible because of validators' numerosity and pseudonymity. It may also be unfair because validators do not make conscious decisions about which transactions to validate; it is largely automated and unthinking. The Peraire-Bueno case thus represents the most significant legal test of validator accountability to date, and the mistrial leaves the normative question —whether validators owe duties of conduct to other network participants— formally unresolved.

These four cases —The DAO, Mango Markets, Platypus, and Peraire-Bueno— reveal a broad pattern: Courts and prosecutors around the world are grappling with how to apply traditional legal concepts to the exploitation of blockchain protocols and decentralized finance systems.

1485 Sarah Wynn, *Prosecutors seek new trial for MIT brothers after $25 million Ethereum fraud case ends in mistrial*, TheBlock (Nov. 11, 2025) https://www.theblock.co/post/378414/prosecutors-seek-new-trial-mit-brothers-25-million-ethereum-fraud-case-ends-mistrial.

1486 *Peraire-Bueno Motion to Dismiss*, *supra* note 1481, at 1–2; Beam, *supra* note 1484.

1487 *Peraire-Bueno Motion to Dismiss supra* note 1481, at 6–10.

1488 Amicus Brief in Support of the Peraire-Bueno Defendants' Objections to the "Honest Validator" Theory of Fraud, Coincenter (Nov. 3, 2025), https://www.coincenter.org/amicus-brief-in-support-of-peraire-buenos-objections-to-honest-validator-theory-of-fraud/

1489 Michael Lewitt, *What the DOJ's First MEV Lawsuit Means for Ethereum*, CoinDesk (May 15, 2024), https://www.coindesk.com/opinion/2024/05/15/what-the-dojs-first-mev-lawsuit-means-for-ethereum.

1490 *See* Anders Brownworth et. al, Fed. Reserve Bank of New York, Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash (2024), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1112.pdf.

While none of these decisions is likely to serve as a clear precedent, and outcomes may vary significantly across jurisdictions, prosecutors have in several instances struggled to sustain criminal charges. This uncertainty raises a related question: When harm results from the operation of blockchain code, who should be held responsible? The next section examines whether liability should fall on the developers who write the code.

6.3. THE DEBATE ON DEVELOPERS' LIABILITY

The cases examined above demonstrate that exploiting code vulnerabilities can result in devastating financial losses. The uncertainty surrounding the legal treatment of code exploits intensifies the question of developer accountability. If exploiters cannot be reliably identified or prosecuted —and if the code itself occupies an alegal space— should responsibility fall on those who created the flawed code in the first place?

When a blockchain application, such as a DAO, malfunctions and causes substantial financial losses, there is a strong inclination to attribute responsibility to its developers, particularly when the failure stems from a vulnerability in the code, as in the case of *The DAO*. This raises several questions: Can developers be held liable for software they have created but do not operate? Can they incur liability when their code enables harmful outcomes for users, such as financial loss or the loss of control over private keys? And can they be held accountable for the actions of third parties who use the software they have developed?

These issues have been examined in both academic scholarship and case law.

6.3.1. Rationale and Limits of Developers' Liability

In 2018, the former CFTC Commissioner (and future Chairman) suggested that software developers could be held responsible if, at the time of creating their code, they could reasonably foresee that it would likely be used to violate the law.[1491] Building on this broader question of developers' accountability, blockchain scholar Angela Walch has argued that those who create, operate, or modify public blockchains often function as fiduciaries toward those who rely on these systems.[1492] She challenges the myth of "decentralized governance" and underscores that developers make crucial discretionary decisions that affect all users of a network. This dynamic, she contends, closely resembles relationships in which fiduciary duties typically arise, since users of blockchain networks place significant trust in core developers to act competently and loyally—that is, without conflicts of interest.[1493] For these reasons, Walch argues that influential developers of public blockchains should owe fiduciary duties to users and third parties who rely on these networks. Other proponents of this view maintain that holding developers accountable is the only way to create a social and regulatory framework that fully capitalizes on the benefits of new technology.[1494]

These ideas have faced a significant push back. Opponents contend that this line of reasoning reflects a fundamental misunderstanding of how blockchain networks function.[1495] They highlight that, unlike

1491 Brian D. Quintenz, Comm'r, Commodity Futures Trading Comm'n, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16.

1492 *See* Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, in REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 58-60, 64-67 (Philipp Hacker et al. eds., 2019). https://commons.stmarytx.edu/facarticles/613/?ref=blog.block.science.

1493 Walch argues, however, that many compensation schemes for blockchain developers raise conflict of interest concerns. *Cf. id.* at 66-67.

1494 *See generally* Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer & Nelson M. Rosario, *Blockchain Development and Fiduciary Duty*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 139 (2019), https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty.

1495 *See* De Filippi et al., *Alegality, supra* note 1390, at 359, 364-67.

centralized platform operators, developers cannot unilaterally impose changes on a network. Any modification or upgrade requires the active participation and cooperation of network participants, including token holders, miners, validators, and other stakeholders. None of the actors involved in blockchain governance can act independently of the collective. Accordingly, it would be both problematic and unjust to attribute liability to individual actors for actions that are collectively undertaken by the network and beyond their sole control. Other scholars caution against creating developer liability or establishing a developer fiduciary duty, as such duties represent an "unprecedented expansion of fiduciary law" unsuited to decentralized systems.[1496]

Furthermore, imposing liability on developers could expose any open-source software contributor to legal risk whenever third parties reuse their code. Importantly, the initial developers are rarely those who operate the protocol. In blockchain systems, core developers typically write smart contracts, but third parties may deploy them, and a distributed network of validators or miners may execute them. The actual functioning of the system is carried out by a vast, decentralized network of participants, rather than by a centralized entity or a clearly defined group. As a result, responsibility for the operation of smart contracts extends far beyond the developers who wrote the code. In this context, the prospect of legal liability could exert a chilling effect on innovation and deter developers from participating in blockchain development.

In most jurisdictions, open-source software developers have generally not been held liable for the code they create or publish. In the United States, under the First Amendment to the U.S. Constitution, speech is constitutionally protected, and courts have recognized source code as expressive and, therefore, protected speech "in much the same way that mathematicians use equations or economists use graphs."[1497] Accordingly, those who write or publish code are not, by that fact alone, responsible for how others implement or use it on blockchain networks.[1498] However, this protection is not absolute. American courts generally distinguish between the publication of code — which may qualify as protected speech — and its operational deployment, which may constitute regulable conduct. Liability generally falls instead on the parties who deploy the code, operate the service, or host the platform, rather than on the developers who originally authored the software.[1499]

This distinction has direct relevance to blockchain contexts: publishing and maintaining a smart contract on a public repository may be treated as a form of expression, whereas deploying —and, critically, continuing to control or update— a protocol that executes financial transactions may be subject to regulation. As a result, the speech/conduct distinction does not categorically shield blockchain developers from liability. This framework resurfaced prominently in the *Tornado Cash* litigation *(See below section 6.5.3)*, where defendants and civil challengers argued that publishing and maintaining open-source smart contract code constituted protected expression, while

1496 Peter Hunn, Matthew Kimber & Sarah Worthington, *Developers of Software Code as Fiduciaries: Whatever Next for Crypto-assets and Bitcoin*, *in* THE HANDBOOK OF DIGITAL ASSETS AND THE LAW (Allen et al. eds., forthcoming 2026) (manuscript at 1, 6-12), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5060411. *See also* Haque et al., *supra* note 1494.

1497 In *Bernstein v. United States Department of Justice*, the Ninth Circuit held that source code constitutes a form of expression comparable to scientific or academic writing, and that publishing code may qualify as protected speech under the First Amendment, since it communicates ideas and technical information to a developer community capable of understanding it. However, the court also found that not all software is expressive and, therefore, protected. *See* Bernstein v. U.S. Dep't of Just., 176 F.3d 1132, 1141 (9th Cir.), *reh'g en banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

1498 *See* Mark C. Bennett, *Was I* Speaking *to You?: Purely Functional Source Code as Noncovered Speech*, 92 N.Y.U. L. REV. 1494, 1515-28 (2017); Universal City Studios v. Corley, 273 F.3d 429, 448, 453-58 (2d Cir. 2001) (code itself can be expressive but the use of it can constitute conduct subject to regulation), https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-92-5-Bennett.pdf.

1499 *See* Kyle Langvardt, *Crypto's First Amendment Hustle*, 26 YALE J.L. & TECH. 130, 208-13 (arguing that while code is speech, the law may still target conduct, such as operating a service or trading on a platform), https://yjolt.org/sites/default/files/langvardt_26yalejltech130.pdf. *See generally* Jeff Kosseff, *First Amendment Protection for Online Platforms*, 35 COMPUT. L & SEC. REV. 199 (2019) (supporting the idea of channeling responsibility to intermediaries).

prosecutors and regulators characterized the protocol as a financial service facilitating money laundering.

6.3.2. Case Studies

There is increasing legal support for the view that developers should not be held liable for the code they create, particularly when imposing such liability would result in unreasonable or impractical outcomes. The *Tulip Trading* and *Uniswap* cases discussed below offer instructive illustrations of this principle in practice.

6.3.2.A. Tulip Trading Case

In a matter before the English courts, Tulip Trading Limited initiated proceedings against a group of Bitcoin network developers for allegedly breaching duties owed to Bitcoin owners.

FIGURE 48.

The Tulip Trading Limited claim

In 2020, Tulip Trading Limited, a Seychelles company beneficially owned by Craig Wright, lost access to approximately 111,000 bitcoins (BTC) after a hacker allegedly gained control of Wright's computer environment and deleted the private keys necessary to access certain Bitcoin addresses. [1500]

Following this incident, Tulip Trading filed a claim in the English High Court against a number of core developers and maintainers of various Bitcoin-related software protocols. The company argued that the defendants owed fiduciary and tortious duties to owners of bitcoins because they exercised control over the operation of the networks and, by extension, over the property of others.

The company sought orders compelling the developers either to:

- create a software "patch" or equivalent code modification that would enable network users to regain access to their bitcoins (for instance, by transferring them to a new address or reissuing private keys); or
- pay damages or equitable compensation if such restoration proved impossible. [1501]

In response, the developers denied owing any such duties to bitcoin owners. They argued:

- that the claim conflicted with the core principles of Bitcoin, which operates on a decentralized model with a large, shifting group of contributors;[1502]
- that any proposed solution would likely be ineffective, as miners would refuse to implement it;
- that such an attempt could result in a "fork" in the network, leading to the creation of additional networks, rather than a resolution; and
- that compelled intervention could harm their reputations and discourage participation in open-source development.[1503]

1500 Tulip Trading Ltd v. Bitcoin Association for BSV [2022] EWHC (Ch) 667, at paras 1-5(Eng.), https://www.bailii.org/ew/cases/EWHC/Ch/2022/667.html [hereinafter, *Tulip Trading, High Court decision*]. Interestingly, Tulip Trading CEO Craig Wright had been claiming since 2016 that he was Satoshi Nakamoto and aggressively suing people who challenged his assertion. The blockchain industry fought back, securing an anti-suit and anti-threat injunction against Wright in July 2024. *See generally* Crypto Open Patent Alliance v. Dr. Craig Steven Wright [2024] EWHC 3315 (Ch). Wright continued to threaten to sue cryptocurrency actors, for which he was held in contempt of court; Joe Tidy, *Man Convicted for Repeatedly Lying About Inventing Bitcoin*, BBC (Dec. 19, 2024), https://www.bbc.com/news/articles/c74x0j47gz8o.

1501 *Tulip Trading, High Court decision*, *supra* note 1500, at paras 6, 53.

1502 *Tulip Trading, High Court decision*, *supra* note 1500, at para 34.

1503 *Tulip Trading, High Court decision*, *supra* note 1500, at paras 34-45.

The High Court dismissed Tulip Trading Ltd's claim at the jurisdictional stage, finding that there was no serious issue to be tried.[1504] The court held that the facts pleaded did not disclose a realistic basis for imposing fiduciary or tortious duties on Bitcoin software developers. In particular, there was no arguable case that developers owed duties of loyalty or had assumed responsibility to take positive steps —such as writing and implementing a patch— to restore access to lost or stolen private keys.[1505]

As a result, the court declined jurisdiction and set aside the claim.[1506]

The Court of Appeal reversed the High Court's decision and held that the first-instance judge had erred in concluding that Tulip Trading had no real prospect of establishing that such fiduciary duties might exist.[1507] The Court recalled that key characteristics of a fiduciary relationship include acting for or on behalf of another person in a particular matter, and the existence of a relationship of trust and confidence.[1508] It found it "clearly arguable" that Bitcoin developers had taken on such a role vis-à-vis bitcoin owners. The Court emphasized that developers exercise a measure of control over the Bitcoin software, which involves, for example, taking active steps to update the code in response to bugs or vulnerabilities. That control over the Bitcoin software and this ability to make decisions that affect all users are the kinds of authority and discretion typical of fiduciaries.[1509]

While the Court of Appeal acknowledged that recognizing such duties would "involve a significant development in the common law on fiduciary duties," it found it "conceivable"—and, therefore, triable—that developers might owe both a *negative duty* "not to act in their own self interest" and a *positive duty* to act to protect users' assets, especially given how much users rely on developers' competence and integrity.[1510] This argument rested on the view that Bitcoin owners have no practical alternative but to rely on developers' competence and integrity in maintaining the network.[1511]

The Court rejected the developers' contention that they could not be identified as a determinate group because the developers of open-source networks such as Bitcoin are constantly in flux, decentralized, and, therefore, incapable of being held responsible.[1512] It also dismissed the argument that the proper defendant was the hacker rather than the developers.[1513] Instead, the Court held that Tulip Trading's claim—that the developers constitute an identifiable group exercising significant discretionary control over the network—was sufficiently arguable to proceed to trial.

Finally, the Court of Appeal rejected the suggestion that the dispute fell beyond the reach of judicial authority. It observed that denying jurisdiction would effectively mean that no court could adjudicate such claims.[1514] The Court therefore unanimously allowed the appeal, enabling

1504 *Tulip Trading, High Court decision*, *supra* note 1500, at paras 73-83.

1505 *Id.*

1506 *Tulip Trading, High Court decision*, *supra* note 1500, at paras 100-01.

1507 Tulip Trading Ltd. v. Van der Laan, [2023] EWCA (Civ) 83, at paras 86, 91, 90 (Eng.), https://www.judiciary.uk/wp-content/uploads/2023/02/Tulip-v-Van-Der-Laan-judgment-030223.pdf [hereinafter *Tulip Trading, Appellate Court decision*].

1508 *Tulip Trading, Appellate Court decision, supra* note 1507, at para 91. ("The conclusion is not that there is a fiduciary duty in law in the circumstances alleged by Tulip, only that the case advanced raises a serious issue to be tried.").

1509 *Tulip Trading, Appellate Court decision, supra* note 1507, at paras 70-78.

1510 *Tulip Trading, Appellate Court decision, supra* note 1507, at paras 76, 86. As the Court observed, "since the developers do have the practical ability to prevent anyone else from doing this, one can see why a concomitant duty to act in that way is properly arguable." *Id.* at para 78.

1511 *Tulip Trading, Appellate Court decision, supra* note 1507, at paras 76-78.

1512 *Tulip Trading, Appellate Court decision, supra* note 1507, at paras 72, 77.

1513 *Tulip Trading, Appellate Court decision, supra* note 1507, at para 89.

1514 *Tulip Trading, Appellate Court decision, supra* note 1507, at para 83.

the case to proceed, while leaving open the substantive question of whether blockchain developers owe legal duties to the users of their networks. That question, which required determination at trial on the merits, could have provided much-needed judicial clarity. However, Tulip Trading ultimately withdrew its claim before the case reached that stage.[1515]

Overall, case law demonstrates that the liability of blockchain developers remains uncertain across most legal frameworks. While traditional defenses rooted in decentralization and free speech have largely shielded developers from accountability, the appellate decision in Tulip Trading leaves open the possibility that developers exercising significant control over user assets may, indeed, owe fiduciary-like duties. Moreover, while *Uniswap*, described below, and *Tulip Trading* both address the legal obligations of developers, distinguishing between the coder and the deployer could offer further nuance in allocating liability, as deployment decisions may carry distinct legal implications.[1516] Ultimately, solving the question of developers' liability may require additional judicial interpretation or even targeted legislative intervention.

6.3.2.B. The Uniswap Case (2023)

A U.S. district court held in 2023 that Uniswap Labs, the developer of the Uniswap decentralized exchange protocol, bore no liability for user losses associated with the acquisition of scam tokens on Uniswap.[1517]

FIGURE 49.

The Uniswap class action

Uniswap is an automated liquidity protocol first deployed on the Ethereum blockchain by Uniswap Labs, an open-source decentralized finance (DeFi) development company. The Uniswap protocol popularized the use of self-executing smart contracts that enable asset exchanges ("swaps") without the involvement of traditional financial intermediaries, such as brokers or dealers. Functionally, Uniswap operates as a decentralized exchange (DEX) through smart contracts known as liquidity pools, which facilitate token swaps directly between users without a centralized intermediary.

Although Uniswap offers a user interface that simplifies interaction with these smart contracts, the company itself does not control the underlying smart contracts. Users interact with each other through smart contract liquidity pools.[1518]

In 2022, a group of users filed a putative class action alleging losses from purchases of so-called "scam tokens" on the Uniswap DEX. The plaintiffs claimed that Uniswap Labs and related entities failed to prevent fraudulent token listings and profited —directly or indirectly— from those transactions, or at least enabled them by maintaining the protocol and interface.

1515 *See* Brian Sanya Mondoh, *When Code Creates Duty: The Tulip Trading Case and the Future of Liability in Web3 and Blockchain Networks*, The Barrister Grp. (July 8, 2025), https://thebarristergroup.co.uk/blog/the-tulip-trading-case-and-the-future-of-liability-in-web3-and-blockchain-networks.

1516 *See* Jeceaca An, *Framing Regulation Around the Potential Liabilities of Parties in the Blockchain & Smart Contract Industry*, 25 Fordham J. Corp. & Fin. L. 529, 554-57, 561-63 (2020) (distinguishing coders who write code from users and miners who deploy and upload contracts, and treating financing users who launch offerings as issuers with corresponding disclosure duties), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1488&context=jcfl.

1517 Opinion and Order at 2, Risley v. Universal Navigation Inc., No. 1:22-cv-02780-KPF (S.D.N.Y. Aug. 29, 2023), ECF No. 90.

1518 *Id.* at 4–5, 7–11. *See also How Uniswap Works*, Uniswap, https://docs.uniswap.org/contracts/v2/concepts/protocol-overview/how-uniswap-works (last visited Jan. 15, 2026).

In the *Uniswap* litigation, the plaintiffs sought to hold Uniswap Labs responsible for harms allegedly caused by fraudulent or "scam tokens" traded through the decentralized Uniswap protocol. They argued that, even if Uniswap Labs did not directly facilitate those trades, it failed to prevent or mitigate the resulting losses.[1519]

The U.S. District Court for the Southern District of New York rejected these arguments entirely, holding that the Uniswap protocol's open-source, decentralized architecture precluded imposing liability on its developers for third-party misuse. The court analogized the claim to suing a self-driving car company because one of its vehicles was used "to rob a bank."[1520] In such circumstances, "one would not sue the car company for facilitating the wrongdoing; they would sue the individual who committed the wrong."[1521] According to the court, it would "defy logic that a drafter of computer code underlying a particular software platform" could be liable for a third party's misuse of that platform.[1522] Because of the protocol's decentralized and pseudonymous design, the plaintiffs had an "identifiable injury but no identifiable defendant."[1523]

The Second Circuit U.S. Court of Appeals affirmed in part this decision in February 2025, agreeing with the district court that it "defies logic" to hold smart contract developers liable for third party misuse of their smart contracts.[1524] The Second Circuit vacated the judgment and remanded the state-law claims to the district court.

Taken together, the *Tulip Trading* and *Uniswap* cases illustrate both the persistence of the debate on developers' liability and the emerging contours of judicial reasoning in this area. The contrast between the two cases is especially instructive: whereas *Uniswap* reflects a strong judicial reluctance to impose liability on developers for third-party misuse of decentralized protocols, *Tulip Trading* leaves open the possibility that control, discretion, and user reliance may, in certain circumstances, justify a different allocation of responsibility. The factual configurations of the two cases, however, differ significantly. *Uniswap* concerned harms arising from third-party use of an open protocol, while *Tulip Trading* centered on the technical architecture of the Bitcoin network and the absence of any built-in mechanism to recover access to assets following the loss of private keys. Ultimately, these cases suggest that the degree of effective control over a system—together with the nature of users' reliance on developers—may prove determinative in future litigation.

6.4. THE UNCERTAIN LEGAL STATUS OF DAOs

The ability of decentralized autonomous organizations (DAOs) to operate as fully functioning and autonomous organizations raises fundamental questions about their legal status. Should a DAO be regarded as merely a set of computer code? Should the law recognize it as a legal person? Or does it occupy an intermediate position between these categories? The answer has significant implications for determining whether a DAO possesses legal personality sufficient to be sued or held liable. It also raises the related question of how to define and identify its members and whether blockchain stakeholders —such as founders, developers, token holders, or validators— may be held responsible for the DAO's activities.

1519 Opinion and Order, *supra* note 1517, at 13-14.

1520 *Id.* at 36-37.

1521 *Id.* at 37.

1522 *Id.* at 31.

1523 *Id.* at 2.

1524 *Risley v. Universal Navigation Inc.*, No. 23-1340-cv, 2025 WL 3641289, at 10 (2d Cir. Feb. 26, 2025).

6.4.1. Legal Classification Challenges for DAOs

The contractual nature of DAOs appears difficult to dispute.[1525] By acquiring DAO tokens and choosing to participate in a DAO, token holders manifest their intention to collaborate within the framework established by the underlying computer protocol. The governance rules encoded in the smart contract may thus be viewed as analogous to the articles of association or bylaws of a conventional organization.[1526] Nevertheless, in most jurisdictions, the acquisition of legal personality requires that a DAO be registered or formally recognized under the laws of at least one state.[1527]

While both common law and civil law systems have developed mechanisms for recognizing *de facto* corporations, DAOs present distinctive challenges. Their lack of centralized authority and conventional management structures makes classification under existing legal frameworks particularly difficult. Moreover, in most cases, a DAO's existence can be discerned only through online communication channels —such as a website, social media page, or chat forum— or through treasury funds administered by on-chain smart contracts.

In the absence of a legal entity that subsumes or "wraps" the DAO, the most plausible characterization is that of an unincorporated association or other informal entity lacking separate legal personality. In common law jurisdictions, such arrangements are often analogized to general partnerships or, in some cases, to joint ventures in which the DAO itself lacks legal personhood and its participants may bear unlimited personal liability *(See below section 6.4.2.B.)*.[1528] Alternatively, founders may choose to "wrap" a DAO within a legal entity incorporated under a given jurisdiction. These DAO "legal wrappers" commonly take the form of limited liability companies (LLCs) or —in civil law contexts— foundations, non-profit associations, or trusts.[1529] These are frequently located in favorable regulatory environments, such as Switzerland or Liechtenstein. Various reasons exist for registering a legal entity that embeds DAO governance rules,[1530] with a major one being that a DAO can interact with the off-chain legal world through opening bank accounts and signing employment and other contracts.

The uncertain legal status of DAOs is particularly consequential in matters of liability and legal proceedings. Enforcing legal actions against a DAO is often difficult, if not impossible, because of the ambiguity surrounding its legal classification and the absence of a clearly identifiable legal person. A further question concerns who should be held accountable for the DAO's activities and decisions: the developers who designed the system or the token holders who participate in its governance? These issues are compounded by the pseudonymity of participants and their global dispersion across multiple jurisdictions, both of which render effective enforcement exceptionally challenging.

1525 James J. Park, *Crypto Associations*, 73 UCLA L. Rev. (forthcoming 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5254379.

1526 Florence G'sell & Florian Martin-Bariteau, Council of Eur., The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law 39 (2022), https://rm.coe.int/report-on-blockchains-en/1680a8ffc0.

1527 Some argue that deploying a set of smart contracts is "functionally" equivalent to registering a company in an official registry, but this perspective has not been adopted by major legal systems. Constance Choi et al., Coal. of Automated Legal Applications, Model Law for Decentralized Autonomous Organizations (DAOs) 9 (2021), https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf. On the COALA DAO model law, see below section 7.3.1.A.

1528 In civil law countries like France or Belgium, for example, it can be a *société en participation* (silent partnership). See G'sell & Martin-Bariteau, *supra* note 1526, at 39.

1529 *See* Chris Brummer & Rodrigo Seira, *DAO Strategy and Legal Wrappers*, Paradigm (June 8, 2022), https://www.paradigm.xyz/2022/06/dao-strategy-and-legal-wrappers; *DAO Legal Entity Matrix*, Paradigm, https://daos.paradigm.xyz/ (last visited Jan. 15, 2026). *See generally* David Kerr & Miles Jennings, Andreessen Horowitz, A Legal Framework for Decentralized Autonomous Organizations Part II: Entity Selection Framework 8 (June 2022), https://api.a16zcrypto.com/wp-content/uploads/2022/06/dao-legal-framework-part-2.pdf.

1530 DAOs can also register legal structures for tax law purposes and to limit their members' liability. *See* Vanessa Villanueva Collao, Decentralized(?), But Far From Disorganized: A Comparative Analysis of Legal Wrappers and the Evolving Structure of DAOs 20-21 (May 2, 2025) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5143035.

6.4.2. Case Studies

In the United States, where most DAO-related litigation has taken place, courts have played a central role in addressing legal ambiguities and extending existing liability frameworks to this emerging form of organization. DAOs have largely been analyzed under pre-existing legal categories, such as partnerships, joint ventures, or unincorporated associations.[1531] As a result, U.S. case law has become a testing ground for theories of liability, developed through incremental, case-by-case adjudication rather than through comprehensive legislative or regulatory reform.

6.4.2.A. DAOs as Incorporated Associations: The Ooki DAO Case (2022)

Ooki DAO is a decentralized organization that governs a blockchain-based protocol enabling cryptocurrency margin trading, lending, and borrowing through smart contracts, without centralized management. It is the successor to the bZx protocol operated by bZeroX *(See below Figure 50)*. In September 2022, the U.S. Commodity Futures Trading Commission (CFTC) filed and settled an administrative proceeding against bZeroX, LLC and its founders. At the same time, the CFTC brought a parallel civil enforcement action against the Ooki DAO alleging that it had continued the same unlawful activities after control was transferred to token holders.

FIGURE 50.

From bZx DAO to Ooki DAO

The bZx Protocol was developed for margin trading and lending on the Ethereum blockchain. Initially, bZeroX, LLC, which was co-founded and managed by two developers, controlled the bZx protocol.[1532] In August 2021, bZeroX, LLC transferred control of the protocol to the bZx DAO, a decentralized autonomous organization governed by holders of BZRX tokens, its native cryptocurrency.[1533] The bZx DAO assumed responsibility for maintaining the protocol, developing new products, marketing, and managing the user community. Token holders could propose and vote on governance decisions that, once approved, were automatically executed by the protocol. Following this transition, bZeroX LLC transferred all its assets to the bZx DAO, which was later renamed the Ooki DAO.

The CFTC argued that a "bZeroX objective in transferring control of the bZx Protocol [to the bZx/Ooki DAO] was to attempt to render the [bZx/Ooki DAO], by its decentralized nature, enforcement-proof"—that is, to evade regulatory oversight.[1534] The CFTC also alleged that:

- defendants unlawfully offered leveraged and margined retail commodity transactions in digital assets;[1535]
- Ooki DAO operated as an unregistered futures commission merchant and failed to conduct Know-Your-Customer (KYC) checks on their customers;[1536]
- Ooki DAO was an unincorporated association (i.e.,

1531 Int'l Org. of Sec. Comm'ns, Policy Recommendations for Decentralized Finance (DeFi) 70 (Sept. 2023) [hereinafter IOSCO Sept. 2023 Report], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

1532 *In re* bZeroX, LLC, CFTC No. 22-31, 2022 WL 4597664, at 2 n.1 (Sept. 22, 2022).

1533 *Id.* at 2.

1534 *Id.* at 3.

1535 This argument is drawn from the description of a violation of the Commodity Exchange Act alleged in both the CFTC's administrative decision and the complaint filed in the U.S. District Court for the Northern District of California.

1536 Complaint at 2, Commodity Futures Trading Comm'n v. Ooki DAO, No. 3:22-cv-05416-WHO (N.D. Cal. Sept. 22, 2022), ECF No. 1.

a legal entity) of governance token holders who governed the Ooki DeFi protocol.[1537]

The Ooki DAO litigation raised two major legal challenges: First, did the DAO have the legal capacity to be sued and how could it be served; second, would the governance token holders of the DAO be considered as liable?

1. Can a DAO Be Sued?

The CFTC faced a major obstacle in attempting to sue the Ooki DAO: It could not identify any representative authorized to accept service of process, since the DAO had no physical address or publicly identifiable individuals associated with it.[1538] Since regular means of service of process, like certified mail or physical delivery of the complaint and summons, would not work, the CFTC filed a motion seeking the court's authorization to serve the Ooki DAO using alternative means.[1539] Specifically, the CFTC wanted to "service Ooki DAO 'via the online mechanisms the Ooki DAO has created to allow itself to be contacted by the public,' namely a 'Help Chat Box' and 'an online discussion forum' on its public website."[1540] In October 2022, the U.S. District Court for the Northern District of California granted the CFTC's motion, allowing alternative service via the DAO's online communication channels.[1541]

Ooki DAO did not respond to the CFTC's complaint, nor did any representative appear in court. Several organizations, including advocacy groups such as the DeFi Education Fund, filed *amicus curiae* briefs supporting Ooki DAO. They argued that the DAO could neither be served nor held liable because it was merely a technological protocol rather than a legal entity or unincorporated association.[1542] The court rejected these arguments. In December 2022, the U.S. District Court for the Northern District of California held that Ooki DAO had the capacity to be sued as an unincorporated association under California law[1543]—effectively treating the token-governed entity as a "person" within the meaning of the Commodity Exchange Act (CEA).[1544] The court reasoned that the protocol was controlled by token holders and founders who retained administrative keys, and that it was the conduct of these individuals—not the protocol itself—that the CFTC sought to hold liable.[1545] Accordingly, the court rejected the argument raised by the amici and found that the CFTC's strategy of suing the entity (rather than individual token-holders) was permissible.[1546]

2. Are Governance Token Holders Liable for a DAO's Activities?

The fact that Ooki DAO could be sued did not automatically resolve the question of liability. This issue was addressed separately when the CFTC obtained a default judgment against Ooki DAO for violations of the CEA. Judge William H. Orrick confirmed his earlier determination that the CFTC had presented sufficient factual evidence to establish that Ooki DAO qualified as an unincorporated association under

1537 *In re* bZeroX, LLC, 2022 WL 4597664, at 38-50.

1538 Under California law, unincorporated associations can be sued in accordance with the California Civil Procedure Code. Order Concluding that Service Has Been Achieved at 9, Commodity Futures Trading Comm'n v. Ooki DAO, No. 3:22-cv-05416-WHO (N.D. Cal. Sept. 22, 2022), ECF No. 63 (quoting Cal. Civ. Pro. Code § 369.5(a)).

1539 *Id.* at 4-5.

1540 *Id.* (quotation omitted).

1541 *Id.*

1542 *See id.* at 7.

1543 The court found that the DAO met the definition of an unincorporated association under state law: it is a group of two or more persons (i.e., token holders), joined by mutual consent (i.e., there was a consensual transfer of governance control from bZeroX LLC to the DAO), who organized with a common lawful purpose (i.e., "governing the DAO, particularly through the use and distribution of funds from its central [t]reasury"), and the entity that functions under a common name under circumstances where fairness requires the group be recognized as a legal entity. *Id.* at 10-13 (quotations omitted).

1544 *Id.* at 7, 20-21.

1545 *Id.* at 7 (quotation omitted).

1546 *Id.* at 20-21.

both California and federal law.[1547] Consequently, the court concluded that Ooki DAO was liable for CEA violations and implied that its members—governance token holders—could be held responsible for the DAO's actions, as they are the ones who vote, propose, and exercise governance power.[1548] Notably, the question of individual member liability had already been foreshadowed in the administrative order against bZeroX and its founders discussed above, in which the CFTC held the founders liable both as controlling persons of bZeroX and for their direct participation in the protocol's unlawful activities. The subsequent enforcement action against the Ooki DAO developed this approach further by treating the DAO as an unincorporated association and suggesting that participants in its governance could, under certain conditions, bear liability for its violations.

6.4.2.B. DAOs as General Partnerships

1. Sarcuni v. bZx DAO (2023)

A hacker executed a phishing attack in November 2021 against one of the developers of the bZx protocol, stole the developer's private key, and, using the key, took $55 million in cryptocurrency from the platform, the developer's wallet, and bZx users.[1549] The bZx DAO approved a compensation plan to reimburse those affected by the hack, offering replacement BZRX tokens that vested over time and "debt tokens" that would be gradually repurchased to fully compensate the victims.[1550] Some bZx token holders filed a class action against the original bZeroX LLC, its developers, two investors, and bZeroX successor, Ooki DAO.[1551] The plaintiffs claimed to have lost approximately $40 million in the cyberattack and argued that the repayment plan would take thousands of years to fully compensate them.[1552] Critically, the plaintiffs argued that the bZx DAO was a general partnership made up of all BZRX token holders —meaning each defendant, as a token holder, could be jointly and severally liable for the losses resulting from the cyberattack.

In *Sarcuni v. bZx DAO*, the U.S. District Court for the Southern District of California held that the plaintiffs had plausibly alleged that both the bZx DAO and its successor, the Ooki DAO, could constitute general partnerships under California law, with governance token holders acting as partners.[1553] On that basis, the court allowed the case to proceed, finding that token holders could potentially be held jointly and severally liable for the DAO's alleged negligence in connection with the phishing attack that resulted in the losses suffered by plaintiffs.[1554] The court emphasized that even token holders who did not actively vote could fall within the scope of potential liability, given their ownership and governance rights in the DAO.[1555]

2. Samuels v. Lido DAO (2024)

The Lido DAO governs the Lido liquid staking protocol and collects a portion of the collective's proof-of-stake rewards

1547 Commodity Futures Trading Commission v. Ooki DAO, No. 22-cv-05416-WHO, 2023 WL 3912667, at 8 (N.D. Cal. June 8, 2023). While the question of Ooki DAO's status under federal law was not central for the service of process issue—federal courts look at state law to determine proper service methods—it was important to bring its conduct under the CEA's regulatory scheme.

1548 The court did not directly state that token holders were subject to the judgment. But federal and state law generally state that even though members of an unincorporated association are not liable just because they are members, they can be personally liable if they authorize, ratify, or commit the wrongful acts. *See, e.g.*, CAL. CORP. CODE §§ 18610, 18615 (Deering 2025); NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982).

1549 *Putative Class Action Lawsuit Alleges DAO Members Are Jointly and Severally Liable for a Cryptocurrency Hack*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (May 2022), https://www.skadden.com/insights/publications/2022/05/putative-class-action-lawsuit-alleges-dao-members.

1550 Order at 6, Sarcuni v. bZx DAO, No. 3:22-cv-00618-BEN-DEB (S.D. Cal. Mar. 27, 2023) [hereinafter March 27, 2023 Order].

1551 SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP, *supra* note 1549.

1552 Complaint at 18, Sarcuni v. bZx DAO, No. 3:22-cv-00618-BEN-DEB (S.D. Cal. May 2, 2022).

1553 March 27, 2023 Order, *supra* note 1550, at 6.

1554 *Id.* at 29.

1555 Following a settlement reached during an Early Neutral Evaluation on July 18, 2023, the parties stipulated to dismissal on November 16, 2023.

earned.[1556] An investor, Andrew Samuels, who purchased Lido tokens, alleged securities violations against the Lido DAO and four of its venture capital investors who held large positions in Lido governance tokens.[1557]

Plaintiff argued that the large token holders, through their active governance participation, acted as partners in a general partnership with the DAO.[1558] The defendants countered that the Lido DAO was not a legal entity and that Lido was merely "autonomous software that runs without human management."[1559] Therefore, in effect, defendants argued that the Lido DAO was incapable of being sued at all.

In *Samuels v. Lido DAO*, the U.S. District Court for the Northern District of California denied a defendants' motion to dismiss. It found that the plaintiff had sufficiently alleged that Lido DAO may be a general partnership under California law, thereby exposing certain large token holders to potential liability.[1560] The court held that the DAO's alleged securities violations could be viewed as those of an entity operated by individuals, rather than purely autonomous software. Although the court did not define precisely who the partners would be, it found the complaint adequate to infer that a general partnership had been formed under California law.[1561]

The court also sustained the plaintiff's arguments that three of the four major token holders (venture capital firms) "meaningfully participated" in governance —by voting, influencing decisions, and guiding the DAO's development— and thus might be treated as partners. The court found it reasonable to infer that these defendants "took an active role in [the DAO's] management or intended to do so," such that they could not categorically avoid liability for the DAO's alleged wrongful acts.[1562] By contrast, the fourth venture capital defendant was treated differently because the complaint did not allege sufficient facts to establish comparable participation in governance, leaving its potential liability unresolved pending further factual development.

3. Houghton v Leshner (2023)

In *Houghton v. Leshner*, Amanda Houghton and other plaintiffs —purchasers of COMP tokens, a cryptocurrency created by Compound Labs, Inc.— filed a class action in the U.S. District Court for the Northern District of California against several defendants. The lawsuit alleged losses arising from the sale of unregistered securities in the form of COMP tokens.[1563] Compound Labs had developed the Compound protocol, a decentralized finance platform that enables users to lend and borrow crypto-assets. In 2020, the company transferred control of the protocol and its related business operations to the Compound DAO, a decentralized autonomous organization governed by holders of COMP tokens.

According to the complaint, a small group of individuals, including several of the defendants, owned more than 50 percent of COMP tokens. The lawsuit alleged defendants used their majority holdings to exercise effective control

1556 Order at 3-4, Samuels v. Lido DAO, No. 3:23-cv-06492-VC (N.D. Cal. Nov. 18, 2024).

1557 *Id.* at 2, 7-8.

1558 *Id.* at 8-11, 13.

1559 *Id.* at 8.

1560 *Id.* at 11-12.

1561 Whether the partnership is narrower and includes only the founders, or broader and includes everyone who has voted on a governance proposal or holds Lido tokens will be decided at trial. *See id.* at 10-11.

1562 *Id.* at 5.

1563 *Houghton v. Leshner*, No. 3:22-cv-07781-WHO (N.D. Cal. filed Dec. 12, 2022), https://static1.squarespace.com/static/64add1640de92140042af4ac/t/659af1ade0f70c15213d23ff/1704653229403/Houghton+v+Lessner.pdf; Alexander C. Drylewski, Stuart D. Levi & Daniel Michael, *Digital Assets and DAOs: New Theories of Liability,* Reuters Legal News (June 10, 2024), https://www.skadden.com/-/media/files/publications/2024/06/digital_assets_and_daos_new_theories_of_liability.pdf?rev=3e7a7d73cf50496d944e87efccdd90dc.

over the governance and operation of the Compound protocol. Robert Leshner and Geoffrey Hayes, the co-founders of Compound Labs and architects of the protocol, were among the defendants.

The plaintiffs alleged that Compound DAO sold or solicited the plaintiffs' purchase of COMP tokens and argued that the DAO should be treated as a general partnership under California law. Because certain defendants allegedly held a majority of the tokens and actively participated in governance proposals, the plaintiffs contended that the defendants should be considered partners of the DAO. On this theory, those token holders would be general partners subject to joint and several liability for the DAO's alleged violations of federal securities laws. The defendants, however, reserved their right to contest both the characterization of Compound DAO as a general partnership and the claim that any of them should be deemed general partners.

On September 20, 2023, the court denied the defendants' motion to dismiss and allowed the case to proceed. The court explained that the "exact contours of liability, whether it flows from the acts of 'Compound DAO' or from the acts of one or more Partner Defendants, cannot be determined at this juncture" and that such issues would be more appropriately resolved on a full evidentiary record at summary judgment or trial.[1564]

6.4.2.C. Conclusion

U.S. federal courts have shown a willingness to adopt theories that attribute liability to governance token holders. Recent decisions suggest that DAOs operating through governance tokens and being "unwrapped" —that is, lacking any formal, legal ties to a registered entity ("wrapper")— may be characterized as unincorporated associations or general partnerships, comprising some or all of token holders. And in either characterization, token holders may incur joint and several liability for the DAO's activities.[1565] In *CFTC v. Ooki DAO*, the court held that the DAO qualified as an unincorporated association and hinted that its members — namely, governance token holders who participated in DAO activities— could be held accountable for certain activities. Similarly, in *Sarcuni v. bZx DAO* and *Samuels v. Lido DAO*, courts found that plaintiffs had plausibly alleged that the DAOs operated as general partnerships under California law.

These developments reflect a broader judicial response to the alleged alegality of DAOs: Courts are, in effect, using partnership and association law to reanchor within established legal frameworks entities that were designed to operate outside them, thereby challenging the longstanding assumption that decentralization itself shields participants from legal accountability. The decisions emphasize that governance token holders who vote on proposals, influence governance, or otherwise participate in collective decision making may be treated as partners and, thus, be potentially subject to joint and several liability for the DAO's wrongful acts. U.S. courts have tended not to treat decentralization as a defense to liability but as a factor that potentially broadens the range of individuals who may be held responsible.[1566] New cases continue to be filed, asserting collective, joint, and several theories of liability for DAOs, precisely because they are decentralized. Accordingly, they have "no explicit liability protection; and no distinction between managers and directors, or between general and limited partners."[1567]

1564 *Houghton v. Leshner*, No. 22-cv-778 (N.D. Cal. Sept. 20, 2023) (order denying motion to dismiss), https://www.courtlistener.com/docket/66623711/94/houghton-v-leshner/.

1565 A third case against a DAO in the United States was dismissed for lack of standing and never reached the merits, including whether the DAO was a partnership. *See* MK Manoylov, *Judge Dismisses Lawsuit Claiming DeFi Protocol Operated Illegal Lottery*, THE BLOCK (June 7, 2023), https://www.theblock.co/post/233633/judge-dismisses-lawsuit-claiming-defi-protocol-operated-illegal-lottery.

1566 *See, e.g.*, Order at 9-10, Houghton v. Leshner, No. 3:22-cv-07781-WHO (N.D. Cal. Sept. 20, 2023) (finding allegations sufficient that "partners" in a DAO can be subject to liability, reserving for trial the question of whether liability "flows from the acts of [the DAO] or flows from the acts of one or more [partners]").

1567 *See, e.g.*, Compl. at 3, Carbone v. Kaal, No. 2:23-cv-03443-ALM-CMV (S.D. Ohio Oct. 17, 2023).

These rulings raise concerns about the legal viability of DAOs in their current form. Without explicit liability protections or corporate structures, DAOs risk exposing token holders to substantial personal liability, at least in the United States. Some commentators note that token holder liability can compound other structural weaknesses of DAOs, including coordination failures arising from the absence of leadership, technical vulnerabilities to attacks, and persistently low voter participation.[1568] As more cases are filed, asserting collective (joint and several) liability,[1569] courts are likely to continue treating DAOs as unincorporated associations rather than as autonomous software systems.[1570] The broader adoption and long-term success of DAOs will likely depend on balancing decentralization with clearer frameworks for liability and governance.[1571]

The legal uncertainty surrounding DAOs is compounded by similar ambiguity regarding the fundamental building blocks of blockchain applications: smart contracts. While DAOs raise questions about organizational form and participant liability, smart contracts raise even more foundational questions about the nature of agreement, consent, and contractual obligation in code-based systems. The following section examines whether smart contracts can constitute legally binding agreements and how courts should interpret code-based interactions.

6.5. LEGAL AMBIGUITY SURROUNDING THE STATUS OF SMART CONTRACTS

The legal status of smart contracts remains one of the most unsettled and consequential areas in the study of blockchain technology. While smart contracts are employed across a range of use cases —from automating the transfer of funds from an escrow account to facilitating the distribution of estate assets— their adoption has generated considerable debate over their compatibility with established doctrines of contract law.[1572] This section addresses the definitional ambiguities that cloud the discourse. It also analyzes the enforceability of smart contracts under current legal frameworks, all within the context of a rapidly evolving global regulatory landscape.

6.5.1. Conceptualizing Smart Contracts in Law

Much of the legal and regulatory confusion surrounding smart contracts arises from a fundamental divergence in

1568 Miles Jennings, *Machiavelli for DAOs: Principles for Fixing Decentralized Governance (Part 1)*, a16z CRYPTO (Sept. 21, 2023), https://a16zcrypto.com/posts/article/machiavelli-principles-dao-decentralized-governance/.

1569 *See* Tim Copeland, *A DAO is Funding a Lawsuit Against Its Own Founding Team*, THE BLOCK (Nov. 21, 2023), https://www.theblock.co/post/263924/a-dao-is-funding-a-lawsuit-against-its-own-founding-team; Zhiyuan Sun, *Azuki DAO Rebrands to 'Bean' as It Drops Lawsuit Against Founder*, COINTELEGRAPH (Nov. 25, 2023), https://cointelegraph.com/news/azuki-dao-rebrands-bean-drops-lawsuit-against-founder.

1570 Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373 (2019), https://www.gwlr.org/wp-content/uploads/2019/04/87-Geo.-Wash.-L.-Rev.-373.pdf.

1571 *See generally* ELLEN NAUDT, EUR. CENTR. BANK, OCCASIONAL PAPER SERIES: THE FUTURE OF DAOS IN FINANCE (2023).

1572 *See generally* Nicolas Cornell & Kevin Werbach, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017) https://scholarship.law.duke.edu/dlj/vol67/iss2/2/ (arguing that smart contracts will not replace contract law); Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2018) (arguing that smart contracts create new inefficiencies as compared to human-language contracts), https://repository.law.upenn.edu/Documents/Detail/smart-contracts-and-the-cost-of-inflexibility/155845; Shaanan Cohney et al., *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019) (analyzing smart contracts in the context of initial coin offerings (ICOs) https://repository.law.upenn.edu/Documents/Detail/coin-operated-capitalism/395371; Sandra A. Jeskie & Peter L. Michaelson, *Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts*, 74 DISP. RESOL. J. 89 (2019) (arguing that arbitration is the sole viable approach for resolving disputes involving smart contracts), https://www.ccarbitrators.org/wp-content/uploads/2021/05/Michaelson_Jeskie_Arbitrating-Disputes-Involving-Blockchains_AAA_DRJ_Oct2020.pdf; Primavera De Filippi et al., *Smart Contracts*, 10 INTERNET POL'Y REV. 1 (2021) (clarifying misconceptions about smart contracts' definitions and explaining how they differ technically and legally from traditional contracts), https://policyreview.info/pdf/policyreview-2021-2-1549.pdf; Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 WASH. & LEE L. REV.1521 (2021) (arguing that existing UCC frameworks can be adapted to accommodate smart contracts), https://scholarlycommons.law.wlu.edu/wlulr/vol78/iss4/7/; Carla L. Reyes, *A Unified Theory of Code Connected Contracts*, 46 J. CORP. L.981 (2021) (proposing a unified framework for analyzing the legal significance of contracts that incorporate or are performed through computer code, including smart contracts), https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Reyes_Final_Web_0.pdf; Carla L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, 2022 WISC. L. REV. FORWARD 85 (2022) (discussing how language data could resolve ambiguity when it comes to interpreting contracts, including smart contracts), https://wlr.law.wisc.edu/wp-content/uploads/sites/1263/2023/03/CLR-Final-1.pdf; Mateja Durovic & Chris Willett, *A Legal Framework for Using Smart Contracts in Consumer Contracts: Machines as Servants, Not Masters*, 86 MOD. L. REV. 1390 (2023) (arguing that smart contracts should embody consumer law values to operate fairly), https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12817; Bahadir Köksal & Roee Sarel, *The Smart Contracts Trilemma*, 2025 U. ILL. L. REV. 1253 (2025) (discussing how legislators must approach regulating and enforcing smart contracts) https://illinoislawreview.org/wp-content/uploads/2025/08/Sarel-1.pdf.

how the technical and legal communities define the term. In computer science, "smart contract" is a term of art referring to a piece of software. Legal scholars, by contrast, tend to focus on the "contract" component and interpret it as an agreement that generates legal consequences. This conceptual misalignment has had tangible regulatory effects, as illustrated by legislative attempts to define smart contracts that have been criticized as both technically imprecise and legally redundant. Given these persistent misunderstandings, developing a clear typology is essential to navigating this conceptual landscape.

6.5.1.A. Smart Contracts and Smart Legal Contracts

From a technical perspective, a smart contract is a computer program or script that runs on a decentralized network *(See above section 2.5.1.)*.[1573] It is designed to automatically execute predefined actions when specific conditions are met. This is often summarized by the logic, "if the data value equals X, then perform step A, else perform step B."[1574] This concept was first articulated in the 1990s by computer scientist Nick Szabo, who envisioned "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[1575] Primavera De Filippi and Aaron Wright defined smart contract as an "if-then" statement that runs on the blockchain where "parties can enter into a binding commercial relationship, either entirely or partially memorialized using code, and use software to manage contractual performance."[1576] Ethereum founder Vitalik Buterin offered a more functional definition, describing smart contracts as "systems which automatically move digital assets according to arbitrary pre-specified rules."[1577]

Three scholarly positions appear. In essence, the technical community views smart contracts as self-executing code, a tool for automation that is not inherently a legal instrument. As one review notes, the name is deceptive; in many contexts, a "smart contract" is "only stupid computer code."[1578]

While the technology community understands a "smart contract" as a software program that executes predefined instructions, the legal community often conflates the term with a legally enforceable agreement. Some scholars maintain that smart contracts may, in principle, be legally binding, as they can contain the essential elements of a contract comparable to traditional written agreements.[1579] For example, Max Raskin defines a smart contract as "an agreement whose execution is automated" and "effected through a computer running code that has translated legal prose into an executable program."[1580] Likewise, Anne Duke argues that smart contracts satisfy the criteria for contract formation under the United Nations Convention on Contracts for the International Sale of Goods (CISG) and are, therefore, legally binding in international sales.[1581]

1573 According to Cornell & Werbach, *supra* note 1572, at 319-20, 333, 372-73, smart contracts can be generally defined as "self-executing digital transactions using decentralized cryptographic mechanisms for enforcement."

1574 Jeskie & Michaelson, *supra* note 1572, at 111.

1575 Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (last visited Jan. 15, 2026).

1576 Primavera de Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code, 74 (2018).

1577 Reyes, *Emerging Technology's Language Wars: Smart Contracts*, *supra* note 1572, at 93 n. 31 (citing the original Ethereum White Paper authored by Buterin).

1578 Hamed Taherdoost, *Smart Contracts in Blockchain Technology: A Critical Review*, 14 Info. 117 (2023), https://www.mdpi.com/2078-2489/14/2/117

1579 Dino Gliha & Sandra Markovic, *Smart Contracts and the Evolution of a Legal Perspective on the Protection of Human Rights*, *in* Digital Technologies and the Law of Obligations 166 (Zvonomir Slakoper & Ivan Tot eds., 2021); Riccardo De Caria, *The Legal Meaning of Smart Contracts*, 26 Eur. Rev. Priv. L. 731, 731-752 (2019), https://cointhinktank.com/upload/crypto/Legal%20Meaning%20of%20Smart%20Contracts.pdf.

1580 Max Raskin, *The Law and Legality of Smart Contracts*, 1 Geo L. Tech. Rev. 305, 309 (2017), https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf.

1581 Köksal & Sarel, *supra* note 1572, at 1276 (referencing Anna Duke, Comment, *What Does the CISG Have to Say About Smart Contracts? A Legal Analysis*, 20 Chi. J. Int'l L. 141 (2019), https://chicagounbound.uchicago.edu/cjil/vol20/iss1/4).

By contrast, other scholars regard smart contracts as purely technical instruments that execute or enforce performance automatically and that are often mistaken for legal contracts due to misleading terminology.[1582] Fabio Bassan and Maddalena Rabitti emphasize that "the smart contract as a 'code' does not possess the necessary characteristics to qualify it as a (legal) contract."[1583]

Still others adopt a pragmatic position, emphasizing that no categorical statement can be made as to the legal status of smart contracts: The characterization of a smart contract depends on its specific function and purpose.[1584]

In sum, there is an ongoing debate as to "whether smart contracts are in fact "contracts" under civil and common law."[1585] This uncertainty has fueled debates over whether computer code can meet the traditional requirements of contract law.[1586] The lack of conceptual alignment has had tangible consequences. In 2017, Arizona amended its version of the Uniform Electronic Transactions Act to recognize "smart contracts" and blockchain signatures as legally valid.[1587] However, the definition of "smart contract" was technically imprecise, describing it as an "event-driven program, with state, that runs on a distributed, decentralized, shared, and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."[1588] The statute did not clarify whether a smart contract refers to code or to a legal contract implemented via code, thereby conflating technical and legal meanings. As a result, the law has been criticized for being technologically inaccurate and for failing to achieve its intended goal of subjecting smart contracts to traditional legal rules.[1589]

To resolve this ambiguity, scholars have proposed a more nuanced vocabulary distinguishing the technical "smart contract" from the "smart legal contract."[1590] According to this view, a smart legal contract refers to a traditional legal agreement whose performance is automated, in whole

---

1582 For example, Pierluigi Cuccuru, *Beyond Bitcoin: An Early Overview on Smart Contracts*, 25 Int'l J.L. & Info. Tech. 179, 185 (2017), https://www.iris.sssup.it/handle/11382/524614 notes that "smart contracts are not legally binding contracts in a technical meaning" and that they "basically work as independent agents which control [and manage] certain digital assets." Similarly, Daniel S. Sloan, *Smart Contracts: A Leap Forward in Technology and a Step Backward in Law*, 60 Washburn L.J. 387, 395-96 (2021), argues that smart contracts are "merely a tool parties may use to perform the actual contract" and that it is simply a way to express parties' objectives in code, https://contentdm.washburnlaw.edu/digital/api/collection/wlj/id/7365/download.

1583 Fabio Bassan & Maddalena Rabitti, *From Smart Legal Contract to Contracts on Blockchain: An Empirical Investigation*, 55 Comput. L. & Sec. Rev., 2024, at 3-4, https://doi.org/10.1016/j.clsr.2024.106035 (also referencing other scholars and blockchain experts who said that naming a piece of code "smart contract" is a misnomer for what it actually is).

1584 *See, e.g.*, Enas Mohammed Alqodsi & Leila Arenova, *Smart Contracts in Contract Law as an Auxiliary Tool or a Promising Substitute for Traditional Contracts*, 16 J. Legal Affs. & Disp. Resol. Eng'g & Constr. (2024), https://doi.org/10.1061/JLADAH.LADR-1132 (comparing smart contracts to "traditional" contracts, arguing that whether they should be treated similarly depends on their specific function, context, laws in a jurisdiction, and other externalities, ultimately finding that smart contracts cannot supplant "traditional" contracts in the near future).

1585 Amy J. Schmitz, *Resolving NFT and Blockchain Disputes*, 6 Stan. J. Blockchain L. & Pol'y 156, 160 (2023), https://stanford-jblp.pubpub.org/pub/resolving-nft-blockchain-disputes/release/4. *See also* Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 Wash. & Lee L. Rev. 1521, 1543 (2021), https://scholarlycommons.law.wlu.edu/wlulr/vol78/iss4/7/ ("many [blockchain] projects seek to use smart contracts to perform legal obligations imposed by statute and regulation"); De Caria, *supra* note 1579, at 744.

1586 "Many lawyers, and legal academics, . . . agonize over the details of whether, and under what circumstances, smart contracts meet the classic contract law requirements of offer, acceptance, mutual consideration, and meeting of the minds"), Reyes, *Emerging Technology's Language Wars: Smart Contracts*, *supra* note 1572, at 90.

1587 Ariz. Rev. Stat. § 44-7061 (2017) (One of the paragraphs states, "Smart contracts may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term.")

1588 *Id.*

1589 Reyes, *Emerging Technology's Language Wars: Smart Contracts*, *supra* note 1572, at 87–88.

1590 Josh Stark of Ledger Labs proposed to use the term "smart legal contracts" as a way to differentiate legally binding contracts from purely technical code. Josh Stark, *Making Sense of Blockchain Smart Contracts*, CoinDesk (June 4, 2016), https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts (last visited Jan. 15, 2026). The concept of "smart legal contracts" was later picked up by scholars, for example, Christopher D. Clack et al., *Smart Contract Templates: Foundations, Design Landscape and Research Directions*, arXiv (Aug. 2, 2016), https://doi.org/10.48550/arXiv.1608.00771, and interpreted as "a legal agreement, at least some of which is capable of being implemented in software." Various actors, from trade organizations, like the International Swaps and Derivatives Association, to government bodies tasked with reforming the law, such as the U.K. Law Commission, have since adopted and built on this idea. *See, e.g.*, Int'l Swaps & Derivatives Ass'n & Linklaters, Smart Contracts and Distributed Ledger – A Legal Perspective (Aug. 2017), https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-%20legal-perspective.pdf ("Smart contract code could either be entirely separate from the legal contract, or the legal contract could incorporate some form of code in certain areas."); The Law Comm'n, Smart Legal Contracts: Advice to Government No. 401, at 5 (Nov. 2021), https://webarchive.nationalarchives.gov.uk/ukgwa/20220916180919/https://www.lawcom.gov.uk/project/smart-contracts/ [hereinafter Advice to Government] (suggesting to the government of the United Kingdom that "[c]urrent legal principles can apply to smart legal contracts in much the same way as they do to traditional contracts").

or in part, by computer code.[1591] The code functions as a "computerized transaction protocol that executes the terms of a contract."[1592] In this sense, the smart legal contract is not itself a contract in the legal sense but rather a computer program that encodes, in part or in full, the substantive terms of an agreement so that they can be executed automatically. Some scholars conceive of smart legal contracts more broadly as digital architectures that organize or constrain the negotiation process rather than directly represent the parties' substantive interests or obligations.[1593] Others, such as Primavera De Filippi and Aaron Wright, emphasize that smart contracts govern *conduct* through code rather than create *legal obligations* in the classical contractual sense.[1594]

6.5.1.B. Typology of Smart Contracts

The United Kingdom's Law Commission provided a clear and technology-neutral definition of a smart legal contract as "a legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program."[1595] This definition emphasizes the legal effect of the arrangement rather than the underlying technology that enables it.

FIGURE 51.

The typology of smart contracts by the U.K. Law Commission

The U.K.Law Commission has developed a typology of *smart legal contracts* based on varying degrees of automation, that is, the extent to which computer code merely performs contractual obligations defined elsewhere or instead defines and performs those obligations itself. This distinction is critical for legal analysis and interpretation.

- **Natural-language contract with automated performance:** In this configuration, the contract is drafted entirely in natural language (for example, English), while a smart contract is used solely as a tool to automate the performance of one or more obligations, such as recurring payments or conditional transfers. The code does not define the contractual terms; it merely executes them.[1596]
- **Hybrid contract:** This form combines natural-language provisions with coded components. Some obligations are expressed in prose, while others are defined and performed by code. In certain cases, a single obligation may even be represented simultaneously in natural language and in code, raising the question of which formulation prevails in the event of a conflict.[1597]

Continued

1591 *See* Karolina Kasprzyk, *The Concept of Smart Contracts from the Legal Perspective*, 34 Rev. Eur. & Compar. L. 101, 103, 105 (2018), https://pdfs.semanticscholar.org/7a7b/92cf45ae205b73c2cb0a68e5c3f0928ed85a.pdf; Raskin, *supra* note 1580, at 312.

1592 Nick Szabo, *Smart Contracts* (1994), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (last visited Jan. 15, 2026).

1593 *See* Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 Neb. L. Rev. 384, 396-99 (2017), https://ssrn.com/abstract=2914103 (pointing out that Szabo's original idea of a smart contract was broad enough to, in addition to the "contract" element, accommodate the idea of procedural frameworks that regulate how parties negotiate and structure their performance).

1594 De Filippi & Wright, *supra* note 1576, at 74, 78 ("Even where smart contracts entirely replace formal legal agreements, these programs do not operate in a vacuum. While they can automate payment obligations and the transfer of valuable assets, smart contracts do not obviate the need for parties to agree to these arrangements.")

1595 Advice to Government, *supra* note 1590, at 1.

1596 *Id.* at 22, 25-26.

1597 *Id.* at 22-23, 26-27.

FIGURE 51. (continued)

The typology of smart contracts by the U.K. Law Commission (continued)

- **Solely code contract:** In this configuration, the entire agreement is both defined and executed through a computer program. No separate natural-language version of the agreement exists, meaning that the parties' rights and obligations must be determined through interpretation of the code itself.[1598]

These categories should not be applied too rigidly. Within a single contractual arrangement, the degree of automation may vary across obligations, and what matters for legal analysis is the specific role played by the code in each instance. Automation should therefore be understood as existing along a spectrum: Smart legal contracts involving relatively routine forms of automation —such as the automated execution of payment instructions— are unlikely to raise novel legal issues, whereas arrangements drafted primarily or entirely in code and recorded on distributed ledger systems are more likely to generate new legal questions.[1599]

The European Law Institute (ELI) has proposed a slightly different classification in its *Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (2023).[1600] ELI distinguishes among smart contracts as:

- Mere code (no legal agreement exists, the situation is a mere transaction in the technical sense of the word);
- Code functioning as a tool to execute an off-chain agreement;
- Code constituting "a legally binding declaration of will, such as an offer or acceptance or constitutes a legal agreement itself;" and
- Code merged with the legal agreement and therefore exist simultaneously on-chain and off-chain (code and natural language jointly constitute the contract, *on-chain/off-chain hybrid*).

Both proposed categorizations focus on the level of integration between code and legal terms, and the degree of code involvement in expressing legal agreement. The Law Commission and ELI highlight that wholly-coded contracts (mere code without legal agreement in natural language) give rise to novel problems, such as agreement formation, legal interpretation, remedies, vitiating factors, consumer protection, and jurisdiction.[1601] Traditional contracts are more familiar and, therefore, better understood, mainly because they are agreements anchored in natural language negotiated by humans using conventions that have existed in contract law for thousands of years. However, once natural language is entirely replaced by code that defines terms, this full dependence on code, in the words of the Law Commission, "takes the contract out of the realm of legal familiarity."[1602]

1598 *Id.* at 23, 29-30.

1599 The U.K. Law Commission's work has continued since 2021 in related adjacent areas, though none of these subsequent publications have revisited or modified the smart contract typology. These include a Final Report on Digital Assets (2023), a supplemental report and draft bill on digital assets as personal property (2024), and a consultation paper on private international law and digital assets focusing on wholly decentralized applications of DLT and private international issues they raise (2025). *See* The Law Comm'n, Digital Assets: Final Report No 412 (June 27, 2023), https://cdn.websitebuilder.service.justice.gov.uk/uploads/sites/54/2025/12/Final-digital-assets-report-FOR-WEBSITE-2.pdf; The Law Comm'n, Digital Assets as Personal Property: Supplemental Report and Draft Bill (July 29, 2024), https://cdn.websitebuilder.service.justice.gov.uk/uploads/sites/54/2025/12/Digital-assets-as-personal-property-supplemental-report-and-draft-Bill-web-version.pdf; The Law Comm'n, Digital Assets and Electronic Trade Documents in Private International Law: Consultation Paper (June 5, 2025), https://cdn.websitebuilder.service.justice.gov.uk/uploads/sites/54/2025/06/Digital-assets-conflicts-CP-2025.pdf.pdf

1600 Eur. L. Inst., ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection 13, 22 (2023) [hereinafter ELI Principles], https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf.

1601 *See generally Id.*; Advice to Government, *supra* note 1590.

1602 Advice to Government, *supra* note 1590, at 13.

Scholars continue to debate whether smart contracts are merely technical instruments for automating performance or whether they can constitute legally binding agreements,[1603] as well as which body of law should govern these borderless digital transactions (on private international law aspects, *see Section 6.6*). The central tension lies in their dual nature: They are simultaneously computer code and, potentially, legal agreements capable of producing normative effects.

6.5.2. The Legal Significance of Smart Contracts

The preceding section established that smart contracts defy easy categorization —they are simultaneously code and, potentially, legal instruments. That dual nature raises a practical question: Under what conditions and in which jurisdictions can a smart contract produce enforceable legal obligations? This section examines whether code-based interactions can satisfy the requirements of traditional contract formation. It also examines how legal systems address challenges posed by automation, immutability, and the absence of natural language to express contractual intent. It looks across different jurisdictions to analyze contract formation requirements and explores the inherent limitations of code-based contracting. The answers vary significantly across jurisdictions and reflect deep divergences between common-law and civil-law traditions. No global consensus has yet emerged.

6.5.2.A. Can Smart Contracts Be Legally Binding Agreements?

For a smart legal contract to produce legal effects and bind the parties, it must meet the traditional requirements of contract formation and validity under the applicable legal system —such as consent, capacity, lawful object (and cause, where relevant), and compliance with mandatory rules. The fact that a contract is executed automatically through code does not alter these fundamental requirements.

Some scholars assert that smart contracts may meet the formal criteria for contract formation under the United Nations Convention on Contracts for the International Sale of Goods (CISG) and, thus, may be legally enforceable in the context of cross-border commercial transactions.[1604] The CISG's Article 11, which states that a contract needs no specific form and need not be in writing, elegantly sidesteps the debate over formalities that has occupied domestic law.[1605] From a more global perspective, the legal landscape remains fragmented. This fragmentation means the enforceability of the same code can become dependent on geographical location, creating significant compliance challenges and spurring regulatory arbitrage in a borderless ecosystem.[1606]

1. In the United States

a. Core Elements Required for Contract Formation

Under U.S. law, the mere deployment or use of a smart contract does not, by itself, preclude a determination that

1603 *See, e.g.*, Köksal & Sarel, *supra* note 1572, at 1274-75 (whether a smart contract is legally binding "depends on what precisely the smart contract does"—binding if it programs the terms of the contract and unclear if "it is used for convenience . . . not as a framework of an offer and acceptance"); Leana Ter-Martirosyan, Note, *Smart Contract Accountability Problems: Default Oracle Liability as the Solution*, 2025 Colum. Bus. L. Rev. 587, 598-601, 607-13 (2025), https://doi.org/10.52214/cblr.v2025i1.14257 (arguing that smart contracts meet traditional requirements of offer, acceptance, and consideration to create a valid legal agreement and that proposing a framework of oracle and developer liability for failures stemming from errors in code). *See generally* Bassan & Rabitti, *supra* note 1600 (discussing advantages and limits of smart legal contracts, distinguishing code that merely automates performance from code that also embodies legal obligations).

1604 *See generally* Anna Duke, Comment, *What Does the CISG Have to Say About Smart Contracts? A Legal Analysis*, 20 Chi. J. Int'l L. 141 (2019), https://chicagounbound.uchicago.edu/cjil/vol20/iss1/4/.

1605 United Nations Convention on Contracts for the International Sale of Goods art. 11, Apr. 11, 1980, 1489 U.N.T.S. 3., https://uncitral.un.org/en/texts/salegoods/conventions/sale_of_goods/cisg.

1606 *See* Köksal & Sarel, *supra* note 1572, at 1257 (introducing the concept of the "legislators' trilemma" for smart contracts: to enforce smart contracts similarly to written contracts; to prohibit or severely restrict the scope of smart contracts; or to mandate smart contracts in situations where they potentially reduce social costs).

the parties manifested mutual assent or entered into a binding contractual obligation. Lawyers typically focus on the core elements traditionally required for contract formation and assess whether these can be reflected within the design of a smart contract. While various formulations appear in legal scholarship, the most widely accepted list includes three fundamental elements: (i) offer, (ii) acceptance, and (iii) consideration. Some frameworks also include (iv) capacity and (v) legality.

Although the analysis is usually fact-specific, the prevailing view in the United States is that established legal frameworks are, in principle, sufficiently adaptive to recognize smart contracts as valid and enforceable.[1607] U.S. contract law, grounded in an objective theory of assent, is highly accommodating to smart contract formation.[1608]

Deploying a smart contract may in some circumstances constitute an *offer* to all potential counterparties who interact with the blockchain. It could operate as a unilateral offer because performance, such as sending tokens, is usually enough to trigger automatic execution without negotiation or a return promise to perform.[1609] The offer is also likely to be sufficiently clear because it uses executable code —although it may not be necessarily clear to non-technical users, who could raise questions of mutual assent.

Interaction with a smart contract that triggers its execution may constitute *acceptance* because it is an affirmative user action "in a manner invited or required by the offeror."[1610] In practice, however, users may not fully understand the consequences of their on-chain actions, especially when the underlying smart contract code is hidden behind the user interface: Users typically interact with decentralized applications through simplified front-end interfaces that translate their inputs into transactions executed by the smart contract, without exposing the underlying code.[1611] Functionally, this dynamic resembles the logic of British common-law precedents involving automated contracting systems, such as vending machines, where acceptance occurs through interaction with a pre-programmed mechanism rather than through explicit negotiation of terms.[1612]

Finally, *consideration* is usually satisfied when there is a bargained-for exchange of something of value. In the smart contract context, each party transfers value —such as cryptocurrency, tokens, or other digital assets— or performs an on- or off-chain action in exchange for something of value, thus satisfying the consideration prong.[1613] Here, consideration issues may arise as to automatic (self-executing) transactions, where there may be no real bargain or exchange.

Some questions remain unanswered regarding the status of smart contracts, but U.S. contract law's flexibility toward recognizing contract formation elements seems to be well-suited to accommodate smart contracts on a basic level. This adaptability, exemplified by the Uniform Commercial Code's broad definition of contract as made "in any manner sufficient to show agreement," also allows courts to fill the gaps through evolving precedent.[1614]

1607 *See, e.g.*, U.C.C. art. 12 (Am. L. Inst. & Unif. L. Comm'n 2022) (creating a legal framework for digital assets and calling them "controllable electronic records"; Article 12 and related amendments have been adopted by 33 jurisdictions as of Jan 15 2026); Köksal & Sarel, *supra* note 1572, at 1267-69.

1608 *See* Restatement (Second) of Contracts § 17 (Am. L. Inst. 1981), (requiring a bargain with manifestation of mutual assent and consideration).

1609 Under U.S. contract law, offers can be unilateral, in which only one party promises to perform, or bilateral, in which both parties promise to perform. Usually, offers made generally and offered for the public to accept are unilateral offers.

1610 Restatement (Second) of Contracts § 50 (Am. L. Inst. 1981).

1611 *See id.* § 19(1) ("The manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by failure to act.").

1612 *See, e.g.*, Thornton v. Shoe Lane Parking Ltd [1970] EWCA (Civ) 2 (Eng.) (finding a contract was formed when a driver took a ticket from an automated machine).

1613 Cornell & Werbach, *supra* note 1572, at 370-71 ("A typical smart contract involves some consideration that induces the reciprocal promise.").

1614 U.C.C. § 2-204(1) (Am. L. Inst. & Unif. L. Comm'n 2002).

b. Formal Requirements

Formal requirements, like "writing" and "signature," can also be met under U.S. law.[1615] Cryptographic signatures generated by a user's private key are recognized as valid under the federal ESIGN Act, the Uniform Electronic Transactions Act (UETA), and the Uniform Commercial Code (UCC):

The **Federal Electronic Signatures in Global and National Commerce Act ("E-Sign Act")**,[1616] which took effect in 2000, applies to transactions in interstate and foreign commerce in states that have not adopted the UETA or a comparable electronic signature statute.[1617] This act permits electronic records to satisfy requirements for written documentation when introduced in interstate commerce.[1618] Contracts and signatures cannot be denied legal effect merely because they are electronic.[1619] E-SIGN expressly authorizes states to supersede its provisions by adopting UETA.

The **Uniform Law Commission–Uniform Electronic Transactions Act ("UETA")**[1620] is a model code for states to adopt that governs electronic signatures, records, and transactions. Its core provisions are set out in Sections 7(a) and 7(b), which provide that: "(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form; (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation." As of January 2026, the UETA has been adopted by 49 U.S. states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. New York has not adopted the UETA but has enacted its own electronic signatures law that recognizes the legal validity of electronic signatures.[1621]

The **Uniform Commercial Code (UCC)** is a model code to govern commercial transactions broadly. In one way or another, all U.S. jurisdictions have adopted the UCC. For UCC-governed agreements other than sales or leases of goods, electronic records and signatures are governed directly by the UCC, rather than by the ESIGN Act or the UETA. In these cases, the UCC establishes rules that are substantively equivalent to those set out in ESIGN and UETA.

In sum, despite different sources of law, the rules governing electronic signatures everywhere in the United States are "substantially the same."[1622] These statutes provide that a signature, contract, or other record may not be denied legal effect solely because it is electronic. These statutes also provide a basis for the enforceability of self-executing transactions on the blockchain through the concepts of an "automated transaction" and an "electronic agent."[1623]

1615 Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, Harv. L. Sch. Forum on Corp. Governance (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

1616 *See* Electronic Signatures in Global and National Commerce Act (ESIGN Act), 15 U.S.C. § 7001(a); Unif. Elec. Transactions Act § 7(a) (Unif. L. Comm'n 1999).

1617 15 U.S.C. § 7002.

1618 Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000).

1619 Electronic Signatures in Global and National Commerce Act § 101, 15 U.S.C. § 7001 (2000) ("a contract … may not be denied legal effect, validity, or enforceability solely because it is in electronic form").

1620 *Uniform Electronic Transactions Act* § 2, *Unif. L. Comm'n* (1999), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=9637c6eb-b80b-d7ca-72cd-1c3ee12f2b68&forceDialog=0.

1621 New York has enacted the Electronic Signature and Records Act ("ESRA") (N.Y. State Tech. Law § 301 et seq.). *See generally* N.Y. State Tech. Law § 301-09 (McKinney 2025). ESRA provides that "An electronic record shall have the same force and effect as those records not produced by electronic means." N.Y. State Tech. Law § 305 (McKinney 2025). The New York Office of Information Technology Services, which administers ESRA, has affirmed that the definition of "electronic signature" in ESRA § 302(3) aligns with the definition in the E-SIGN Act. See N.Y. Office of Info. Tech. Servs., *Electronic Signatures and Records Act (ESRA) Regulation* (Apr. 6, 2023), https://its.ny.gov/electronic-signatures-and-records-act-esra-regulation.

1622 *Comment Concerning Use of Electronic Signatures and Third-Party Opinion Letters*, Am. Bar Ass'n (Apr. 7, 2020), https://www.americanbar.org/groups/business_law/resources/business-law-today/2020-april/comment-concerning-use-of-electronic-signatures/.

1623 *See, e.g.*, Unif. Elec. Transactions Act § 2(2) (Unif. L. Comm'n 1999) (automated transactions are "transaction[s] conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction"); 15 U.S.C. § 7006(3) (electronic agents are computer programs or the like "used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response").

While this general rule of accepting electronic records extends by implication to smart contracts,[1624] several states —including Arizona,[1625] Tennessee,[1626] Illinois,[1627] and others[1628]— have expressly amended their laws to confirm that blockchain-based records and smart contracts qualify as electronic records or signatures. Many other jurisdictions have passed various statutes related to the blockchain and digital assets. Some state statutes focus on the use of distributed ledgers to maintain corporate records.[1629] Others have formed working groups to assess the usefulness of blockchain to keep records of state infrastructure.[1630] But, these do not specifically concern electronic records and regulation of smart contracts.

States adopting blockchain-specific provisions regarding electronic signatures and records have inadvertently created a novel situation in the current ESIGN Act-UETA-UCC framework. On the one hand, the states have added more guidance for parties and courts in interpreting notions like "electronic record" and "electronic agent." And they have clarified whether a smart contract satisfies the traditional requirements of contract formation. On the other hand, through these variations, states have shaken up the current legal framework applying to electronic signatures and records —a framework that had previously been largely uniform across jurisdictions. The Uniform Law Commission called these proposed and enacted frameworks "unnecessary" and "redundant."[1631] It also pointed out that legislation attempting to define a blockchain or a smart contract[1632] "differ[s] from those of industry groups and from each other."[1633] The Commission argued that such legislation does not actually achieve the intended result of making these jurisdictions "blockchain-friendly for start-ups and entrepreneurs." Instead, it creates more legal uncertainty and invites unnecessary litigation.[1634] In addition to these concerns, there is also an issue of whether such statutes become "preempted"

1624 The Uniform Law Commission, in charge of drafting uniform acts like the Uniform Electronic Transactions Act, has endorsed the view that blockchain and smart contracts are covered by the current legal framework because it was designed to apply to "all electronic technologies through broad definitions for electronic signatures and records." Unif. L. Comm'n, Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal ESIGN Act, Blockchain Technology and "Smart Contracts" 5-7 (Jan. 2019) [hereinafter 2019 ULC Guidance Note].

1625 In 2017, Arizona was the first state to pass legislation on the use of smart contracts. The law, HB 2417, formally amended the Arizona Electronic Transactions Act (AETA) to say, among other things, that signatures, contracts, and records "secured through blockchain technology" qualify as electronic signatures or electronic records See: H.B. 2417, 53d Leg., 1st Reg. Sess. (Ariz. 2017); Ariz. Rev. Stat. § 44-7061 (2017); https://legiscan.com/AZ/text/HB2417/id/1588180. The law provides that a smart contract is "an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger." The law added that "a contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term."

1626 In 2018, Tennessee issued legislation providing that a contract is not denied effect "solely because" it is executed through a smart contract; the statute also recognizes blockchain-secured records and signatures.S.B. 1662, 110th Gen. Assemb., 1st Reg. Sess. (Tenn. 2017), https://legiscan.com/TN/bill/SB1662/2017; Tenn. Code Ann. § 47-10-202 (2024).

1627 The state of Illinois, as part of its 2020 Blockchain Technology Act, prevented smart contracts from being denied legal effect or from being excluded as evidence in legal proceedings. The Blockchain Technology Act states that a "smart contract…shall not be denied legal effect or enforceability" and may not be excluded from evidence solely due to its electronic nature. See Blockchain Technology Act, 205 Ill. Comp. Stat. 730/10 (2020).

1628 Nevada (2017) passed Senate Bill 398 on June 5, 2017, stating that the "writing" requirement of a document can be legally satisfied under Nevada's UETA (*Uniform Electronic Transactions Act*) if the document is recorded on a blockchain. S.B. 398, 79th Sess. (Nev. 2017), https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB398_EN.pdf; Ohio amended its UETA in 2018 (SB 220) to state that a record or signature "secured through blockchain technology" counts as an electronic record or signature, see S.B. 300, 132d Gen. Assemb., Reg. Sess. (Ohio 2017), https://legiscan.com/OH/text/SB300/2017. Vermont adopted a law that provides that a digital record registered on a blockchain is self-authenticating (with a sworn declaration) and may be treated as a record of regularly conducted activity, unless circumstances indicate a lack of trustworthiness Admissibility and weight remain subject to ordinary evidence rules. See: Vermont House Bill 868, An act relating to miscellaneous economic development provisions, June 2 2016. *See* H. 868, 2015-2016 Bien. Sess. (Vt. 2016), http://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf.

1629 Delaware amended its General Corporation Law (DGCL, § 224) in July 2017 to allow electronic databases and blockchain technology to store and administer corporate stock ledgers, books of account, and other corporate records. That concerned corporate recordkeeping rather than a general smart-contract enforceability rule. See: S.B. 69, 147th Gen. Assemb., Reg. Sess. (Del. 2013), https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69. *See, e.g.*, Md. Code Ann., Corps. & Ass'ns § 2-114 (West 2019)

1630 *See, e.g.*, Ky. Rev. Stat. Ann. § 42.747 (West 2025).

1631 2019 ULC Guidance Note, *supra* note 1624 , at 6.

1632 In 2024 Wyoming enacted the Decentralized Unincorporated Nonprofit Association Act, which defines "smart contract "and supports on-chain governance. See Wyo. Stat. §§ 17-32-101 to -121 (2024); Lewis Rinaudo Cohen, *Wyoming Adopts New Legal Structure for DAOs*, Fintech and Digital Assets (Apr. 24, 2024), https://www.fintechanddigitalassets.com/2024/04/wyoming-adopts-new-legal-structure-for-daos/.

1633 *Id.* at 7.

1634 *Id.*

(superseded) by the ESIGN Act, completely nullifying their legal force.[1635]

There is no consensus on the issue of whether there needs to be special legislation concerning the blockchain and smart contracts. The Uniform Law Commission and some states endorse the view that UETA and other general statutes in the field "adequately encompass signatures secured by blockchain technology and smart contracts." However, there is a consensus about adjusting the current legal framework to cover specific *applications* of the blockchain and smart contracts, such as in the context of secured transactions and control over digital assets. As a result of these discussions, the Uniform Law Commission updated the UCC —a widely accepted model law— to apply to non-fiat transactions on the blockchain specifically.

c. The UCC Amendments

The Uniform Commercial Code (UCC) was amended in 2022 to modernize its treatment of digital assets and electronic transactions.[1636] The amendments replaced the requirement of a "writing" with the broader concept of a "record," thereby extending legal recognition to information stored electronically as an "electronic record."[1637] More importantly, the amendments introduced a new Article 12, which governs *Controllable Electronic Records* (CERs) —essentially, digital assets, like cryptocurrencies or tokenized records, that can be subjected to "control."[1638] In practice, if someone has the exclusive ability to use a digital asset and prevent others from using it —through holding the necessary cryptographic keys, for example— that person has control over the asset, which is different from the traditional notion of possession.[1639] The new framework gives legal weight to the concept of control. For example, if a lender obtains control of a CER, they can gain priority over other creditors (those who do not have control over the asset) without a traditionally required filing of a financial statement.[1640] Also, if a party purchases digital assets in good faith, the party takes them free of any competing claims.[1641] This is similar to how transfer of assets works with tangible property, for example, which promotes legal certainty. As of January 2026, 33 jurisdictions including New York have adopted Article 12 and related amendments, with six states introducing bills to adopt it in the near future.[1642]

These 2022 amendments to the UCC address only certain aspects related to the blockchain. They propose a framework to regulate transactions involving digital assets, primarily by extending current UCC rules of resolution of competing claims and property interests. The amendments also clarify terminology that previously

1635 The issue is whether these blockchain-specific statutes, such as the one Arizona has, are UETA-like. If they are not, then the ESIGN Act, being the federal law, must prevail. *See* Riley T. Svikhart, Essay, *Blockchain's Big Hurdle*, 70 Stan. L. Rev. (2017), https://www.stanfordlawreview.org/online/blockchains-big-hurdle/ (stating that Arizona's law is either consistent with ESIGN or ensures equal treatment of electronic signatures on the blockchain as compared to other technologies, making it non-preempted, but pointing out that it is a close call given the current preemption doctrine).

1636 Prefatory Note to Article 12, Uniform Commercial Code Amendments (2022), at 229 (Am. Law Inst. & Unif. Law Comm'n 2022), https://www.uniformlaws.org/viewdocument/final-act-164?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac&tab=librarydocuments; Alexander C. Kim, *The Promise and Potential of Blockchain and the New UCC Article 12*, Mayer Brown (Dec. 12, 2023), https://www.mayerbrown.com/en/insights/publications/2023/12/the-promise-and-potential-of-blockchain-and-new-ucc-article-12; Matthias Lehmann, *Digital Assets in the Conflict of Laws: A Comparative Search* for the 'Ideal Rule', 2024 Sing. J. Legal Stud. 197, 200 (2024), https://ssrn.com/abstract=5105124.

1637 U.C.C. § 1-201(b)(31) (Am. L. Inst. & Unif. L. Comm'n 2022) (defining "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form").

1638 U.C.C. art. 12 (Am. L. Inst. & Unif. L. Comm'n 2022).

1639 *See* Overview of 2022 Amendments to the Uniform Commercial Code—Emerging Technologies, Unif. L. Comm'n 1-2 (2022); U.C.C. § 12-105 (Am. L. Inst. & Unif. L. Comm'n 2022) (a person has control of a CER if they (1) have the power to avail themselves of substantially all the benefit from the record, the exclusive power to prevent others from doing so, and the exclusive power to transfer control of the record to another, and (2) can readily identify themselves—by name, number, cryptographic key, or other means—as the person possessing those powers).

1640 *See generally* U.C.C. art. 9 (Am. L. Inst. & Unif. L. Comm'n 2010) (as amended in 2022).

1641 U.C.C. §§ 12-104(d)-(e), 12-102(a)(2) (Am. L. Inst. & Unif. L. Comm'n 2022).

1642 *UCC, 2022 Amendments to: Legislative Bill Tracking*, Unif. L. Comm'n, https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac#LegBillTrackingAnchor (last visited Jan. 15, 2026).

applied to transactions on paper and tangible money, as well as conflict of laws questions. Importantly, however, the scope of these rules is limited to digital assets themselves and the rights of parties who control or transfer them. They "do not regulate the use of CERs, address the taxation of CERs, alter the law governing money transmitters, or revise anti-money laundering rules." In short, Article 12 does not regulate *how* smart contracts or blockchain systems operate or should be treated.[1643]

2. In European Countries

In Europe, doctrinal debates on *smart legal contracts* have centered on their compatibility with the foundational principles of the civil-law tradition. Unlike the common-law approach, which focuses primarily on offer, acceptance, and consideration, civil-law systems situate contract formation within a diverse yet broadly normative framework that generally focuses on the declaration of intent, a lawful object, and the principle of good faith. This raises questions about whether agreements expressed solely in code can satisfy the formal and substantive requirements of civil-law contracts.

The European Law Institute (ELI) has undertaken the most systematic analysis of these issues in its *Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (2022).[1644] The report identifies several areas of concern: (i) whether offer and acceptance can be validly expressed using code; (ii) how to recognize and assign responsibility to contracting parties in decentralized networks; (iii) whether automated "clauses" in smart contracts comply with law, including consumer protection laws; (iv) how to ensure that consumers and other weaker parties receive equivalent protection both in on-chain and off-chain contracts; (v) how to prevent automation and immutability from negatively impacting fairness and legal protections; and (vi) whether dispute resolution is possible fully on-chain.

More specifically, the ELI's framework offers guidance for applying existing law to this new technology. Key provisions include:

- Principle 5 (Legal Nature of Transactions): A transaction on a blockchain can constitute a contractual declaration (e.g., an offer or acceptance) if, based on the circumstances, it can be reasonably understood as a declaration of will attributable to a party.[1645]
- Principle 7 (Formal and Substantive Validity): Formal legal requirements, such as a requirement for a contract to be in writing, should be deemed fulfilled if the use of blockchain technology serves the same underlying purpose (functional equivalence, *See section 1.3.2*).[1646]
- Principle 9 (Off-Chain Prevails over On-Chain): In a hybrid contract, the terms of the off-chain, natural-language agreement prevail over any conflicting conditions in the on-chain code, unless the parties have explicitly agreed otherwise. This principle is a vital safeguard for ensuring that the parties' original intent is honored[1647]and functions as a corrective mechanism against unintended automated outcomes.
- Principle 10 (Unwinding by Reverse Transaction): Acknowledging the immutability of most ledgers, the ELI recommends that, where the law requires a transaction to be unwound, this should normally

1643 *See for further discussion* Heather Hughes, *Blockchain and the Future of Secured Transactions Law*, 3 Stan. J. Blockchain L. & Pol'y 1 (2020), https://stanford-jblp.pubpub.org/pub/blockchain-secured-transactions/release/1.

1644 *See* ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, at 27-50 (2023), https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf.

1645 *Id.* at 29.

1646 *Id.* at 33.

1647 *Id.* at 35.

> be accomplished by executing a new, "reverse" transaction on-chain, rather than attempting to alter the historical record.[1648]

Scholars have examined how the automation of performance interacts with traditional doctrines of consent. For example, Michel Cannarsa argues that contracts written in computer code are less likely to be ambiguous and subject to disputes over the meaning of individual provisions. The code either executes the contract or does not. But this precision is double-edged: The rigidity that eliminates ambiguity also eliminates flexibility. This so-called "dry code" limits the courts' ability to correct inequitable outcomes and prioritize the literal meaning over the intent of the parties.[1649] Some parties may find it difficult to modify or terminate a contract. Similarly, Mateja Durovic and Chris Willett warn that, while smart contract automation can make transactions faster and more reliable, it might also harm the efficacy of laws, such as consumer protection laws, by reducing human involvement in deciding complex issues of fairness.[1650] Marisaria Maugeri argues that smart contracts must be supplemented by corrective and protective mechanisms of European law so that governments and courts can provide remedies based on fairness to parties, especially weaker ones.[1651]

These analyses reveal an emerging consensus among European scholars that smart contracts can serve as a substitute for performance automation, but they need to meet the traditional requirements of offer, acceptance, and consent[1652]. Experts also caution that there are inherent risks to substantive justice arising from automation; smart contracts cannot circumvent existing consumer protection, fairness, and other important rules governing public policy.[1653]

3. The United Kingdom

The United Kingdom also made progress in passing legislation legitimizing different aspects of smart contracts and blockchain transactions, similar to the United States. In 2023, the United Kingdom passed the Electronic Trade Documents Act, which gives electronic documents the same legal effect as their paper counterparts —a similar approach to the one outlined in the U.S.'s UETA.[1654] But even before this legislation was adopted, U.K. courts were already adapting to the new kinds of commerce. In a line of cases since 2019, courts have endorsed the view of the UKJT's *Legal Statement* and held that cryptocurrency could be treated as property.[1655]

Courts have also found a way around the issue of decentralized networks obscuring the identities of real

---

1648 *Id.* at 35.

1649 Michel Cannarsa, *Contract Interpretation*, *in* The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms 111-12 (Larry A. DiMatteo, Michel Cannarsa & Cristina Poncibò eds., 2020).

1650 *See generally* Mateja Durovic & Chris Willett, *A Legal Framework for Using Smart Contracts in Consumer Contracts: Machines as Servants, Not Masters*, 86 Mod. L. Rev. 1390 (2023), https://repository.essex.ac.uk/35781/1/Modern%20Law%20Review%20-%202023%20-%20Durovic%20-%20A%20Legal%20Framework%20for%20Using%20Smart%20Contracts%20in%20Consumer%20Contracts%20%20Machines%20as.pdf.

1651 *See generally* Marisaria Maugeri, *Smart Contracts, Consumer Protection, and Competing European Narratives of Private Law*, 23 German L.J. 900 (2022), https://doi.org/10.1017/glj.2022.58.

1652 Even scholars arguing that code can produce legally meaningful effects such as "de facto property rights" acknowledge that state involvement will remain necessary to "fill loopholes in enforcement and to curb undesirable abuses of property without law".*See* Stefan Bechtold, Giuseppe Dari-Mattiacci, Edoardo D. Martino & Gideon Parchomovsky, *Property Without Law: Personalized Property Rights Through Smart Contracts on the Blockchain*, Amsterdam Center for Law & Economics Working Paper No. 2025-04, Yale J. on Reg. (forthcoming 2026) https://ssrn.com/abstract=5497820.

1653 For example, some of these principles regarding smart contracts have been embodied in the Data Act, which became applicable on September 12, 2025 (See section 7.3.3.A). Article 36 of the Act that governs "smart contracts for executing data sharing agreements" lists requirements for deployed smart contracts. They include the integrity of access control, the ability to terminate or interrupt automated execution, auditability, and "consistency . . . with the terms of the data sharing agreement that the smart contract executes," which implies that its code must operate within contractual terms of the data sharing agreement and comply with applicable civil, contractual, and consumer protection laws and regulations. Regulation (EU) 2023/2854, of the European Parliament and of the Council of December 13, 2023, on Harmonized Rules on Fair Access and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1818 (Data Act), 2023 O.J. (L 2854) 1, 62-63, https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

1654 Electronic Trade Documents Act 2023, c. 38, §§ 3(2)-(3) (Eng.).

1655 *See, e.g.*, AA v. Persons Unknown [2019] EWHC (Comm) 3556 [3-4] (Eng.); Zi Wang v. Graham Darby [2021] EWHC (Comm) 3054 [2-3] (Eng.).

defendants. In *D'Aloia v. Persons Unknown & Others*, the High Court allowed the notification of unknown defendants hidden behind private addresses on the blockchain of the pending lawsuit against them (service of proceedings) via alternative means —by allowing service via a non-fungible token sent to their addresses.[1656] Although *D'Aloia* is a fraud case, its reasoning may be instructive in the context of smart contracts. The party that deployed a smart contract cannot easily be identified because it operates behind a pseudonymous blockchain address. The case suggests that legal proceedings may, nevertheless, be brought against unknown or unidentified defendants. In principle, therefore, the pseudonymous nature of blockchain interactions does not entirely prevent a claimant from seeking judicial remedies in the event of breach.

In sum, the United Kingdom has made it clear that its current legal framework can accommodate smart contracts —that only "incremental and principled development of the common law" would be necessary to accommodate them.[1657] It is pursuing a flexible, common law-centric approach that relies on evolving case law.

6.5.2.B. Limitations of Smart Contracts

The absence of natural language in smart contracts poses a fundamental challenge for their legal significance, specifically in terms of legal interpretation and adaptability. Scholars often refer to the "dark side" of smart contracts to describe the risks inherent in automating legal relationships through code —particularly the rigidity and irreversibility that result from immutability.[1658] Computer code can carry out agreements in a precise and automatic manner; but, it also has drawbacks.

First, computer code can capture only a limited subset of human intent —those aspects that can be formalized into machine-readable logic. Consequently, when human language, with its interpretive richness, is translated into programming language, part of its semantic and normative content is lost or distorted. This could be described as the *incompleteness* of contracts. In traditional contract theory, a contract is incomplete when it cannot foresee or specify all possible future contingencies or when its terms are too vague or open-ended to be perfectly enforceable.[1659] In the context of smart contracts, incompleteness reflects the gap between the legal meaning of the parties' agreement and what the code is actually capable of performing.[1660]

Second, automation eliminates the flexibility traditionally afforded by contract law. Code is an imperfect tool to express flexible legal terms, like "reasonable" or "good faith." It leaves little room for human judgment and interpretation. Once deployed, a smart contract executes precisely as programmed, without the possibility of human intervention or judicial restraint —even when performance becomes unjust, mistaken, or unlawful.[1661]

1656 *See generally* D'Aloia v. Persons Unknown [2024] EWHC (Ch) 2342.

1657 Advice to Government, *supra* note 1590, at 5.

1658 Massimiliano Vatiero, *The "Dark Side" of Smart Contracts: A Contract Theory Perspective*, 21 Eur. Mgmt. Rev. 516, 517-18 (2024) (arguing that smart contracts can actually create additional transaction costs because of their lack of adaptability that many parties seek from contractual arrangements).

1659 Oliver Hart & John Moore, *Foundations of Incomplete Contracts* 36-38 (Nat'l Bureau of Econ. Rsch., Working Paper No. 6726, 1998), https://www.nber.org/system/files/working_papers/w6726/w6726.pdf.

1660 "Most contracts are incomplete, in the sense that they do not specify an outcome for every possible state of the world. Courts can fill in the blanks when the contractual expression of the parties' intent is unclear. With a smart contract, this approach is foreclosed." Cornell & Werbach, *supra* note 1572, at 369. *See also* Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 9 Law, Innovation & Tech. 269, 290-92 (2017); *see also* Jeffery M. Lipshaw, *The Persistence of "Dumb" Contracts*, 2 Stan. J. Blockchain L. & Pol'y 1 (2019), https://stanford-jblp.pubpub.org/pub/persistence-dumb-contracts/release/1 (arguing that code cannot replicate the "infinite regress" of human judgment required for normative legal determination).

1661 Cuccuru, *supra* note 1582, at 189 ("the semantic barrier affects the reviewability of code-expressed and computer-executed agreements"); Paul Catchlove, Smart Contracts: A New Era of Contract Use 11-13 (Dec. 1, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090226 (describing issues of reviewability of smart contracts).

As a result, the automatic execution of smart contracts whose purpose or effect contravenes mandatory legal rules or public policy cannot be halted. The determinism inherent in smart contract code also precludes adaptation to unforeseen circumstances or to the parties' evolving intentions. Consequently, interpreting contractual provisions or granting equitable remedies becomes difficult, if not impossible, when performance fails.

Third, the absence of natural language in smart contract code raises concerns regarding the parties' awareness and comprehension of the coded terms. Since most individuals lack the ability to understand or review code, asymmetries of understanding and consent inevitably arise. Because the provisions of a smart legal contract are executed according to predetermined code, rather than interpreted in light of the parties' intent or governing legal norms, the system may perform actions that diverge from what the parties originally intended in context.[1662] A single bug or logical error can produce irreversible and potentially catastrophic consequences.[1663] This issue is particularly acute in sectors such as banking and finance, where transparency and intelligibility are fundamental to ensuring fair dealing.[1664] Accordingly, a critical question emerges: Who bears responsibility for verifying that the coded version faithfully represents the parties' shared intent? In this context, parties, lawyers, and courts may become increasingly dependent on technical experts.[1665] Although smart contracts eliminate the risk of *ex post* breach through automatic execution, they shift the risk to "ex ante formalization[]" flaws in the code.[1666] Consequently, the focus of legal practice may move from litigation toward pre-deployment auditing and "responsible intermediaries."[1667] The "good" middleman will be the legal or technical expert who ensures the code accurately reflects the parties' intent before it becomes irreversible.[1668]

Finally, the pseudonymity of blockchain participants makes it particularly challenging to apply traditional contract-law safeguards to smart contracts. These difficulties include verifying contractual capacity[1669] and invoking doctrines that address duress, mistake, or fraud.[1670]

These challenges are not merely theoretical. As the following case study illustrates, the pseudonymity and autonomy of blockchain-based protocols can place their operators beyond the reach of certain forms of enforcement, while leaving the human architects behind those systems exposed to criminal liability.

1662 Cornell & Werbach, *supra* note 1572, at 346; Matt Blaszczyk, *Decentralized Autonomous Organizations and Regulatory Competition: A Race Without a Cause*, Univ. of Mich. Law Sch. Schol. Rep., 108, 114 (2024), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1008&context=research. (suggesting that smart contracts cannot themselves establish the legal status quo and will have to remain subject to and compatible with the law).

1663 For a review of the security vulnerabilities of Ethereum smart contracts, see Nicola Atzei, Massimo Bartoletti & Tiziana Cimoli, *A Survey of Attacks on Ethereum Smart Contracts*, 10204 Proc. of the 6th Int'l Conf. on Principles of Sec. & Tr. 164 (2017). The number of such incidents has only been increasing.

1664 Cornell & Werbach, *supra* note 1572, at 318; Christopher D. Clack & Ciarán McGonagle, *Smart Derivatives Contracts: The ISDA Master Agreement and the Automation of Payments and Deliveries*, arXiv 9 (Apr. 1, 2019), https://arxiv.org/abs/1904.01461 ("To ensure financial services sector confidence in the accuracy and reliability of smart derivatives contracts, it is essential that the final version of the smart contract code behaves in a manner that is faithful to the legal agreement."). *See generally* Christopher D. Clack, Vikram A. Bakshi & Lee Braine, *Smart Contract Template: Foundations, Design Landscape and Research Directions*, arXiv (Aug. 2, 2016), https://arxiv.org/abs/1608.00771.

1665 De Filippi & Wright, *supra* note 1576, at 78.

1666 Farshad Ghodoosi, *Contracting in the Age of Smart Contracts*, 96 Wash. L. Rev. 51 (2021) (quoting Kevin Werbach, The Blockchain and the New Architecture of Trust 163 (2018)), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=5156&context=wlr.

1667 William F. J. Ardinger et al., Comm'n on Cryptocurrencies & Digit. Assets, Report of Governor's Sununu's Commission on Cryptocurrencies and Digital Assets app. A at 5 (Dec. 21, 2022), https://www.governor.nh.gov/sites/g/files/ehbemt336/files/inline-documents/sonh/cryptocurrencie-report.pdf ("crypto cuts out the middle man, but sometimes the middle man is good").

1668 Nick Hsu & Jagjit S. Sahota, *Interpreting Smart Contracts: The Reasonable Coder and the Need for a Stronger Contextual Approach*, 12 Oxford Univ. Undergraduate L.J. 146, 147, 167 (2023) (arguing that adaptation of an agreement to code and subsequent interpretation will require the help of expert coders), https://www.law.ox.ac.uk/sites/default/files/inline-files/OUULJ%2012th%20Edition_Interpreting%20Smart%20Contracts-%20the%20Reasonable%20Coder%20and%20the%20need%20for%20a%20Stronger%20Contextual%20Approach.pdf.

1669 *See Legal Risks of Smart Contracts: Enforceability Explained*, LegalGPS (Nov. 23, 2024), https://www.legalgps.com/crypto/legal-risks-smart-contracts-enforceability.

1670 *See* Tiffany M. Sillanpää, *Freedom to (Smart) Contract: The Myth of Code and Blockchain Governance Law*, 7 IALS Student L. Rev. 38, 42-43 (2020), https://journals.sas.ac.uk/lawreview/issue/view/582.

6.5.3. Case Study: Tornado Cash

6.5.3.A. What Is Tornado Cash?

Tornado Cash is a non-custodial privacy protocol[1671] deployed on Ethereum (and, in some instances, on other blockchains). The litigation discussed in this section concerns the Ethereum deployment. Tornado Cash enables users to obscure the on-chain link between the source and destination of cryptocurrency transfers.[1672] Tornado Cash operates through a set of open-source smart contracts that enable users to deposit tokens from one blockchain address into the protocol. The smart contracts pool and mix tokens from multiple users' deposits, thereby obfuscating the link between the sender and the recipient. Using cryptographic proofs, users may withdraw an equivalent number of tokens to a different address, optionally after a delay, effectively breaking the public traceability of transactions that typically characterizes blockchain systems. As a result, users may withdraw and use their funds without revealing their complete transaction history to third parties.[1673] Each liquidity pool constitutes an independent smart contract, accessible to any user without intermediaries.

Governance of the protocol is exercised through a decentralized autonomous organization (DAO) that issues the Tornado Cash governance token (TORN), which allows holders to vote on protocol parameters and updates.[1674] No singular entity or individual controls the core Tornado Cash contracts, which are immutable and operate autonomously once deployed.

Although Tornado Cash is designed as a blockchain-based privacy tool, rather than a custodial "mixing service," its functionality *can* be used to obscure the provenance of assets by commingling legitimate and illicit funds.[1675] In practice, it has been employed both by users seeking financial privacy and by users wanting to cover up their criminal activities.

6.5.3.B. Legal Proceedings

1. The Bar on Using Tornado Cash

In August 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned a series of Tornado Cash smart contract addresses under its Specially Designated Nationals and Blocked Persons (SDN) list.[1676] The agency alleged that Tornado Cash had, since its creation, facilitated the laundering of more than $7 billion in cryptocurrency. The $7 billion included $455 million allegedly stolen by the Lazarus Group, a North Korea-sponsored cybercrime organization, and approximately $96 million associated with the June 2022 Harmony Bridge hack.[1677] The action was widely viewed as novel because OFAC treated smart-contract addresses —open-source code deployed on-chain— as blocked "property" on the SDN list, rather than targeting

1671 A *non-custodial privacy protocol* is a system in which no intermediary takes custody or control of users' funds. Instead, assets remain under users' control and transactions are executed automatically by smart contracts, while privacy mechanisms obscure the link between sending and receiving addresses.

1672 *Introduction to Tornado Cash*, Tornado, https://docs.tornado.ws/ (last visited Jan. 15, 2026).

1673 Alex Wade, Michael Lewellen & Peter Van Valkenburgh, *How Does Tornado Cash Work?*, CoinCenter (Aug. 25, 2022), https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/.

1674 *Id. See also Tornado Cash Markets*, CoinMarketCap, https://coinmarketcap.com/currencies/torn/ (last visited Jan. 15, 2026).

1675 Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

1676 Van Loon v. U.S. Dep't of the Treasury, 122 F.4th 549 (5th Cir. 2024). *See also* Soo-Mi Rhee et al., *Fifth Circuit Limits OFAC's Sanctioning Authority*, Arnold & Porter (Dec. 11, 2024), https://www.arnoldporter.com/en/perspectives/advisories/2024/12/fifth-circuit-limits-ofacs-sanctioning-authority; Gina M. Parlovecchio et al., *Federal Appeals Court Tosses OFAC Sanctions on Tornado Cash and Limits Federal Government's Ability to Police Crypto Transactions*, MAYER BROWN (Dec. 3, 2024), https://www.mayerbrown.com/en/insights/publications/2024/12/federal-appeals-court-tosses-ofac-sanctions-on-tornado-cash-and-limits-federal-governments-ability-to-police-crypto-transactions.

1677 Press Release, *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft,* Fed. Bureau of Investigation (Jan. 23, 2023), https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft.

only rather than a natural person, corporate entity, or traditional property interest.[1678]

The direct legal effect of this action was to prohibit U.S. persons from engaging in any transaction with the sanctioned Tornado Cash contracts. The sanctions also had substantial indirect effects: Services such as Github took down Tornado Cash's code repository and suspended its developers' accounts,[1679] while certain block builders and other third parties began refusing to process transactions involving Tornado Cash addresses.[1680] These developments were widely interpreted as a challenge to the principle of *blockchain neutrality* —the idea that network participants should process all valid transactions impartially, according to protocol rules and irrespective of their origin or content.[1681]

2. The Trial Court's Decision

Members of the crypto community, such as CoinBase, a leading exchange, and Tornado Cash users, responded to OFAC's sanction of Tornado Cash by contesting the action on two principal grounds. First, they said sanctioning code development threatened programmers' ability to write and publish open-source software. Second, they said that sanctioning the use of neutral technology risked inhibiting blockchain users' capacity to preserve transactional privacy. Such precedents, critics argued, could have a chilling effect on the development of privacy-enhancing technologies, discouraging innovation whenever potential misuse by illicit actors might expose developers to liability.

Coinbase financed a lawsuit by Tornado Cash users to contest OFAC's action. The plaintiffs argued that Tornado Cash is merely software and thus cannot be sanctioned under the International Emergency Economic Powers Act (IEEPA),[1682] which authorizes sanctions only against a foreign "national" or "person."[1683] The plaintiffs argued that smart contracts operate autonomously without human control; therefore, they are not "property" owned by anyone, not even individuals who possess certain cryptocurrency tokens. They further alleged that OFAC's action violated the U.S. Constitution's First Amendment by preventing thousands of U.S. citizens from using the software for constitutionally protected speech, including socially valuable forms of expression.

A federal district court rejected these arguments, holding that Tornado Cash was "an association within the ordinary meaning of the term" and therefore "an entity that may be designated per OFAC regulations".[1684] The court further found that Tornado Cash's smart contracts *are* "property" and that Tornado Cash held a beneficial interest in them. It concluded that the smart contracts could therefore be treated as sanctionable interests under IEEPA, characterizing the smart contracts as a form of code-enabled unilateral contract.[1685]

1678 Blender.io was the first cryptocurrency mixer sanctioned by OFAC, but it was centralized and custodial, operated by identifiable persons. On May 6, 2022, OFAC sanctioned Blender.io, saying that it was used by the Democratic People's Republic of Korea (DPRK) to launder over $20.5 million of illicit proceeds. Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Operators of Cryptocurrency Mixers Charged with Money Laundering (Jan. 10, 2025), https://www.justice.gov/archives/opa/pr/operators-cryptocurrency-mixers-charged-money-laundering.

1679 Mike Dalton, *Circle, GitHub Comply with Tornado Cash Sanctions*, CRYPTO BRIEFING (Aug. 8, 2022), https://cryptobriefing.com/circle-github-comply-with-tornado-cash-sanctions/.

1680 Anders Brownworth et al., Fed. Rsrv. Bank of N.Y., Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash 19-25 (2024), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1112.pdf.

1681 Primavera De Filippi & Morshed Mannan, *Tornado Cash: The End of Blockchain Neutrality*, ZINE (Dec. 6, 2022), https://zine.zora.co/tornado-cash-primavera-de-filippi-morshed-mannan.

1682 A U.S. law that authorizes the President to impose sanctions and take other emergency steps that regulate international commerce. *See* 50 U.S.C. §§1701-07.

1683 Complaint at 3, Van Loon v. U.S. Dep't of Treasury, No. 6:22-cv-00920-ADA-JCM (W.D. Tex. Sept. 8, 2022), ECF No. 1, https://storage.courtlistener.com/recap/gov.uscourts.txwd.1188185/gov.uscourts.txwd.1188185.1.0.pdf.

1684 Van Loon v. U.S. Dep't of Treasury, 688 F. Supp. 3d 454, 466-67 (W.D. Tex. 2023), *rev'd and remanded sub nom.* Van Loon v. Dep't of the Treasury, 122 F.4th 549 (5th Cir. 2024).

1685 *Id.* at 468.

3. The Appeal

In a pivotal ruling on November 26, 2024, the Fifth Circuit U.S. Court of Appeals overturned the lower court decision. While noting that mixers are a "go-to tool" for cybercriminals, the court held that OFAC had exceeded its statutory authority by sanctioning the immutable smart contracts at the core of Tornado Cash.[1686] The court's reasoning turned on the distinction between Tornado Cash's mutable governance smart contracts and immutable core smart contracts.[1687] It reasoned that the latter could not constitute "property" under IEEPA because property must be capable of having owners, which entails control and the right to exclude others. Tornado Cash's immutable smart contracts operate autonomously and beyond the control of any party, including their original developers,[1688] who have irrevocably relinquished control to the immutable programs upon deployment. Consequently, no person or entity could be deemed to "own" the immutable smart contracts which, instead, function as public, autonomous software tools.[1689]

The court further held that immutable smart contracts are not "contracts" for purposes of IEEPA, as they lack any reciprocal agreement between parties, without an offeror or contracting party. They represent unilateral interactions with autonomous code —software that executes predefined instructions, not mutual assent. Nor are they "services," since no human effort is expended in their operation. Smart contracts may facilitate a service, but they are a "tool" used in the performance of a service, not the service itself.[1690] In other words, smart contracts are not automated contracts, like those formed with a vending machine; they are software only.[1691]

After the Fifth Circuit's November 26, 2024 decision, Treasury later exercised its discretion to delist Tornado Cash on March 21, 2025.[1692] A district court in the Western District of Texas, heeding the Fifth Circuit's ruling, also entered an amended judgment finding the sanctions unlawful and enjoining their enforcement.[1693] The government did not appeal.[1694] In the meantime, the delisting did not affect the ongoing criminal proceedings against Tornado Cash's founders. Roman Storm and Roman Semenov were charged in the Southern District of New York with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and conspiracy to violate sanctions by aiding North Korea's Lazarus Group.[1695] U.S.-based developer Roman Storm was convicted of conspiring to operate an unlicensed money transmitting business, although the jury deadlocked on the remaining counts of money laundering and sanctions violations.[1696] Storm's conviction is being contested through post-trial motions. His co-founder, Alexey Pertsev,[1697] was convicted and sentenced to 64 months imprisonment in the Netherlands for aiding

1686 Van Loon v. Dep't of the Treasury, 122 F.4th 549, 559, 571 (5th Cir. 2024).

1687 *See id.* at 565-71.

1688 *Id.* at 568-69.

1689 *Id.* at 568.

1690 *Id.* at 570.

1691 *Id.* at 569.

1692 Press Release, U.S. Dep't of the Treasury, *Tornado Cash Delisting* (Mar. 21, 2025), https://home.treasury.gov/news/press-releases/sb0057.

1693 Amended Final Judgment at 1, Van Loon v. U.S. Dep't of Treasury, No. 1:23-cv-00312-RP (W.D. Tex. Apr. 28, 2025), ECF No. 111.

1694 Joint Motion to Vacate and Remand with Instructions to Dismiss at 2, Coin Ctr. v. Sec'y, U.S. Dep't of Treasury, No. 23-13698-E (11th Cir. June 20, 2025), ECF. No. 62.

1695 *See generally* Indictment, United States v. Storm, No. 1:23-cr-00430 (S.D.N.Y. Aug. 21, 2023), https://www.justice.gov/usao-sdny/file/1311391/dl?inline.

1696 Luc Cohen, *US Jury Deadlocks on Tornado Cash Founder's Money Laundering Charge*, Reuters (Aug. 6, 2025), https://www.reuters.com/legal/government/us-jury-deadlocks-tornado-cash-founders-money-laundering-charge-2025-08-06/.

1697 MK Manoylov, *Netherlands Indictment Alleges Alexey Pertsev Aided in Laundering $1.2 Billion Through Tornado Cash: Report*, The Block (Mar. 19, 2024), https://www.theblock.co/post/283515/netherlands-indictment-alleges-alexey-pertsev-aided-in-laundering-1-2-billion-through-tornado-cash-report.

money laundering.[1698] The third co-founder of Tornado Cash, Roman Semenov, remains at large.

6.5.3.C. Doctrinal Significance

The Tornado Cash case illustrates the growing complexity and doctrinal uncertainty surrounding DAOs, smart contracts, and liability within decentralized ecosystems. The Fifth Circuit's appellate decision drew a clear legal distinction between immutable and mutable smart contracts, holding that immutable smart contracts do not constitute "property" under the IEEPA. This reasoning supports the view that truly autonomous, decentralized code may occupy a zone of alegality *(See section 6.1.3)*, existing beyond the state's direct capacity for regulation or control. Yet this ruling and others regarding the people involved in the illegal activity simultaneously underscore that human actors remain within the reach of the law. Although the code itself was deemed beyond OFAC's authority, criminal charges against Tornado Cash's founders proceeded.

Significant questions remain regarding the legal status of decentralized protocols and legal responsibility for harms or criminal conduct they cause or facilitate. The Fifth Circuit declined to determine whether Tornado Cash qualified as an "entity" or whether it had an "interest" in the immutable smart contracts.[1699] The court emphasized that extending statutory authority to cover decentralized technologies is a matter for Congress, and declined to broaden the statute through interpretation.[1700] Moreover, the court's reasoning applied only to immutable contracts and left unresolved whether *mutable* contracts —those still subject to human modification— could fall within the scope of sanctionable "property."[1701] As a result, the legal status of mutable smart contracts and DAOs as sanctionable entities remains uncertain.[1702]

While autonomous code may be alegal, its human designers, maintainers, and users are not. The emerging legal distinction between uncontrollable code and upgradeable systems poses a central dilemma for developers: Immutability may provide a shield against certain forms of regulation, yet upgradeability remains essential for correcting vulnerabilities, adapting to evolving technological and legal environments, and responding to illegal conduct on the blockchain.[1703] Ultimately, the decision also left intact the broader sanctions regime, which continues to prohibit dealings with custodial cryptocurrency mixers and sanctioned entities, including custodial cryptocurrency mixing services and exchanges.[1704]

The Tornado Cash litigation underscores that, while code may operate autonomously, legal responsibility ultimately attaches to identifiable human actors. There is a paradox here: The Fifth Circuit's reasoning —that immutable code has no owner, cannot be controlled, and therefore cannot be sanctioned— effectively confirms the alegality thesis for autonomous code, while simultaneously demonstrating its limit: alegality protects the code, not the humans who designed it. Yet even when human responsibility

1698 Elizabeth Napolitano, *Tornado Cash Developer Alexey Pertsev Sentenced to 64 Months: Report*, The Block (May 14, 2024), https://www.theblock.co/post/294322/tornado-cash-developer-found-guilty-alexey-pertsev-money-laundering-charges-to-serve-five-year-prison-sentence.

1699 Van Loon v. Dep't of the Treasury, No. 23-50669, slip op. at 22 (5th Cir. Nov. 26, 2024); *see also* Andrew W. Shoyer & Carys Golesworthy, *Fifth Circuit Issues Rare Finding: Office of Foreign Assets Control Exceeded Authority in Sanctioning Cryptocurrency Software*, Sidley Austin LLP (Dec. 5, 2024), n.16, https://www.sidley.com/en/insights/newsupdates/2024/12/fifth-circuit-issues-rare-finding.

1700 Van Loon, *supra* note 1676, at 33.

1701 Van Loon, *supra* note 1676, at 28, 33.

1702 *See generally Global FinTech Series: 2024 Review and 2025 Outlook / Digital Asset Disputes*, Norton Rose Fulbright (Jan. 2025), https://www.nortonrosefulbright.com/en-pl/knowledge/publications/6bf1f774/digital-asset-disputes-2024-review-and-2025-outlook.

1703 *See* Joshua Morris, *Smart Contracts Under Legal Scrutiny: Implications of Recent Court Rulings*, LETSEXCHANGE (Apr. 30, 2025), https://letsexchange.io/blog/implications-of-recent-court-rulings/.

1704 Peter E. Jeydel, *Tornado Cash Whiplash – What's Next for Sanctions?*, Troutman Pepper Insights (Feb. 4, 2025), https://www.troutman.com/insights/tornado-cash-whiplash-whats-next-for-sanctions.html.

can be established, a further set of challenges emerges: determining which court has authority to adjudicate blockchain disputes and which substantive law should govern them. These jurisdictional and choice-of-law questions, examined in the following section, add yet another layer of complexity to blockchain's legal landscape.

6.6. INDETERMINACY IN JURISDICTION, FORUM, AND APPLICABLE LAW FOR BLOCKCHAIN TRANSACTIONS

The legal uncertainty surrounding blockchain code and its various applications, such as smart contracts and DAOs, is compounded by the question of how disputes arising from these systems should be resolved.[1705] Even when legal responsibility can be established, as discussed in previous sections, determining the competent jurisdiction and identifying the applicable law present profound challenges given blockchain's distinctive characteristics.[1706] Jurisdiction and choice-of-law questions have long been difficult to resolve for network-based technologies such as the internet. Blockchain systems, however, intensify these difficulties because they are not only transnational but also decentralized, with participants, nodes, and effects dispersed across multiple jurisdictions without a clear territorial anchor.[1707] Blockchain transactions and smart contracts thus raise complex questions about adjudicatory authority and governing law, since traditional connecting factors —such as territory, domicile, or place of performance— are often indeterminate or absent entirely.

6.6.1. Conflict-of-Laws and Jurisdictional Challenges in Blockchain Systems

In most international contractual disputes, the applicable law and competent jurisdiction are determined in advance through contractual clauses. When a contract is silent on these matters, courts generally apply principles of private international law —such as the "closest connection" test—[1708] to identify the appropriate governing law. For jurisdictional questions such as where to bring the case, in the United States, for example, courts typically apply the "purposeful availment" (for contracts) or "purposeful direction" (for wrongful conduct)[1709] to online transactions;[1710] but, similar concepts exist in other common law and civil law jurisdictions.[1711] They assess jurisdiction based on whether the parties purposefully

1705 *See generally* on challenges in dispute resolution in DAOs: Bianca Kremer, *Code, Community, and Conflict: DAO Disputes*, *in* Kevin Werbach, Eva Micheler, and Bianca Kremer (eds), Foundations of Decentralized Organizations : Blockchain and the Future of Corporate Law, 184-214 (OUP, 2026), https://doi.org/10.1093/law/9780198946113.003.0011.

1706 While questions of jurisdiction and forum determine which court may hear a dispute, conflict-of-laws rules address the distinct question of which substantive law applies to the merits of the case.

1707 *See* Gérardine Goh Escolar, *The Role and Prospects of Private International Law Harmonisation in the Area of DLT*, *in* Blockchain and Private International Law 13-14 (Andrea Bonomi, Matthias Lehmann & Shaheeza Lalani eds., 2023), https://www.researchgate.net/publication/375631728_The_Role_and_Prospects_of_Private_International_Law_Harmonisation_in_the_Area_of_DLT-NC-ND_40_License_httpcreativecommonsorglicensesCC-BY-NC-ND40; Florence Guillaume, *Aspects of Private International Law Related to Blockchain Transactions*, *in* Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law 70-71 (Daniel Kraus, Thierry Obrist & Olivier Hari eds., 2019).

1708 *See* Guillaume, *supra* note 1707, at 63, 64.

1709 "A purposeful availment analysis is most often used in suits sounding in contract. A purposeful direction analysis, on the other hand, is most often used in suits sounding in tort." Schwarzenegger v. Fred Martin Motor Co., 374 F.3d 797, 802 (9th Cir. 2004) (cleaned up).

1710 In the U.S. context, this assumes that most plaintiffs prefer to sue in their home state, which would require specific jurisdiction and trigger the "purposeful availment" test, not in the state where their counterparty or a company operating a platform is based (for which general jurisdiction is required).

1711 For example, Canada uses the "real and substantial connection" test, see Club Resorts Ltd. v. Van Breda, [2012] S.C.R. 572 (Can.), https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/8004/index.do; Australia uses a similar test for cases that involve the internet, *see* Dow Jones & Co, Inc. v. Gutnick, Melb. J. Int'l L, https://law.unimelb.edu.au/__data/assets/pdf_file/0007/1680343/Garnett.pdf (discussing Dow Jones & Co, Inc. v. Gutnick (2002) 210 CLR 575 (Austl.)); and the United Kingdom requires some form of voluntary submission or targeting, see Bitar v. Banque Libano-Française [2021] EWHC (QB) 2787 (Eng.), https://www.casemine.com/judgement/uk/6178eabab50db98e0c00c80f. The European Union looks at a member state toward which the defendant directed commercial activity by performing his obligations, see Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Recast), 2012 O.J. (L 351) 1, 12-13.

directed their activities toward or targeted the forum.[1712] These and other jurisdictional tests require a balancing of factors, including the location of the parties, the place of contractual performance, the nature of the dispute, the physical location of servers, and the accessibility of the digital service.[1713] In the case of smart contracts, the prevailing legal doctrine holds that the current connecting factors are sufficient.[1714] Theoretically, it would mean that traditional principles, such as the *lex loci solutionis* —that is, the law of the place where performance occurs,— should apply to smart contracts.

However, scholars note that applying these criteria to blockchain transactions is challenging.[1715] In a fully decentralized environment —where validator nodes are distributed across the globe— there is no clear basis for determining the appropriate forum or applicable law. Validator nodes are difficult to locate geographically, and participants may join or leave the network from any location at any time without restriction. This global dispersion generates significant uncertainty in identifying a place of performance of a contractual obligation or a nexus to any jurisdiction. The network comprises a dynamic and constantly shifting set of actors, rendering it nearly impossible to identify a single, stable jurisdiction.

In practical terms, the "right" jurisdiction is both everywhere and nowhere at once. Furthermore, applying the law of the closest connection to smart contracts proves difficult when the parties are unidentified or their residence is unknown, and when the subject matter of the transaction lacks a fixed geographical location.[1716] The automated execution of smart contracts —particularly within decentralized autonomous organizations (DAOs)[1717]— adds another layer of complexity to the determination of jurisdiction.

In certain cases, it may be possible to identify real-world connections. For example, when the identity of an application developer is publicly known, a litigant might rely on the developer's habitual residence or domicile to determine the jurisdiction most closely connected to the assets concerned. Yet, because blockchain participation is predominantly pseudonymous, the identities of actors are rarely ascertainable. This pseudonymity complicates the identification of the jurisdiction with the closest connection, the determination of the competent court, and the enforcement of legal rules.

One approach is to allow parties to specify the governing law and forum for potential disputes.[1718] This might be specified

1712 Yueh-Ping (Alex) Yang, *When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?*, 6 Stan. J. Blockchain L. & Pol'y 137, 140 (2023), https://stanford-jblp.pubpub.org/pub/jurisdiction-rules-blockchain/release/1.

1713 *See* Marketa Trimble, *Targeting Factors and Conflicts of Laws on the Internet*, 40 Rev. Litig. 1, 18, 20-43 (2020), http://dx.doi.org/10.2139/ssrn.3692247. Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 351-61 (2013), https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?params=/context/mlr/article/3605/&path_info=73_1_313_personal.pdf and Regulation 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), 2008 O.J. (L 177) 6, 18 ("In relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall be had to the law of the country in which performance takes place."), for factors that determine which law should apply and jurisdictional questions for claims arising from internet activities.

1714 *See generally* Amy Held, *Crypto Assets and Decentralised Ledgers: Does Situs Actually Matter?*, *in* Blockchain and Private International Law 209-58 (Andrea Bonomi, Matthias Lehmann & Shaheeza Lalani eds., 2023), https://brill.com/edcollchap-oa/book/9789004514850/BP000017.xml?language=en&srsltid=AfmBOoriYI-eMvqRlpu4SrVzsD4ab-cTzZTv-qIxidBDfjX98I-Q6RZ1; Matthias Haentjens & Matthias Lehmann, *The Law Governing Secured Transactions in Digital Assets*, *in* Blockchain and Private International Law 456-78 (Andrea Bonomi, Matthias Lehmann & Shaheeza Lalani eds., 2023), http://dx.doi.org/10.2139/ssrn.4353371.

1715 *See, e.g.*, Mehdi El Harrak, *Do Smart Contracts Need New Conflict-of-Laws Rules?*, *in* Blockchain and Private International Law, 489, (Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani eds., 2023) https://doi.org/10.1163/9789004514850_019, ("[s]ince [a smart contract] is immersed in the digital world, the place of performance is not *a priori* obvious").

1716 Anne-Grace Kleczewski, *The Good, the Bad and the Ugly: The Private International Law, the Crypto Transactions and the Pseudonyms*, *in* Blockchain and Private International Law 143-44, 151 (Andrea Bonomi, Matthias Lehmann & Shaheeza Lalani eds., 2023) (arguing that pseudonymity creates major challenges for the current private international law regime on many levels, especially for "the possibility of effectively enforcing any legal provisions").

1717 *See generally* Florence Guillaume, *Decentralized Autonomous Organizations (DAOs) Before State Courts: How Can Private International Law Keep Up with Global Digital Entities*, *in* Decentralized Autonomous Organisation (DAO) Regulation 135 (Madalena Perestrelo de Oliveira & António Garcia Rolo eds., 2024).

1718 Florence Guillaume, *Choice of Court Agreements in Disputes Involving Decentralized Autonomous Organizations (DAOs)*, *in* Foundations of Decentralized Organizations: Blockchain and the Future of Corporate Law (Kevin Werbach, Eva Micheler & Bianca Kremer eds.) (2026).

within the coding comments of smart contracts, DAOs, and NFTs or, alternatively, in the terms of service, constitutional documents, or similar provisions. For instance, if the law and forum are embedded in the software's source code, this would make them binding on anyone connecting to the network. In practice, however, blockchains and blockchain-based applications rarely contain such clauses. Such provisions are found only in enterprise or other private permissioned blockchains, such as the Corda blockchain, developed by a consortium of banks.[1719]

Another potential solution is to try to identify a perspective on smart contracts that could make them compatible with the current framework for determining the governing law and jurisdiction. Smart contracts that have a real-world outlet could be subject to the law of the jurisdiction where they produce their effects. As Mehdi El Harrak notes, "if a smart contract is used to perform the transfer of traditional or cryptocurrencies to a bank registered in a given country or for a delivery of goods to be performed in a given country, then this country will be the place of performance."[1720] For transactions that exist exclusively on the blockchain, however, the place of performance could potentially be determined by either the location of the cryptocurrency after it has been transferred from one account to another or by the location of one of the parties to the transaction.[1721] However, even under such approaches, the issue of connection to the forum remains. Courts will still need to assess whether the transaction or its effects create a meaningful nexus that justifies the forum's interest in adjudicating the controversy and applying its law.

This uncertainty creates substantial compliance challenges for protocols that operate simultaneously across multiple jurisdictions. Different legal systems may impose inconsistent or even contradictory regulatory requirements —for instance, a blockchain service might be classified as a commodity trading platform in one jurisdiction while being regulated as a payment services provider in another.[1722]

6.6.2. Examples from U.S. Case Law

The following paragraphs provide examples from U.S. case law. Among major jurisdictions, the United States generally adopts the most expansive view of its own jurisdiction and the extraterritorial application of its laws. In the context of blockchain, U.S. courts have asserted jurisdiction over blockchain-related activities when there have been sufficient minimum contacts within the United States as a whole, notwithstanding the general presumption against extraterritorial jurisdiction.[1723]

In an early ruling involving the Tezos blockchain, a U.S. court found jurisdiction, taking into consideration several connecting factors: U.S. investors had participated in the token sale through an interactive website hosted on U.S. servers and operated by a Tezos founder, in response to marketing directed primarily at U.S. residents, and Tezos network nodes were "clustered more densely in the United States than in any other country."[1724] Other courts have rejected reliance on such a "node density" theory, finding either that the location of the first node to validate the transaction should control or that the

1719 André Carneiro, *What Is Corda and How It Works*, BLOCKCHAINLAB (Oct. 21, 2022), https://blockchainlab.network/en/blog-blockchainlab/what-is-corda-and-how-it-works.

1720 El Harrak, see *supra* note 1715, at 490.

1721 *Id.* (referencing ADVICE TO GOVERNMENT, *supra* note 1590, at 193-94).

1722 Ben Charoenwong et al., *Blockchain Compliance: A Framework for Evaluating Regulatory Approaches* 14 (INSEAD, Working Paper No. 2025/46/FIN, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5368708.

1723 *See, e.g.*, William S. Dodge, *The New Presumption Against Extraterritoriality*, 133 HARV. L. REV. 1582 (2020), https://harvardlawreview.org/print/vol-133/the-new-presumption-against-extraterritoriality/.

1724 Order at 14-15, In re Tezos Sec. Litig., No. 3:17-cv-06779 (N.D. Cal. Aug 7, 2018), ECF No. 148; *See also* David Felsenthal, Steven Gatti & Jesse Overall, *Tokens and the Extraterritorial Reach of US Securities Laws*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Oct. 24, 2018), https://corpgov.law.harvard.edu/2018/10/24/tokens-and-the-extraterritorial-reach-of-us-securities-laws/.

location of nodes is not relevant at all.[1725] Nevertheless, the *Tezos* ruling suggests that, where plaintiffs have a legitimate grievance and cognizable harm, American courts may be inclined to find jurisdiction to hear the dispute where there is greater connection to the United States than other countries. Taken together, these elements suggest that corporate and transactional structuring may, in some cases, mitigate the likelihood that American courts will find jurisdiction by clustering nodes outside the United States.[1726] However, a similar expansive approach to jurisdiction can be observed in *Williams v. Binance* in 2024.

FIGURE 52.

***Williams v Binance* (2024)**

In *Williams*, plaintiffs filed a class action lawsuit in a federal district court against the Binance exchange. The district court granted the defendant's motion to dismiss the action, and the plaintiffs appealed. On appeal, Binance claimed to have no home jurisdiction and no domicile, making it immune to lawsuits in the United States. The U.S. Court of Appeals for the Second Circuit rejected Binance's arguments and protestations of "operat[ing] in a decentralized manner."[1727] It reasoned that, even if the company and its exchange lacked a physical location in the U.S., the transactions disputed by plaintiffs "cannot be 'nowhere.'"[1728] The appellate court found that the case may proceed on two independent grounds: first, that the disputed transactions were plausibly completed on servers located in the U.S.; and second, that Binance's Terms of Use rendered plaintiffs' purchase orders irrevocable once submitted, which plaintiffs alleged occurred from their homes in the United States. The court cautioned, however, that server location alone may not always be a sufficient basis for establishing that transactions are domestic.[1729]

Though the Second Circuit in *Williams v. Binance* articulated an interest in extending jurisdiction over blockchain activities occurring online, there remains a considerable degree of uncertainty about whether American courts will find jurisdiction in any given blockchain case.

While *Williams v. Binance* reflects judicial willingness to assert jurisdiction over blockchain activities with U.S. connections, this expansive approach must be reconciled with the traditional presumption against extraterritorial application of U.S. law to purely foreign conduct.[1730]

1725 Jake Chervinsky & Daniel Barabander, *A Practical Guide to Geofencing*, Variant Blog (Sept. 30, 2024), https://variant.fund/articles/practical-guide-to-geofencing/ (mentioning cases like *Barron v. Helbiz Inc.*, 2023 WL 5672640, at 6 (S.D.N.Y. Sept. 1, 2023) and *Williams v. Block.One,* 2022 WL 5294189, at 7 (S.D.N.Y. Aug. 15, 2022)).

1726 *See generally* Alina Veneziano, *Extraterritoriality and the Regulatory Power of the United States: Featured Issues of Sovereignty, Legitimacy, Accountability, and Democracy*, 6 Univ. Baltimore J. Int'l L. 189 (2019), https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=1071&context=ubjil.

1727 Williams v. Binance, 96 F.4th 129, 133 (2d Cir. 2024), *cert. denied sub nom.* Binance v. Anderson, 145 S. Ct. 1048 (2025).

1728 Williams, 96 F.4th at 138.

1729 *Id.* at 137-39 (but also noting "it may not always be appropriate" to determine whether a digital asset transaction is domestic or foreign "solely based on the location of the servers the exchange runs on").

1730 *See generally* Robert A. Schwinger, *When Blockchain Transactions Meet US Limits on Extraterritoriality*, Norton Rose Fulbright (Sept. 2019), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/when-blockchain-transactions-meet-us-limits-on-extraterritoriality-updated.pdf. In the context of securities, which is also applicable to blockchain transactions, the presumption against extraterritoriality is outlined in Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).

FIGURE 53.

***SEC v Schueler (aka Heart)* (2025)**

In the U.S. Securities and Exchange Commission's (SEC) case against Richard Heart (the founder of the Hex cryptocurrency and a U.S. citizen residing in Finland), the SEC sued Heart for securities fraud relating to Hex. The U.S. District Court for the Eastern District of New York dismissed the case in 2025 because Heart's alleged activities lacked sufficient ties to the United States.[1731] The court declined to exert jurisdiction over Heart's online promotions because, while he targeted a global audience, he did so without purposefully and actively directing his activities at U.S. residents.[1732] Heart's websites, though globally accessible, were not expressly targeting the United States any more than they were targeting other forums.[1733]

The judge contrasted Heart's case with the facts in *Williams v. Binance* *(See above Figure 52)*, noting that the SEC did not allege that Heart's servers were in the United States. The judge also noted that token purchasers in the United States never entered into a term of use agreement with Hex.[1734] The district court acknowledged the Second Circuit's concern that the blockchain transactions could not be "nowhere," but it refused to infer that the transactions occurred in the United States. It remains unclear where those transactions would be.

SEC v. Schueler serves as a good example of the uncertainty of what country has jurisdiction over blockchain transactions and which laws apply. And the courts' "remarkably inconsistent approach" to the location of blockchain transactions has not helped.[1735] Courts have continued to follow different approaches to establishing jurisdiction and applicable law.[1736]

Beyond questions of jurisdiction and applicable law, blockchain systems face a further challenge: compliance with data protection frameworks that were designed for centralized systems with clearly identifiable data controllers. The following section examines how blockchain's decentralized architecture and immutable ledgers create fundamental tensions with privacy regulations, particularly the European Union's General Data Protection Regulation.

1731 Memorandum & Order at 31, U.S. Sec. & Exch. Comm'n v. Schueler, No. 23-cv-5479 (CBA) (PK) (E.D.N.Y. Feb. 28, 2025), https://storage.courtlistener.com/recap/gov.uscourts.nyed.501047/gov.uscourts.nyed.501047.57.0.pdf.

1732 *Id.* at 15-19.

1733 *Id.* at 18-19, 22.

1734 *Id.* at 25-27.

1735 Chervinsky & Barabander, *supra* note 1725.

1736 For example, in *SEC v. PlexCorps*, a U.S. federal court exercised jurisdiction over a Canadian initial coin offering (ICO) due to its impact on U.S. investors, among other things. In that case, jurisdiction was established based on a combination of factors, including founders' trips, the creation of websites, the opening of bank accounts, and the impact of blockchain activity in the United States. Memorandum & Order at 14-41, U.S. Sec. & Exch. Comm'n v. PlexCorps, No. 1:17-cv-07007-CBA-RML (E.D.N.Y. Aug. 9, 2018), ECF No. 84. Relatedly, in *SEC v. Telegram Group Inc.*, the court conducted a preliminary merits analysis and determined that the planned resale of Telegram's cryptocurrency in the United States subjected the whole scheme to the U.S. securities laws. *See* Opinion & Order at 2, U.S. Sec. & Exch. Comm'n v. Telegram Grp. Inc., No. 1:19-cv-09439-PKC (S.D.N.Y. April 1, 2020), ECF No. 234.

6.7. COMPLIANCE WITH DATA PROTECTION FRAMEWORKS

Blockchain technology poses significant challenges for the protection of privacy *(See section 5.5)*.[1737] These difficulties become particularly salient in the context of compliance with data protection regulations. Blockchain technology's promise of decentralization and immutability creates fundamental tensions with data protection frameworks that assume centralized control and the ability to modify or delete information. Moreover, the legal concepts underpinning data protection frameworks, such as the EU's General Data Protection Regulation (GDPR), are often difficult to apply to the technical and organizational characteristics of blockchain systems.[1738] This section examines the challenges blockchain systems face in complying with data protection regulations, particularly the GDPR.

The GDPR is grounded in the principle that "natural persons should have control over their own personal data," thereby promoting the right to informational self-determination.[1739] In theory, the decentralized architecture of blockchain systems may appear to align with this principle, as no central authority unilaterally controls users' credentials or transactions.[1740] However, this form of technical decentralization does not, in itself, ensure compliance with data protection frameworks, nor does it guarantee that users can effectively exercise their legal rights.

The GDPR is designed to regulate data-processing environments in which control over personal data is attributable to identifiable actors, typically referred to as data controllers and processors. It operates on the premise that, for each instance of personal data processing, there exists at least one data controller—a natural or legal person responsible for ensuring compliance with data protection law. The GDPR also assumes that data subject rights are practically enforceable, including the ability to modify or erase personal data where required by law.[1741] By contrast, blockchains are deliberately designed to be tamper-resistant and append-only, making data modification or deletion technically complex and, in many cases, impossible.[1742] This structural feature stands in tension with core GDPR rights, such as erasure and rectification, and with the regulatory assumption that responsibility for compliance can be clearly allocated, which is particularly challenging in decentralized blockchain networks.

6.7.1. The Presence of Protected Personal Data on Blockchain Networks

At first glance, one might assume that the pseudonymity of blockchain systems *(See section 2.6.1.)* results in a situation where no personal data is processed on-chain, thereby excluding compliance concerns under data protection frameworks such as the GDPR[1743] or the California Consumer Privacy Act (CCPA).[1744] This assumption, however, is incorrect.

1737 Inês Campos Ruas, Soumaya Ben Dhaou & Zoran Jordanoski, *Blockchain and the GDPR – The Shift Needed to Move Forward,* Joint Proc. of Ongoing Rsch., Pracs., Posters, Workshops, & Projects at EGOV-CeDEM-ePart 2023, at 2 (Aug. 3, 2023), https://ceur-ws.org/Vol-3449/paper14.pdf; Akm Bahalul Haque et al., *GDPR Compliant Blockchains-A Systematic Literature Review*, 9 IEEE Access, 50593-50606 (2021), https://doi.org/10.48550/arXiv.2104.00648.

1738 *See* Pablo Marcello Baquero, *Layers of Privacy in the Blockchain: From Technological Solutionism to Human-Centred Privacy-Compliance Technologies,* 19 Int'l J.L. Context 51, 54-56 (2023), https://doi.org/10.1017/S1744552322000465.

1739 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, http://data.europa.eu/eli/reg/2016/679/oj [hereinafter GDPR].

1740 Michèle Finck, Eur. Parliamentary Rsch. Serv., Blockchain and the General Data Protection Regulation 91 (2019).

1741 *Id.* at 7, 45, 74.

1742 Rahime Belen-Saglam, Enes Altuncu, Yang Lu & Shujun Li, *A Systematic Literature Review of the Tension Between the GDPR and Public Blockchain Systems*, 4 Blockchain: Rsch. & Applications, June 2023, at 1-2, 20, https://doi.org/10.1016/j.bcra.2023.100129 (identifying the following data privacy issues of blockchain technology: "(i) difficulties in exercising data subjects' rights such as the 'right to be forgotten' (RTBF) due to the immutable nature of public blockchains; (ii) difficulties in identifying roles and responsibilities in the public blockchain data processing ecosystem (particularly on the identification of data controllers and data processors); and (iii) ambiguities regarding the application of the relevant law(s) due to the distributed nature of blockchains").

1743 GDPR suggests that pseudonymization reduces the risks of identification from "personal data." *See* GDPR, art. 4(5).

1744 Cal. Civ. Code § 1798.140(aa) (West 2025) [hereinafter CCPA] (defining "pseudonymize" or "pseudonymization").

In practice, blockchain transactions frequently contain personal data within the meaning of data protection laws, which focus on *identifiability,* rather than direct identification. For instance, Article 4(1) of the GDPR defines personal data to include "any information relating to an identified or identifiable natural person ('data subject')." It further describes an "identifiable natural person" as an individual who can be directly or indirectly identified through criteria such as their name, identification number, location data, online identifiers, or any other factors that are specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.[1745]

Because blockchain pseudonyms do not create full anonymity, the legal assessment of whether the pseudonym and information associated with it constitute personal data focuses on whether linkage to a natural person is reasonably possible. Blockchain transactions generally comprise two components: transaction metadata and transaction content.[1746] Transaction metadata includes identifiers of the parties to the transaction (typically in the form of public keys) as well as other technical information necessary for validation and verification. Where such public keys can be linked to a natural person by means reasonably likely to be used —such as data correlation, behavioral analysis, or following a data breach— they qualify as personal data under the GDPR. Even where only hash values, timestamps, or similar technical markers are recorded on-chain, these typically constitute pseudonymous rather than anonymous data[1747] and may qualify as personal data where re-identification is possible using additional information.[1748] In some cases, certain blockchain nodes, validators, or mining operations may also log IP addresses, which are classified as personal data under EU data protection law.[1749]

Substantive transaction data may, in some cases, include personal data about parties to the transaction or other identifiable persons.[1750] They may also reveal the amount of cryptocurrency transferred, make references to documents, and include information about purchased items and the execution of smart-contract functions.

On-chain personal data is not limited to transaction metadata or transaction content. Other data structures recorded on a blockchain, such as smart contract state or storage variables, may also contain personal data.[1751] Smart contracts may process personal information as part of their input parameters or during execution,[1752] and more sophisticated contracts may directly store or reference personal data on-chain. In addition, blockchain-based identity systems frequently record personal attributes such as biographical details, credentials, or verifiable

1745 The CCPA uses the term "personal information" and defines it as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household . . . ." *Id.* § 1798.140(o)(1)–(2).

1746 European Data Protection Board, *Guidelines 02/2025 on Processing of personal data through blockchain technologies, v. 1.1*, 12 (Apr. 8, 2025), https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

1747 *Id.*

1748 Eugenia Politou et al., *Blockchain Mutability: Challenges and Proposed Solutions*, 9 IEEE Transactions Emerging Topics in Computing 1972, 1976-77 (2019) https://ieeexplore.ieee.org/document/8883080.

1749 *See* Winston Maxwell & John Salmon, Hogan Lovells, A Guide to Blockchain and Data Protection 6, 8 (2018), https://digital-client-solutions.hoganlovells.com/_uploads/blockchain-insights/5649DataProtection-BlockchainPaperARTWORKSTAGE3Low-res-gumfy.pdf (discussing how public keys can be matched with IP addresses and citing a Court of Justice of the European Union case *Patrick Breyer v. Bundesrepublik Deutschland*, in which the court held that IP addresses are personal data if they are "likely reasonably to be used to identify" the individual if combined with other data); Michelle Poelman & Sarfraz Iqbal, *Investigating the Compliance of the GDPR: Processing Personal Data on a Blockchain*, 2021 IEEE 5th Int'l Conf. on Cryptography, Sec. & Priv. 38, 39 (2021), https://ieeexplore.ieee.org/document/9357590/.

1750 *See* Unal Tatar et al., *Law Versus Technology: Blockchain, GDPR, and Tough Tradeoffs*, 38 Comput. L. & Sec. Rev., 4 (Sept. 2020), https://doi.org/10.1016/j.clsr.2020.105454.

1751 EDPB, *Guidelines 02/2025 on processing of personal data through blockchain technologies, supra* note 1746.

1752 *See* Muhammad Al-Abdullah et al., *Designing Privacy-Friendly Data Repositories: A Framework for a Blockchain that Follows the GDPR*, 22 Digital Policy, Regulation and Governance 389, 394-95 (2020), https://doi.org/10.1108/DPRG-04-2020-0050; Haque et al., *supra* note 1737, at 50597.

claims, thereby raising further compliance concerns.[1753] Even where privacy-enhancing techniques such as zero-knowledge proofs (ZKPs) are used, regulatory challenges remain, not because underlying personal data is disclosed as such, but because immutable on-chain commitments, metadata linkability, or future cryptographic compromise could undermine long-term privacy guarantees**.**

In addition to on-chain processing, personal data may be stored wholly or partially off-chain, with only a reference, pointer, or cryptographic commitment included in the transaction content. Further personal data may be generated or processed when users interact with a blockchain through decentralized applications (dApps), wallets, or third-party intermediaries, including infrastructure and service providers. This may include, for example, IP addresses or device identifiers. Although such data is not generally stored directly on the blockchain, it nonetheless remains subject to applicable data protection frameworks.

In practice, although hashed or encrypted data provide a degree of protection,[1754] data subjects can often be re-identified through the combination of on-chain and off-chain information *(See above, Section 5.5.)*.[1755] For example, while a wallet address alone does not directly identify an individual, it may be linked to a natural person through off-chain data (such as KYC information held by an exchange or wallet provider), behavioral analysis (including recurring transactions, timestamps, or interactions with identifiable services), or network-layer data (such as logged IP addresses). In certain configurations, even hash values may indirectly reveal personal data,[1756] for instance where hashes are linked or reused in a manner that enables attribution to a specific individual.[1757] Similarly, while encryption restricts access to parties holding the relevant decryption keys, key compromise or future decryption advances cannot be entirely excluded, particularly given the long-term persistence of blockchain records.[1758]

6.7.2. Who Is the "Data Controller" on Blockchain Systems?

Data protection frameworks, such as the GDPR, presuppose that responsibility for personal data processing can be allocated to one or more identifiable actors, referred to as "data controllers."[1759] Under the GDPR, a controller is the entity that, alone or jointly with others, determines the purposes and means of processing personal data, while a processor acts on behalf of the controller.[1760] However, the decentralized governance model used by blockchain

1753 *See* Galia Kondova & Jörn Erbguth, *Self-Sovereign Identity on Public Blockchains and the GDPR,* Proc. on the 35th Ann. Symp. on Applied Computing 342 (2020), https://ssrn.com/abstract=3515213; *Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, Commission Nationale de l'informatique et des Libertés [French National Commission on Informatics and Liberty] (Oct. 29, 2018), https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data; E.U. Agency for Cybersecurity, Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust 7, 10, 39 (2022), https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Digital%20Identity%20-%20Leveraging%20the%20SSI%20Concept%20to%20Build%20Trust.pdf. *See also* Alexandra Giannopoulou, *Data Protection Compliance Challenges for Self-Sovereign Identity*, *in* Blockchain and Applications 94-95 (Javier Prieto et al., eds., 2020), http://dx.doi.org/10.2139/ssrn.3671523.

1754 Politou et al., supra note 1748, at 1978.

1755 *See generally* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 Geo. L. Tech. Rev. 202 (2017) (on de-anonymization online using a combination of data from different sources), https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Lubarsky-1-GEO.-L.-TECH.-REV.-202.pdf.

1756 *See* Greg McMullen, Primavera De Filippi & Constance Choi, Coal. of Automated Legal Applications, Blockchain Identity Services: Technical Benchmark of Existing Blockchain-Based Identity Systems 14, 16 (2019).

1757 *See* Kondova & Erbguth, *supra* note 1753, at 342, 344, 345.

1758 *See* Baquero, *supra* note 1738, at 54. *See also* Marco Tullio Giordano, *Blockchain and the GDPR: New Challenges for Privacy and Security*, *in* Blockchain, Law and Governance 281 (Benedetta Cappiello & Gherardo Carullo eds., 2021), https://www.springerprofessional.de/blockchain-law-and-governance/18508826.

1759 Ammar Zafar, *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways*, 11 J. Cybersecurity, no. 1, 2025, tyaf002, https://academic-oup-com.stanford.idm.oclc.org/cybersecurity/article/11/1/tyaf002/8024082.

1760 Controllers are described under Article 4(7) of the GDPR as the entities "which, alone or jointly with others, determine the purposes and means of the processing of personal data." Data processors are also defined under Article 4(8) as the entities that process personal data on the data controller's behalf. *See also*: EDPB guidelines on the concepts of controller and processor in the GDPR, V2.0, adopted on 7 July 2021, https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

systems results in a wide range of actors and roles involved in the processing of personal data.[1761] As a result, allocating responsibility for determining the purposes and means of processing is often complex and highly context-dependent, particularly in public and permissionless blockchain environments.[1762]

In public blockchains, the allocation of roles varies depending on the consensus mechanism and the specific blockchain application.[1763] According to the EDPB, because blockchain systems differ widely in structure and design, a case-by-case, factual assessment is required to determine which actors bear which obligations under the GDPR.[1764] Relevant factors include the nature of the service provided, the blockchain's governance mechanism, its technical and organizational configuration, and the relationships between participants. Accordingly, the responsibilities of participants cannot be determined in the abstract but depend on the governance system and other contextual elements of the blockchain in question.

For example, in most cases, nodes store or otherwise access a copy (full or partial) of the distributed ledger and participate in transaction validation.[1765] In these circumstances alone, nodes typically do not determine the purposes or essential means of processing. However, in certain circumstances, nodes may exercise decisive influence over the purposes and essential means of processing —for example, when they participate individually or collectively in decisions concerning protocol modifications, governance rules, or blockchain forks. In such cases, nodes may qualify as controllers or joint controllers within the meaning of the GDPR. By contrast, nodes should not automatically be classified as processors. Under the GDPR, processors must process personal data on behalf of a controller and under its instructions. Where nodes operate autonomously and do not act on behalf of, or under the direction of, any identifiable controller, they cannot be considered processors for the processing activities concerned.

Participants in a blockchain network may, in some circumstances, simultaneously qualify as data controllers —where they exercise control over the purposes and means of processing personal data linked to their wallet addresses— and as data subjects, insofar as the processing relates to information about their own identity or activities.[1766] This coexistence of roles does not create a legal contradiction, but it does add significant practical and interpretive complexity to the application of data protection law.[1767]

In permissioned or private blockchains, the allocation of responsibilities is generally more straightforward, though not automatically compliant with the GDPR. Participation requires authorisation from a designated authority, which may consist of a single organisation or a consortium of entities with aligned interests. Entities that administer access rights to the network —by granting, revoking, or managing participation— are more likely to determine the purposes and essential means of processing and therefore typically qualify as data controllers, or, depending on the

1761 Ruas, Dhaou & Jordanoski, *supra* note 1737, at 2-3; Haque et al., *supra* note 1737, at 50593; Mateusz Godyn et al., *Analysis of Solutions for a Blockchain Compliance with GDPR*, 12 Sci. Reps., 2022, at 2, https://pmc.ncbi.nlm.nih.gov/articles/PMC9440070/pdf/41598_2022_Article_19341.pdf; Giordano, *supra* note 1758, at 279.

1762 Politou et al., *supra* note 1748 at 1976.

1763 Haque et al., *supra* note 1737, at 50597.

1764 European Data Protection Board, *Guidelines 02/2025 on Processing of Personal Data Through Blockchain Technologies*, Version 1.1 (Apr. 8, 2025), https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

1765 *See* Reza Soltani et al., *Distributed Ledger Technologies and Their Applications: A Review*, 12 Applied Scis., 3-6 (2022), https://doi.org/10.3390/app12157898.

1766 Giordano, *supra* note 1758, at 277 ("in the DLT environment, a node of the blockchain could be regarded as a controller or a joint controller for some of the data it processes, or as a processor in relation to other data").

1767 *See* Poelman & Iqbal, *supra* note 1749, at 40.

circumstances, as processors acting on behalf of a clearly identifiable controller.[1768]

6.7.3. Can Data Subjects' Rights Effectively Be Guaranteed on Blockchain Systems?

Certain features of blockchain technology can support some of the GDPR's underlying principles, particularly those concerning data integrity and security.[1769] The cryptographic mechanisms that secure blockchain transactions can help ensure that personal data are not altered or tampered with once recorded. Similarly, the transparency and auditability of blockchain records may facilitate accountability and traceability of data processing. Yet, this transparency should not be conflated with the GDPR's right of access,[1770] as the visibility of transaction data does not necessarily enable data subjects to identify, understand, or control how their personal data are processed.

As with artificial intelligence systems, identifying an appropriate legal basis for processing personal data on blockchain networks can be challenging, particularly where consent is relied upon.[1771] In particular, obtaining and managing consent from data subjects presents significant difficulties.[1772] Traditional mechanisms for obtaining consent, such as opt-in checkboxes, are ill-suited to decentralized blockchain environments.[1773] Moreover, even when consent is initially obtained, the immutable nature of blockchain complicates the practical implementation of consent withdrawal, since records already written to the ledger cannot be erased or retroactively altered; withdrawal can typically only apply to future processing.[1774] Other legal bases under Article 6 GDPR, such as contractual necessity, legitimate interests, or legal obligation, may apply depending on the specific use case, but they do not resolve the structural tension created by immutability and decentralized governance.

Moreover, several principles protected under the GDPR cannot be effectively upheld in many blockchain systems.[1775] Most blockchains depend on extensive data replication, as each validating node maintains a complete or partial copy of the ledger.[1776] This replication, combined with the ledger's append-only and immutable architecture, produces an ever-expanding database that retains information indefinitely.[1777] In some cases, this design may lead to the processing or storage of more personal data than is strictly necessary for operational purposes, thereby conflicting with the principles of data minimization and storage limitation enshrined in Article 5 of the GDPR.[1778] While off-chain storage can mitigate the amount of data recorded on-chain, it introduces additional

1768 Giordano, *supra* note 1758, at 277 ("Perhaps, only a private blockchain, managed by a central body entrusted with the power to grant and revoke permissions, as well as to rewrite the content of transactions included in closed and certified blocks in the chain, could be virtually compliant with the GDPR.").

1769 GDPR, art. 5(1)(f). *See generally* Haque et al., *supra* note 1737.

1770 GDPR protects data subjects' right to obtain information regarding their personal data, including information on the purpose of processing, categories of personal data that are processed, types of recipients of the personal data, as well as its retention period. GDPR, art. 15(1); Poelman & Iqbal, *supra* note 1749, at 41.

1771 *See generally* Florence G'sell, *Statutory Obsolescence in the Age of Innovation: A Few Thoughts About GDPR*, Network L. Rev. (2025), https://www.networklawreview.org/gsell-statutory-obsolescence/ (discussing the interaction between AI and GDPR).

1772 GDPR, art. 7(1) ("Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of [their] personal data.").

1773 Finck, Eur. Parliamentary Rsch. Serv., *supra* note 1740, at 61-62 (stating that consent to the processing of data on the blockchain is challenging because it is not always "a clear affirmative act" and is not easily withdrawn).

1774 Article 7(3) of the GDPR grants data subjects the right to withdraw their consent for the processing of their personal data at any time. Article 7(3) further stipulates that the methods for withdrawing consent should be as easy to use as the process for giving consent.

1775 *See generally* Finck, Eur. Parliamentary Rsch. Serv., *supra* note 1740.

1776 Ruas, Dhaou & Jordanoski, *supra* note 1737, at 6.

1777 Baquero, *supra* note 1738, at 55-56; Poelman & Iqbal, *supra* note 1749, at 40-41; Giordano, *supra* note 1758, at 282.

1778 The principle of data minimization requires data controllers to restrict the collection and processing of personal data to what is strictly necessary for the intended purpose, while the principle of storage limitation mandates that personal data be retained only for as long as necessary to fulfil that purpose. GDPR, arts. 5(1)(c), 5(1)(e); Godyn et al., *supra* note 1761, at 1-11.

risks—most notably security vulnerabilities and potential re-centralization—by creating additional points of failure.[1779]

Additionally, the append-only and immutable design of blockchains directly conflicts with Article 17 of the GDPR, which establishes the right to erasure.[1780] Like the right to erasure,[1781] the right to rectification[1782] can hardly be implemented in the blockchain context, since alteration of data after its on-chain inclusion appears impossible.[1783] Other GDPR rights also raise implementation challenges. The right to object (Art. 21) and the right to restrict processing (Art. 18) are difficult to operationalize in decentralized networks without a clear controller, while the right to data portability (Art. 20), although potentially supported by blockchain's interoperability features, does not mitigate issues relating to immutability or excessive data replication.

Some scholars have proposed that encrypting personal data and subsequently deleting the encryption key could serve as a functional equivalent to erasure.[1784] However, rendering personal data inaccessible by deleting its encryption key does not necessarily fulfill the erasure requirement under Article 17 GDPR. Moreover, relying on a solution such as key deletion reintroduces a point of control and may undermine the decentralized trust model that blockchain systems seek to promote.[1785] Other solutions under consideration include storing only cryptographic hashes or references on-chain while maintaining erasable personal data off-chain,[1786] using encryption with the ability to destroy decryption keys (rendering encrypted on-chain data inaccessible),[1787] or employing zero-knowledge proofs that verify attributes without revealing underlying personal data.[1788] However, regulatory guidance on acceptable approaches remains limited.

1779 This may include only storing hash data, for example a hash link that provides on-chain access to the off-chain data. Baquero, *supra* note 1738, at 58 ("Perhaps the most-discussed technology in that category is that of storing data off-chain and simply leaving on-chain a hash link through which the information contained offline can be accessed.").

1780 Article 17 GDPR requires data controllers to erase the data subjects' personal data under various circumstances, including when the data subject withdraws their consent, and there is no other legal ground justifying the processing of the data. GDPR, art. 17 ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . . "). The California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (VCDPA) also provide for the right to request businesses to delete their personal information. Va. Code Ann. § 59.1-577 (West 2025); Cal. Civ. Code § 1798.105(a) (West 2025).

1781 The right to rectification as enshrined under Article 16 of the GDPR grants data subjects the right to request the rectification of inaccuracies in their personal data, without undue delay. This includes the right to complete any incomplete personal data with supplementary information. Anas Baig & Omer Imran Malik, *CCPA vs GDPR*, Securiti (Aug. 12, 2023), https://securiti.ai/ccpa-vs-gdpr/; Poelman & Iqbal, *supra* note 1749, at 41; Asim Jusić, *Privacy Between Regulation and Technology: GDPR and the Blockchain*, 1 IUS L.J. 47, 54 (2022), https://iuslawjournal.ius.edu.ba/index.php/iuslawjournal/article/view/20. In the United States, for example, the right to correct inaccuracies is addressed in the CCPA, which grants consumers the right to request correction of their personal information, and the federal regulations enacted under the Health Insurance Portability and Accountability Act, also known as HIPAA, which enables individuals to rectify inaccuracies in their health records. *See* Cal. Civ. Code § 1798.106 (West 2025); 45 C.F.R. § 164.526(a)(1).

1782 GDPR, art. 16.

1783 *See* Belen-Saglam et al., *supra* note 1742, at 2, 10, 12; Godyn et al., *supra* note 1761, at 2; Shrisha Sapkota, *The Right to Be Forgotten and the Immutability of Blockchain Technology*, Good L. Software, https://goodlawsoftware.co.uk/law/the-right-to-be-forgotten-and-the-immutability-of-blockchain-technology/ (last visited Jan. 15, 2026).

1784 *See, e.g.*, Zafar, *supra* note 1759, at 9; Shivani Jamwal et al., *A Survey on Ethereum Pseudonymity: Techniques, Challenges, and Future Directions*, 232 J. Network & Comput. Applications, 2024, at 18, https://eprints.gla.ac.uk/334723/1/334723.pdf; Belen-Saglam et al., *supra* note 1742, at 12. *See generally* Nick Scope et al., *Purging Data from Backups by Encryption*, Nat'l Sci. Found. (2021), https://par.nsf.gov/servlets/purl/10310753. *But see* Agencia Española de Protección de Datos [Spanish Data Protection Agency], 10 Misunderstandings Related to Anonymisation 3 (2021) (stating that deleting encryption keys does not render data anonymous because "[o]ne cannot assume that encrypted data cannot be decrypted because the decryption key is said to be 'erased' or 'unknown'").

1785 Enza Cirone, *Building a Techno-Legal Framework for Blockchain Technology and Data Protection Under EU Law* (2024) (Ph.D. dissertation, University of Florence) (on file with the University of Florence repository).

1786 *Personal Data Handling*, WORLD ECON F. BLOCKCHAIN DEPLOYMENT TOOLKIT, https://widgets.weforum.org/blockchain-toolkit/personal-data-handling/index.html (last visited Jan. 15, 2026); Erwin Volodер & Eugenio Reggianini, *European Data Protection Board Puts Blockchain at a GDPR Crossroads*, OMFIF (June 18, 2025), https://www.omfif.org/2025/06/european-data-protection-board-puts-blockchain-at-a-gdpr-crossroads/.

1787 Zafar, see *supra,* note 1759 ; see *also* Commission Nationale de l'Informatique et des Libertés (CNIL), *Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data* (2018), https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

1788 EU Blockchain Observatory & Forum, *Blockchain and the GDPR* (2018), https://blockchain-observatory.ec.europa.eu/document/download/b3a919ed-0045-46f8-89de-f23ca140e037_en?filename=20181016_report_gdpr.pdf

Finally, the cross-border nature of blockchain networks complicates compliance with data protection rules governing international transfers of personal data.[1789] Because blockchain nodes are distributed across multiple jurisdictions, it is often unclear which legal regime applies to the processing activity. Under Article 46(1) of the GDPR, data controllers and processors are prohibited from transferring personal data to third countries that do not provide adequate safeguards for its protection. Furthermore, several jurisdictions have enacted or are working on implementing data localization requirements that restrict or prohibit the storage of personal data abroad.[1790] These overlapping obligations create significant uncertainty for blockchain operators seeking to ensure compliance across decentralized networks.

Overall, the most effective strategy for mitigating compliance challenges under data protection law is to minimize the processing and storage of personal data on-chain, while retaining most personal data off-chain, for example in custodial databases or secure messaging systems. Encryption and advanced privacy-enhancing technologies —such as zero-knowledge proofs and secure multiparty computation— can further reduce the amount of personal data recorded on-chain. Nevertheless, these techniques have inherent limitations: they introduce significant technical complexity, entail substantial computational costs, and do not eliminate the risk of re-identification *(See section 5.5.)*. Moreover, off-chain storage architectures, in which personal data remains outside the blockchain, and only cryptographic hashes, commitments, or references are recorded on-chain, may alleviate certain GDPR compliance burdens. However, this approach shifts rather than resolves the underlying legal and technical challenges. In practice, it reintroduces elements of centralization and creates new vulnerabilities, including single points of failure and increased exposure to unauthorized access or data breaches.

These cumulative difficulties in achieving GDPR compliance help explain why the European Data Protection Board, in its 2025 draft Guidelines on the processing of personal data through blockchain technologies, emphasizes the importance of architectures that enable clear allocation of responsibilities and effective control over data processing. While the Guidelines do not formally mandate the use of permissioned blockchains, they highlight the compliance challenges associated with permissionless systems and the relative advantages of more controlled environments. More broadly, they require controllers to assess, on a case-by-case basis, whether the use of blockchain technology is necessary and appropriate in light of GDPR requirements. Where decentralized architectures are used, particular attention must be paid to governance arrangements that allow for the identification of responsible actors and the effective exercise of data subjects' rights.

1789 Giordano, *supra* note 1758, at 284-85.

1790 For example, China, South Africa, Vietnam, India, and Russia. *See* Alex LaCasse, *IAPP GPS 2024: Localization, Adequacy Define Current Data Transfer Landscape*, IAPP (Apr. 4, 2024), https://iapp.org/news/a/iapp-gps-diverging-data-localization-laws-complicate-future-of-crossborder-dataflows; *Russian Personal Data Localization Requirements*, Microsoft Ignite, https://learn.microsoft.com/en-us/compliance/regulatory/offering-russia-data-localization (last visited Jan. 15, 2026); *Data Localization and Global Privacy Laws: How to Manage the Regulatory Patchwork*, TrustArc, https://trustarc.com/resource/data-localization-global-privacy-laws/ (last visited Jan. 15, 2026).

KEY TAKEAWAYS

■ The debate on whether blockchain lies beyond the reach of law echoes earlier discussions on the regulation of cyberspace. Like the internet in its early days, blockchain challenges traditional legal frameworks. Through its decentralization, pseudonymity, and transnational architecture, blockchain gives rise to forms of governance embedded in code —summarized by the maxim **"code is law."** Building on this idea, some scholars describe the emergence of a distinct normative order, often referred to as *lex cryptographica*, in which rules are enforced through self-executing protocols. The related notion of blockchain's **alegality** suggests that these systems may operate outside, or at the margins of, established legal regimes, even though their technical architecture and evolution remain shaped by human design choices and external regulatory forces.

■ In practice, the **tension between the self-executing authority of blockchain code and the normative authority of law** has been illustrated in widely discussed cases. In *Mango Markets* and *Platypus,* courts confronted the question whether interacting with a protocol in ways its designers did not anticipate constitutes criminal misconduct and reached inconsistent answers through different doctrinal frameworks. While the French courts in *Platypus* acquitted the defendants of all criminal charges, the U.S. court in Mango Markets vacated the commodities convictions on procedural grounds while rejecting the wire fraud conviction on the merits. More recent developments, such as the *Peraire-Bueno* prosecution, extend this inquiry to validator conduct, raising the question of whether strategically manipulating transaction ordering within blockchain infrastructure can constitute fraud, though a mistrial has left these issues unresolved. Taken together, these cases do not yield a coherent solution: they reflect a persistent inability of existing legal frameworks to draw stable boundaries between permissible strategic behavior and unlawful manipulation. Technical compliance with protocol rules does not displace legal standards; instead, it forces courts to adapt traditional doctrines —such as fraud and market manipulation— without yet providing clear or consistent guidance.

■ The question of whether **blockchain developers** can be held liable for software they create but do not operate remains legally unresolved. Some argue that core developers exercise discretionary power that could give rise to fiduciary duties toward users. Others contend that the decentralized architecture of blockchain systems prevents any single individual from exercising meaningful control, and imposing liability on developers risks chilling innovation and exposing open-source contributors to legal risk whenever third parties reuse their code. In the United States, courts have generally distinguished between the publication of code —which may qualify as protected expression under the First Amendment— and its operational deployment, which may constitute regulable conduct. The *Uniswap* decision rejected the imposition of liability on smart contract developers for third-party misuse of their code. In the United Kingdom, the *Tulip Trading* appellate decision left open the possibility that developers exercising significant authority over network maintenance may owe fiduciary-like duties. Beyond the developer/user distinction, caselaw also suggests that the line between the party who writes the code and the party who deploys and operates it may carry distinct legal implications.

■ Another example of how blockchain technologies challenge the boundary between computer code and law is the way DAOs disrupt existing legally recognized organizational forms. While the legal status of DAOs remains largely unsettled, U.S. courts have increasingly been willing to treat **unincorporated or "unwrapped" DAOs** as legal entities. In several cases, courts have analyzed them as unincorporated associations or general partnerships, thereby exposing at least some governance token holders to potential joint and several liability. These developments underscore that decentralization does not shield participants from legal accountability and may, in some contexts, expand the pool of potentially liable actors precisely because governance is distributed rather than eliminated.

■ The **legal status of smart contracts** remains deeply ambiguous, reflecting persistent conceptual divergence between their technical nature as self-executing code and their possible classification as legally binding agreements. Across jurisdictions, no stable doctrinal framework has yet emerged: Some approaches treat smart contracts as potentially enforceable agreements if they satisfy traditional requirements of contract formation. Others emphasize their character as purely technical instruments or adopt a functional, case-by-case analysis. This uncertainty is compounded by the diversity of forms that smart contracts may take, ranging from tools for automating performance to fully code-based arrangements lacking any natural-language expression. In the *Tornado Cash* litigation, the Fifth Circuit held that immutable smart contracts could not be treated as "property" under the relevant statutory framework because they operate autonomously and beyond the control of any party. This reasoning lends support, in a limited context, to the view that certain forms of code may occupy a zone of alegality. Yet the case simultaneously underscores the limits of that claim: Even where code itself escapes direct regulation, human actors involved in its design and deployment remain fully within the reach of the law.

■ Blockchain's pseudonymity and decentralized, borderless architecture disrupt traditional conflict-of-laws principles by undermining established connecting factors such as territory, domicile, and place of performance. While courts continue to rely on existing tests —such as purposeful availment or the closest connection— their application to blockchain transactions remains highly uncertain in environments where participants and infrastructure are globally dispersed. U.S. case law illustrates this indeterminacy: In the *Tezos* litigation, a court asserted jurisdiction by relying, among other factors, on the concentration of validating nodes in the United States. In Williams v. Binance, the Second Circuit allowed the case to proceed on the ground that the relevant transactions were executed on U.S.-based servers despite the platform's claims of decentralization. By contrast, in SEC v. Schueler, the court declined jurisdiction, emphasizing that the defendant's online activities, though globally accessible, were not purposefully directed at the United States and therefore lacked sufficient U.S. contacts to establish a territorial nexus. These divergent approaches underscore the difficulty of determining jurisdiction, forum, and applicable law for blockchain transactions.

■ Blockchain technology challenges **data protection frameworks**, such as the General Data Protection Regulation, by disrupting core assumptions about identifiable actors and controllable data. Despite their pseudonymity, blockchain systems frequently process personal data, while their decentralized governance makes it difficult to identify a responsible data controller. Moreover, key GDPR principles —such as consent, data minimization, and rights of erasure or rectification— presume the existence of modifiable data and enforceable control, both of which are in tension with blockchain's immutability and distributed architecture. While privacy-enhancing technologies and off-chain storage can mitigate certain compliance risks, they do not eliminate them and may reintroduce elements of centralization. Overall, the question of whether and how data protection law applies in decentralized environments remains unresolved.

■ Taken together, these challenges reveal a **structural misalignment** between decentralized architectures and legal frameworks built around identifiable actors, territorial connections, and centralized control. Across domains, existing doctrines are adapted but fail to produce stable or coherent solutions, resulting in persistent uncertainty in how law engages with blockchain systems. As blockchain applications expand beyond cryptocurrency into finance, supply chains, identity management, and governance, this misalignment becomes increasingly difficult to sustain, underscoring the need for more coherent and adapted legal approaches.

CHAPTER 7

Policy Strategies

CHAPTER 7 TABLE OF CONTENTS

CHAPTER 7. POLICY STRATEGIES 299
7.1. Observational Approach 304
7.1.1. Issuing Guidance 305
7.1.2. Sandboxing 307
7.2. Applying Existing Frameworks: The U.S. Experience 309
7.2.1. Guidance Followed by Enforcement: FinCEN and IRS 310
7.2.1.A. FinCEN: Money Transmission Framework 310
7.2.1.B. IRS: Crypto-assets as Property 312
7.2.2. Regulation by Enforcement: The SEC and CFTC Approach 313
7.2.2.A. The SEC: Crypto-assets as Securities 313
7.2.2.B. The CFTC: Crypto-assets as Commodities 318
7.2.3. Regulation by Prosecution: The DOJ Approach 319
7.2.4. The Trump Administration's Policy Shift 320
7.2.4.A. Critiques of "Regulation by Enforcement" 321
7.2.4.B. Reassessment of "Regulation by Enforcement" 322
1. New SEC Policy 322
2. New CFTC Policy 323
7.2.4.C. Ending "Regulation by Prosecution": the Blanche Memo 324
7.2.4.D. New Federal Statutes 324
1. The GENIUS Act 325
2. The CLARITY Act 325
7.3. Proactive Legislative Frameworks 326
7.3.1. Designing a Legal Framework for DAOs 327
7.3.1.A. The COALA Model Law for DAOs 328
1. Key Provisions 328
2. Influence and Challenges 330
7.3.1.B. U.S. State Legal Frameworks for DAOs 331
1. Vermont (2018) 331
2. Wyoming (2021) 332
3. Tennessee (2022) 333
4. Utah (2023) 334
5. New Hampshire (2024) 336
6. Conclusion 337
7.3.1.C. Malta 338
7.3.1.D. Marshall Islands 339
7.3.1.E. Conclusion 340
7.3.2. Solving Conflict of Laws 341
7.3.2.A. The Swiss Reform 341
7.3.2.B. The UNIDROIT Principles 343
1. Determining the Applicable Law 343
2. Content of The Principles 343
7.3.3. Frameworks for the Use of Technology 344
7.3.3.A. The Indirect Regulation of Smart Contracts: The EU Data Act 345
1. Scope of the Data Act 345
2. Regulatory Obligations Governing the Use of Smart Contracts 346
a. Substantive Obligations on Manufacturers and Data Holders 346
b. Technical Requirements for Smart Contracts Under Article 36 346
3. Challenges of Implementing the Data Act in the Blockchain Context 347
4. The Proposed Repeal of the Data Act's Smart Contract Provisions 348
7.3.3.B. Recognizing Decentralized Identities (eIDAS) 349
1. The European Union Digital Identity Wallet 350
a. The Provision of EU Digital Identity Wallets 350

CHAPTER 7 TABLE OF CONTENTS (CONT'D)

b. Acceptance obligations 350

c. Privacy-Preserving Features and Selective Disclosure 351

2. Trust Services and Electronic Ledgers 352

3. European Blockchain Services Infrastructure (EBSI) 354

4. Assessment and Implications for Decentralized Identities 355

7.3.4. Frameworks for the Regulation of Crypto-assets 356

7.3.4.A. Switzerland 356

1. Legal Categories 356

2. The DLT Act 358

3. Sandbox Regulations 359

4. Conclusion 360

7.3.4.B. In the EU: Markets in Crypto-Assets Regulation (MiCA) 360

1. Scope 362

a. Crypto-assets that Do Not Qualify as Financial Instruments 362

b. Exclusion of NFTs 363

c. Exclusion of Fully Decentralized Services 363

2. Requirements 365

a. Offering to the Public and Trading of Crypto-assets in the EU 365

b. Asset-References Tokens (ARTs) 365

c. Electronic Money Tokens (EMTs) 365

d. Crypto-assets Service Providers (CASPs) 366

e. Market Abuse Provisions 366

f. Marketing Communications 366

3. Implementation 366

4. Conclusion 367

7.3.4.C. Strict Oversight: South Korea 368

1. Regulation of ICOs, Cryptocurrencies, and Exchanges 369

2. The South Korean "crypto law" 369

3. Institutional Participation and Proposed Reforms (2025 roadmap) 370

4. Conclusion 371

7.4. Prohibitions and Restrictions 371

7.4.1. The Prohibition of Decentralized Cryptocurrencies: China 371

7.4.1.A. The Ban of Decentralized Cryptocurrencies 372

7.4.1.B. Blockchain Innovation Under Centralized State Control 373

7.4.2. Prohibition of Cryptocurrencies as Means of Payment: Russia 374

7.4.3. Blanket prohibitions of cryptocurrencies 376

KEY TAKEAWAYS 377

CHAPTER 7
Policy Strategies

The previous chapter highlighted the considerable legal uncertainty surrounding the status of blockchain systems and the transactions conducted on them. Recent litigation demonstrates that lawyers and courts adjudicating blockchain-related disputes often hesitate and struggle to resolve the unprecedented legal questions raised by these technologies. A central difficulty concerns the legal nature and effects of computer code, which most legal systems find challenging to conceptualize, particularly in the context of decentralized networks.

Regulators frequently invoke the maxim "same business, same risks, same rules,"[1791] arguing that blockchain activities should be subject to the same regulatory standards as comparable traditional activities. For example, blockchain-based financial activities are exposed to risks of fraud, market abuse, and illicit finance like those present in the traditional financial system. However, industry participants have resisted the extension of financial regulation into the digital-asset sphere.[1792] When the U.S. Treasury sought to extend anti-money-laundering obligations to disintermediated crypto platforms in 2020,[1793] industry actors argued that the proposal would impose disproportionate compliance burdens, compromise user privacy, and remain ineffective in preventing illicit activity.[1794] The proposal was ultimately withdrawn.[1795]

Overall, policymakers face difficult choices. Should they intervene early to clarify the legal regime applicable to blockchain activities —or even introduce technology-specific rules? Should they, instead, adopt a more cautious, wait-and-see approach, allowing the technology to mature without premature regulatory intervention? Or should they rely on courts and administrative authorities to adapt existing legal regimes and principles incrementally to the novel characteristics and risks posed by blockchain technologies?

Against this background, policymakers may adopt a functional-equivalence approach *(See section 1.3.2.A.)*. With this approach, rather than drafting entirely new legislation, policymakers identify parallels between technological functions and traditional legal categories

1791 *See* Rodrigo Coelho, Jonathan Fishman & Denise Garcia Ocampo. Fin. Stability Inst., Bank for Int'l Settlements, FSI Insights on Policy Implementation No. 31: Supervising Crypto-assets for Anti-Money Laundering 1 (2021), https://www.bis.org/fsi/publ/insights31.pdf.

1792 *See, e.g.*, Brief for Defi Educ. Fund as Amicus Curiae Supporting Appellant and Urging Reversal at 10, 22-30, *Harper v. Werfel*, 118 F.4th 100 (1st Cir. 2024) (No. 23-1565), https://www.defieducationfund.org/_files/ugd/e53159_492b137460ef4263aa43f3fcb946a1cd.pdf (arguing in the Fourth Amendment context that cryptocurrency transactions are not like traditional finance and that courts, when confronted with new technology, must refuse to unreasonably extend existing legal standards); Glob. Digit. Asset & Cryptocurrency Ass'n, Re: Response to Request for Consultation on FSB's Proposed Framework for the International Regulation of Crypto-Asset Activities 5-7 (Dec. 15, 2022), https://www.fsb.org/uploads/Global-Digital-Asset-and-Cryptocurrency-Association.pdf (a crypto industry group's response to the Swiss Financial Stability Board arguing that cryptocurrency is unlike other industries and requires distinct regulatory approaches); Peter Van Valkenburgh, Coin Ctr., *A New SEC Proposal Has Serious Change Hidden Within Its Complex Language*, Coin Ctr. (Apr. 14, 2022), https://www.coincenter.org/a-new-sec-proposal-has-a-serious-change-hidden-within-its-complex-language (a think tank arguing that applying a rulebook from the securities context to decentralized finance can chill the freedom of speech); Blockchain Ass'n, *Re: Written Input Regarding Investment Adviser Custody-Related Topics* 6 (2025), https://theblockchainassociation.org/wp-content/uploads/2025/06/BlockchainAssociation-RFI-Response-Re-Custody-Topics.pdf (another crypto industry group arguing that a concept of "custody" in the context of crypto-assets "may be different than for traditional securities").

1793 *See generally Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, 85 Fed. Reg. 83840 (Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022), https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/requirements-certain-transactions-involving.

1794 *See* Kai Wang, *Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act*, 4 U. Chi. Bus. L. Rev. 341, 395-96 (2025), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1058&context=ucblr (summarizing the criticism of the Notice of Proposed Rulemaking by FinCEN).

1795 *Id.* at 347.

and apply established principles and rules to novel contexts. If this approach appears inadequate for a technology's specific characteristics or unique challenges, policymakers may decide to pursue new legal frameworks. These new legal frameworks can adapt established legal principles to the distinctive features of emerging technologies, with the goal of ensuring an equivalent level of protection —a logic of regulatory equivalence *(See section 1.3.2.B.)*. Although more complex, this approach may prove indispensable to ensuring that fundamental principles —such as privacy, accountability, and transparency— can be effectively safeguarded in rapidly evolving technological environments.

Existing scholarship has proposed various typologies of regulatory approaches to blockchain technology. Michèle Finck, for instance, has identified strategies ranging from *wait-and-see* approaches to *informal interpretive guidance,* regulatory *sandboxes,* and targeted legislation focusing on *chokepoints,* such as exchanges, custodial wallet providers, or mining pools.[1796] Since Finck's 2018 study, a growing number of jurisdictions have enacted new laws specific to blockchains, and targeted legislation and bespoke regulatory frameworks have gained particular momentum. Building on this foundation but focusing on developments observable in regulatory practice, this chapter examines four contemporary approaches that have emerged across different jurisdictions.

Contemporary regulatory practices favor four principal strategies:

1. **Observational or Non-Interventionist Approach:** The observational approach is typically regarded as pro-innovation. It emphasizes allowing emerging technologies to develop with minimal regulatory constraints. It typically relies on non-binding guidelines, soft-law instruments, or regulatory sandboxes that enable controlled experimentation under supervisory oversight.
2. **Applying existing frameworks**: Rather than enacting new legislation, some jurisdictions —most prominently the United States— have extended pre-existing legal frameworks to blockchain activities through a combination of interpretive guidance, case-by-case enforcement, and criminal prosecution. Among these, reliance on enforcement actions as a substitute for rulemaking —commonly described as 'regulation by enforcement'— has proven the most consequential. This expression refers to a strategy in which regulatory standards emerge primarily through enforcement actions brought against specific entities under existing legal frameworks. Rather than promulgate detailed *ex ante* rules, regulators rely on the interpretative and precedential effects of *ex post* enforcement decisions to shape market behavior and progressively articulate their policy positions. In the United States agencies, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), have used enforcement as a central policy tool in the absence of comprehensive legislative reform. However, this strategy has recently been significantly recalibrated.
3. **Adoption of *new* legal frameworks:** Some governments have developed entirely new legal frameworks specifically tailored to emerging technologies, exemplified by the European Union's Markets in Crypto-Assets (MiCA) Regulation. In certain cases, these frameworks are designed not only to regulate risks but also to attract technological innovation —a phenomenon often described as regulatory competitiveness.

1796 Michèle Finck, *Blockchains: Regulating the Unknown*, 19 German L.J. 665, 666 (2018), https://germanlawjournal.com/wp-content/uploads/01-Vol_19_No_4_Finck.pdf.

4. **Bans / Prohibition**. Some jurisdictions have imposed partial or complete bans on specific aspects of blockchain technology, most often targeting cryptocurrency issuance, trading, or mining. The People's Republic of China represents the most prominent example, having progressively prohibited cryptocurrency-related activities while continuing to promote state-controlled digital infrastructure, such as the Digital Yuan (e-CNY).

These frameworks are not mutually exclusive; rather, they offer complementary lenses through which regulatory strategies can be understood. A given country may adopt different strategies for different aspects of blockchain technology. Taken together, they reflect distinct regulatory philosophies, varying in their tolerance for risk, their reliance on existing legal categories, and their willingness to adapt or transform legal frameworks in response to technological change. The remainder of this chapter examines each approach in detail, analyzing its implementation, effectiveness, and implications for blockchain governance.

The country case studies in this chapter illustrate the four principal regulatory strategies. Additional jurisdictions with significant blockchain developments—namely Japan, Singapore, Switzerland, and India—are examined in detail in Appendices 17 through 21. Numerous other jurisdictions fall outside the scope of this report, underscoring both the rapid evolution of the field and the growing fragmentation of the global regulatory landscape.

7.1. OBSERVATIONAL APPROACH

The observational approach, generally considered innovation-friendly, is characterized by minimal regulatory intervention while blockchain technology matures. This is not a reflection of hands-off inaction or a preference to let other countries lead the way. Instead, a motto for the approach might be summed up as, "Educate, do not regulate."[1797] Regulators collect facts, monitor industry developments, and refrain from developing formal regulations immediately to avoid engaging in premature, potentially misaligned intervention. It has been notably adopted in jurisdictions such as Switzerland and Singapore, as well as in other countries seeking to signal openness to blockchain innovation. More broadly, this approach reflects a strategic choice to defer binding intervention under conditions of technological uncertainty. In practice, many jurisdictions that initially adopted an observational posture have subsequently transitioned toward more interventionist regulatory frameworks as the technology has matured and its risks have become better understood.

The observational approach manifests primarily through two regulatory techniques: the issuance of non-binding *guidance* and the use of regulatory *sandboxes*. More broadly, this approach allows novel technologies, such as blockchain, to evolve before regulators adopt technology-specific rules or guidelines. The appeal of this strategy lies in the recognition that binding regulation adopted at an early stage may prove ill-suited to the task and require rapid amendment in response to unforeseen technological developments. Once greater clarity emerges regarding a technology's capabilities and risks, regulators may be better positioned to tailor regulatory responses to maximize benefits and mitigate harms, without unduly constraining innovation.

1797 *Id.* at 675.

For technologies still at an early stage of development, this approach may appear particularly attractive. It reflects a regulatory philosophy that views the role of government as one of nurturing innovation while building institutional knowledge. Policymakers recognize the economic potential of blockchain technology and seek to better understand its technical characteristics and use cases before committing to long-term legislative solutions. This does not mean that regulators are "hands-off" during the observation period or that consumer protection is entirely absent. Existing laws remain applicable, and regulators frequently issue guidance clarifying how those laws apply to new technological contexts. In some cases, authorities may also establish regulatory sandboxes, offering developers a controlled environment in which to test new products while regulators observe how existing legal frameworks operate in practice.

7.1.1. Issuing Guidance

Under an observational regulatory posture, regulators remain attentive but refrain from immediate legislative intervention. They maintain supervisory vigilance but delay legislating new rules. Instead, they may issue non-binding interpretative guidance after acquiring preliminary insights into the operation of the technology. This strategy enables technological experimentation while retaining regulatory flexibility. Non-binding regulatory guidance clarifies the scope and application of existing legal norms and the values they reflect without enacting new legislation. It clarifies how existing rules might apply to technological developments that were not in existence at the time the rules were enacted.

Securities regulation occupies a central position in the legal treatment of blockchain. In many jurisdictions, the question of whether a token or digital asset qualifies as a "security" triggers the full set of securities law rules. Accordingly, it is the area of law that requires the most immediate and systematic clarification. The challenge for securities regulators is to assess whether, and under what circumstances, particular digital assets or transactions qualify as securities under existing legal frameworks. Many Western countries have issued regulatory guidance to clarify in what circumstances domestic securities laws apply to crypto trading products, platforms, and issuers. For example, in Switzerland, the Swiss Financial Market Supervisory Authority (FINMA) issued guidance as early as 2018 on the classification of tokens *(See section 7.3.4.A.)*.[1798]

- **Canada**

Canadian authorities have, so far, expanded crypto regulation primarily through guidance. For instance, the Canadian Securities Administrators (CSA), in collaboration with the Investment Industry Regulatory Organization of Canada (IIROC), issued guidance in 2021 to crypto-asset trading platforms.[1799] The joint statement sought to clarify existing regulatory requirements.[1800] On July 6, 2023, the CSA expanded on its guidance with a document intended to clarify the regulatory landscape for new public crypto-asset investment funds.[1801] This predominantly guidance-based and observational approach is now beginning to evolve.

Canada's approach shifted in November 2025, as the federal government introduced Bill C-15, which includes the

1798 *See generally* Swiss Fin. Mkt. Supervisory Auth., *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings* (ICOs) (Feb 16, 2018), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=en&hash=83EE49D77DA54DD079F314D9EDCBDC3D.

1799 *See generally* Can. Sec. Adm'rs & Inv. Indus. Regul. Org. of Can., Joint Staff Notice 21-329: *Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements* (Mar 29, 2021), https://www.osc.ca/sites/default/files/2021-03/csa_20210329_21-329_compliance-regulatory-requirements.pdf.

1800 It noted that "the overall goal . . . is to ensure there is a balance between needing to be flexible in order to foster innovation in the Canadian capital markets and meeting our regulatory mandate of promoting investor protection and fair and efficient capital markets." *Id.* at 1.

1801 *See generally* Can. Sec. Adm'rs, Staff Notice 81-336: Guidance on Crypto Asset Investment Funds that Are Reporting Issuers (2023), *https://www.osc.ca/en/securities-law/instruments-rules-policies/8/81-336/csa-staff-notice-81-336-guidance-crypto-asset-investment-funds-are-reporting-issuers*.

proposed Stablecoin Act.[1802] This legislation would establish a federal framework specifically for fiat-backed stablecoins, requiring issuers to register with the Bank of Canada and maintain 1:1 reserves in high-quality liquid assets. It would also prohibit the offering of yield or interest.[1803] The bill is expected to receive royal assent in spring 2026, with implementation phased over time. This development would mark Canada's first federal statute addressing a specific category of blockchain-based assets, though broader crypto-assets would remain governed primarily by CSA guidance and existing financial-sector legislation.[1804]

- **Australia**

Australia has similarly relied on its securities regulator to develop best practices for digital assets. The Australian Securities and Investments Commission (ASIC), after a year-long consultation,[1805] published Information Sheet 225 in 2025 to clarify that entities handling digital assets meeting the definition of financial products must obtain financial services licenses under the *Corporations Act 2001*.[1806] This guidance-based, regulator-driven approach reflected ASIC's role in applying existing laws to crypto markets, even as industry stakeholders lobbied intensively for clearer and more tailored rules in the lead-up to the May 2025 federal election.

In the wake of those elections, Australia's approach has begun shifting toward a more proactive, legislative framework. On September 25, 2025, the Australian Treasury released the *Treasury Laws Amendment (Regulating Digital Asset, And Tokenised Custody, Platforms) Bill 2025*, followed on 26 November 2025 by the introduction to Parliament of the Corporations Amendment (Digital Assets Framework) Bill 2025, which implements the framework. This Bill proposes a comprehensive regulatory regime for digital-asset platforms.[1807] The Bill would impose a licensing requirement and banking-style capital standards on entities dealing in digital assets and tokenized custody services, signaling a move beyond interpretive guidance toward bespoke statutory obligations. As of early 2026, the Bill has been introduced but is not yet in force.[1808]

- **Singapore**

Singapore *(See Appendix 19)* initially adopted an observational approach —relying on existing legislation and issuing non-binding guidance— to better understand the nascent digital-asset sector. The Monetary Authority of Singapore (MAS) employed interpretative guidelines and policy statements to govern crypto-related activities. In 2022, MAS issued guidance instructing service providers to refrain from promoting cryptocurrency trading to the general public, citing the high risks associated with such investments.[1809] As of January 15, 2026, MAS's FinTech Regulatory Sandbox has not been the primary channel in practice for cryptocurrency payment providers; consistent with MAS's 2023 clarification that no crypto payment firms had qualified for the sandbox,

1802 Bill C-15, Budget 2025 Implementation Act, No. 1, 1st Sess, 45th Parl, 2025, div 45, cl 600 (first reading November 18, 2025) (Can), https://www.parl.ca/DocumentViewer/en/45-1/bill/C-15/first-reading.

1803 Mohammed Muraj, Marissa A. Daniels & Eli Monas, *Canada's Stablecoin Act: overview and implications,* Torys (Dec. 3, 2025), https://www.torys.com/our-latest-thinking/publications/2025/12/canadas-stablecoin-act.

1804 *Id.*; see *also* Joshua Santos, *Why does Ottawa want to regulate Canadian stablecoins?*, BNN Bloomberg (Jan. 5, 2026), https://www.bnnbloomberg.ca/business/2026/01/05/why-does-ottawa-want-to-regulate-canadian-stablecoin/#:~:text=%E2%80%9CI%20think%20the%20biggest%20prompt,issuers%20with%20Bill%20C%2D15.

1805 Press Release, Austl. Sec. & Invs. Comm'n, *ASIC Invites Feedback on Proposed Updates to Digital Asset Guidance* (Dec. 4, 2024), https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-266mr-asic-invites-feedback-on-proposed-updates-to-digital-asset-guidance/.

1806 Press Release, Austl. Sec. & Invs. Comm'n, *Updated ASIC guidance supports digital asset innovation and boosts investor protection* (Oct. 29, 2025), https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-250mr-updated-asic-guidance-supports-digital-asset-innovation-and-boosts-investor-protection/.

1807 Austl. Dep't of the Treasury, Statement on Developing an Innovative Australian Digital Asset Industry 3-6 (2025), https://treasury.gov.au/sites/default/files/2025-03/p2025-628504-s.pdf. This statement builds on an earlier proposed framework and consultations from October to November 2023. *See generally* Austl. Dep't of the Treasury, Regulating Digital Asset Platforms (2023), https://consult.treasury.gov.au/c2023-427004.

1808 *Australia Unveils Crypto Regulation Plan*, Digit. Watch (Mar. 21, 2025), https://dig.watch/updates/australia-unveils-crypto-regulation-plan.

1809 Press Release, Monetary Auth. of Sing., *MAS Issues Guidelines to Discourage Cryptocurrency Trading by General Public* (Jan. 17, 2022), https://www.mas.gov.sg/news/media-releases/2022/mas-issues-guidelines-to-discourage-cryptocurrency-trading-by-general-public.

digital asset businesses have instead been supervised mainly through the licensing regime for digital payment token service providers under the Payment Services Act.[1810] These early measures enabled regulators to study emerging technologies and assess their implications without imposing premature or potentially stifling legislation.

This observational phase proved transitional: MAS subsequently moved beyond a purely guidance-based stance by introducing binding licensing regimes. MAS also postponed the rollout of new prudential crypto-exposure rules for banks until January 1, 2027, to align with evolving international Basel III standards.[1811] Notably, the stablecoin framework and the Digital Token Service Provider (DTSP) licensing regime, established under the Financial Services and Markets Act 2022 (FSMA 2022), entered into force on June 30, 2025.[1812] Singapore's evolution illustrates how jurisdictions may use an observational approach as a preliminary phase before adopting more comprehensive regulatory frameworks.

- **United States**

In the United States, the Securities and Exchange Commission (SEC) issued interpretive guidance in 2017 through its Report of Investigation on The DAO (the "DAO Report"),[1813] followed by the 2019 Framework for "Investment Contract" Analysis of Digital Assets.[1814] However, the SEC's guidance left significant questions unanswered regarding which digital assets would be classified as securities. This ambiguity contributed to the SEC's subsequent reliance on case-by-case enforcement actions to clarify regulatory boundaries, as discussed below in section 7.2.2.A.

While regulatory guidance can provide a degree of legal clarity, it lacks binding force and may be disregarded by courts, which undermines its reliability and limits its capacity to resolve regulatory uncertainty. At the same time, guidance can function as a transitional tool, offering regulated entities a measure of predictability during periods of legal indeterminacy. In practice, an observational approach frequently serves as a preliminary stage for policymakers before the adoption of more comprehensive and formal regulatory frameworks.

7.1.2. Sandboxing

A *regulatory sandbox* is a controlled environment that allows firms to test innovative products, services, or business models under temporarily relaxed legal and regulatory conditions, while remaining under close supervision by regulatory authorities. This framework enables firms to operate in real-world market conditions and interact with actual consumers, while receiving regulatory guidance throughout the experimentation phase. The primary objective is to provide early-stage companies with an opportunity to develop and test new technologies or business approaches without being fully subject to existing regulatory obligations —such as those relating to investor protection or consumer safeguards. This temporary regulatory flexibility allows regulators to gain insight into emerging technologies and to assess their

1810 Dawn Chew, Director (Corp. Commc'ns), Monetary Auth. of Sing., *Response to Letter "Singapore Treads Uneasily in Crypto Sandbox" – Financial Times, 22 August 2023* (Sept. 4, 2023), https://www.mas.gov.sg/news/letters-to-editor/2023/response-to-letter-on-crypto-sandbox (clarifying that no cryptocurrency payment providers had qualified for MAS's FinTech Regulatory Sandbox and that such firms are instead subject to licensing and supervisory requirements, including under Singapore's Payment Services Act.

1811 Monetary Auth. of Sing., *Prudential Treatment of Crypto-asset Exposures and Requirements for Additional Tier 1 and Tier 2 Capital Instruments for Banks*, section 2.5 (Oct. 2025), https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/ppd/2025/response-to-consultation-paper-on-crypto-at1-and-tier2.pdf.

1812 *See generally* Monetary Auth. of Sing., Financial Services and Markets Act 2022: *Guidelines on Licensing for Digital Token Service Providers* (May 30, 2025), https://www.mas.gov.sg/regulation/guidelines/guidelines-on-licensing-for-dtsps; Eng Han Goh & Nicholas Tok, *Singapore Stablecoin Regulation – MAS Confirms Its Framework*, Reed Smith (Aug. 23, 2023), https://www.reedsmith.com/en/perspectives/2023/08/singapore-stablecoin-regulation-mas-confirms-its-framework (describing the single-currency stablecoin framework by the regulator that requires issuers of stablecoins to meet certain consumer protection, anti-money laundering, anti-terrorism financing, and other requirements).

1813 *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Securities Act Release No. 81207, SEC (July 25, 2017), https://www.sec.gov/files/litigation/investreport/34-81207.pdf

1814 *Framework for "Investment Contract" Analysis of Digital Assets*, SEC (Apr. 3, 2019), https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets.

implications for existing legal frameworks. In exchange for this leniency, sandbox participants are typically subject to specific limitations, including caps on customer numbers, transaction volumes, or risk exposure, and they must comply with enhanced supervisory requirements.

The concept originated with the United Kingdom's Financial Conduct Authority (FCA), which introduced the term *regulatory sandbox* in 2015[1815] and outlined provisions for companies with blockchain technologies that would like to subscribe to the program.[1816] The agency approved the first cohort of financial-technology firms in 2016.[1817] In September 2024, the Bank of England, along with the FCA, initiated the Digital Securities Sandbox (DSS).[1818] Blockchain technology firms can use the DSS to "undertake the activities of notary, maintenance and settlement for financial securities either alone, or together with the operation of a trading venue."[1819] Organizations outside the regulatory sandbox may transact with sandbox-participating firms. A participating firm can choose which "financial instruments it wants to trade and/or undertake notary, maintenance or settlement activities in."[1820] The sandbox itself is a four-stage process, with Stage Two serving as a testing phase and Stage Three serving as a scaling option under strict supervision, with the option to do live business with their product under set limits. If a participating firm is found to be compliant with all the sandbox requirements, it can then be given a path to operate outside of the sandbox and in the real world.

Empirical studies found that sandbox participants subsequently raise "significantly more capital in the quarters after entry"[1821] and are more likely to remain in business and produce patents.[1822] Other countries have taken note. The Swiss FINMA introduced a license-exempt sandbox for innovative firms *(See below section 7.3.4.A.)*.[1823] The Canadian Securities Administration launched a regulatory sandbox initiative in 2017.[1824] Other jurisdictions around the world have started sandbox programs, too, including Singapore,[1825] Luxembourg,[1826] the United Arab Emirates,[1827] Indonesia,[1828] Malaysia,[1829] Thailand,[1830] and Brazil.[1831]

1815 Giulio Cornelli, Sebastian Doerr, Leonardo Gambacorta & Ouarda Merrouche, *Regulatory Sandboxes and Fintech Funding: Evidence from the UK*, 28 Rev. Fin. 203, 231 (2024), https://doi.org/10.1093/rof/rfad017.

1816 *Regulatory Sandbox*, Fin. Conduct Auth. (Mar. 27, 2022), https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

1817 *Regulatory Sandbox Accepted Firms*, Fin. Conduct Auth. (Mar. 27, 2022), https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms (scroll down and click on "Cohort 1 firms" to see the first batch of approved applications).

1818 *Digital Securities Sandbox (DSS)*, Bank of Eng., https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox (last visited Jan. 15, 2026).

1819 *Id.*

1820 *Digital Securities Sandbox Joint Bank of England and FCA Consultation Paper*, Bank of Eng. (Apr. 3, 2024), https://www.bankofengland.co.uk/paper/2024/cp/digital-securities-sandbox-joint-bank-of-england-and-fca-consultation-paper.

1821 Cornelli et al., *supra* note 1815, at 231.

1822 *Id.*

1823 Swiss Fin. Mkt. Supervisory Auth., *Fintech: Licensing and Supervisory Issues* (Mar. 17, 2016), https://www.finma.ch/en/news/2016/03/20160317-mm-fintech/. The Swiss sandbox allows companies to accept deposits from the public up to 1 million Swiss Francs without a license to test fintech projects. However, such projects are not supervised by FINMA and the deposits are unprotected. Alexander Vogel, Reto Luthiger & Diana Lafita, *Fintech Laws and Regulations 2025 - Switzerland*, Glob. Legal Insights (Jan. 9, 2025), https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/switzerland/.

1824 *The Canadian Securities Administrators Launches a Regulatory Sandbox Initiative*, Can. Sec. Adm'rs (Feb. 23, 2017), https://www.securities-administrators.ca/news/the-canadian-securities-administrators-launches-a-regulatory-sandbox-initiative/ ("To apply to the CSA regulatory sandbox, businesses should contact their local securities regulator, which will consider its eligibility and refer it to the CSA regulatory sandbox if it provides genuine technological innovation in the securities industry.")

1825 Monetary Auth. of Sing., *Overview of Regulatory Sandbox*, https://www.mas.gov.sg/development/fintech/regulatory-sandbox (last visited Jan. 15, 2026).

1826 *Infrachain: Weaving a Blockchain Ecosystem*, Innovative Initiatives Digit. Lux., https://innovative-initiatives.public.lu/stories/infrachain-weaving-blockchain-ecosystem (last visited Jan. 15, 2026) (a Luxembourg government-supported nonprofit that hosts blockchain nodes for various blockchain projects, conducts research, and is involved in pilots and proof-of-concepts).

1827 *Regulatory Sandboxes in the UAE*, The Off. Platform of the UAE Gov't, https://web.archive.org/web/20250914124031/https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/regulatory-sandboxes-in-the-uae (last visited Jan. 15, 2026) (archived version by the Internet Archive).

1828 *Regulatory Sandbox*, Otoritas Jasa Keuangan [Indon. Fin. Servs. Auth.], https://ojk.go.id/en/Fungsi-Utama/ITSK/Regulatory-Sandbox/Default.aspx (last visited Jan. 15, 2026).

1829 *Regulatory Sandbox*, Bank Negara Malaysia [Cent. Bank of Malay.], https://www.bnm.gov.my/sandbox (last visited Jan. 15, 2026).

1830 *Regulatory Sandbox*, Thanakhan Haeng Prathet Thai [Bank of Thai.], https://www.bot.or.th/en/financial-innovation/digital-finance/fintech-in-thailand/regulatory-sandbox.html (last visited Jan. 15, 2026).

1831 *Regulatory Sandbox*, Banco Central Do Brasil [Cent. Bank of Braz.], https://www.bcb.gov.br/en/financialstability/regulatorysandbox (last visited Jan. 15, 2026).

In Europe, the European Commission launched the European Blockchain Regulatory Sandbox (EBRS) in 2023 as a forum for regulatory dialogue on distributed-ledger and blockchain use cases.[1832] Running through 2026, the EBRS supports approximately 20 projects per year and is open to both public- and private-sector initiatives. Unlike national sandboxes, it does not provide regulatory exemptions, but instead offers legal advice, regulatory guidance, and a confidential space for interaction with EU and national authorities. Its objective is to deepen regulators' technical understanding of blockchain and DLT solutions, facilitate co-learning between innovators and policymakers, and identify best practices for the wider market.

Regulatory sandboxes have attracted scholarly support. Primavera De Filippi, Morshed Mannan, and Wessel Reijers describe regulatory sandboxes as a mechanism for addressing the alegality of blockchain technology *(See section 6.1.3)*.[1833] According to them, the use of regulatory sandboxes allows one to evaluate whether the practices and processes developed by blockchain initiatives achieve "functional equivalence" and "regulatory equivalence" with existing legal requirements (on these concepts, *See section 1.3.2*).[1834] Karen Yeung calls it "efficient alignment," in which both the law and blockchain projects adapt in ways that mutually reinforce each other.[1835] However, despite their benefits, sandboxes raise normative and governance concerns. Their discretionary admission processes may lack transparency and risk conferring disproportionate advantages on selected participants, thereby challenging principles of equality before the law and regulatory neutrality. The selective nature of sandbox admission may also invite judicial scrutiny, especially if the scheme disproportionately favors specific technologies or business models. Moreover, sandboxes blur the line between law-making and administrative experimentation.

7.2. APPLYING EXISTING FRAMEWORKS: THE U.S. EXPERIENCE

The previous section examined *observational* approaches. This section examines more *active* strategies to oversee blockchain activity —strategies that nonetheless stop short of adopting new, tailored legal frameworks specifically designed for blockchain technology. Instead, some regulators, particularly in the United States, have attempted to apply existing legal frameworks to blockchain activities, with varying degrees of success.

The U.S. experience provides a particularly illustrative example of these approaches and merits extended examination given its global influence on crypto regulation. It has taken three distinct forms. First, some agencies, before pursuing enforcement, issue interpretive guidance to put the industry on notice. The U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and the Internal Revenue Service (IRS) have adopted this traditional "guidance followed by enforcement" approach. Second, other agencies, particularly the SEC and CFTC, rely primarily on case-by-case enforcement actions to clarify legal standards ex post, rather than issuing clear rules ex ante, an approach characterized as "regulation by enforcement." Third, the Department of Justice pursues criminal prosecutions to establish regulatory boundaries, a strategy termed "regulation by prosecution."

1832 *European Blockchain Regulatory Sandbox*, Eur. Comm'n, https://digital-finance-platform.ec.europa.eu/cross-border-services/ebsi (last visited Jan. 15, 2026).

1833 *Cf.* Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance*, 92 Geo. Wash. L. Rev. 1229, 1229, 1272 (2024), https://www.gwlr.org/wp-content/uploads/2024/12/92-Geo.-Wash.-L.-Rev.-1229.pdf.

1834 Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 Pol'y & Soc'y 358, 368 (2022), https://ssrn.com/abstract=4001696.

1835 *Id.* at 1272-73 (quoting Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code* of *Law and Code* as *Law*, 82 Mod. L. Rev. 207, 215, 220-22 (2019), https://www.jstor.org/stable/45220933).

The enforcement-focused approach has proven controversial. By 2025, mounting criticism of "regulation by enforcement" and "regulation by prosecution" led to a significant policy shift under the second administration of President Trump. It did not fully abandon enforcement as a regulatory tool but instead moved toward clearer ex ante guidance and new legislative frameworks.

7.2.1. Guidance Followed by Enforcement: FinCEN and IRS

Some federal agencies issued interpretive guidance before pursuing enforcement. FinCEN and the IRS exemplify this strategy: Both clarified how, through advance guidance, existing frameworks —money transmission laws and tax regulations— would apply to digital assets. They then enforced those standards against non-compliant entities.

Applying existing legal frameworks to blockchain activities has required these agencies to classify blockchain-based assets and transactions to determine whether and how their regulatory mandates apply. Because blockchain activities exhibit unprecedented features, both agencies have devoted significant effort to determining whether crypto-assets and related activities satisfy the statutory criteria under their respective jurisdictions. FinCEN focused on whether activities constituted "money transmission" subject to anti-money laundering obligations, while the IRS classified digital assets as "property" for tax purposes. These classifications have carried significant regulatory consequences for market participants.

7.2.1.A. FinCEN: Money Transmission Framework

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has been consistently providing advance notice through guidance, then vigorously pursuing entities that fail to comply with established obligations. Of course, determining whether digital assets fall within the scope of banking regulations or laws regarding money services business (MSB) requires a determination of whether activities involving blockchain qualify as "money transmission." If classified as money transmission, the entities involved become subject to federal anti-money laundering (AML) laws and the obligations countering the financing of terrorism (CFT), in addition to state licensing requirements.

As early as 2011, FinCEN clarified and updated the regulatory definition of "money transmission services" under the Bank Secrecy Act (BSA),[1836] in particular through amendments not specific to digital assets but intended to modernize the MSB framework. These revisions provided a legal foundation that would later be extended to new digital forms of value transfer. In 2013, FinCEN issued interpretive guidance expressly applying this definition to "convertible virtual currencies." It determined that administrators and exchangers of virtual currency —such as cryptocurrency exchanges and certain payment processors acting as intermediaries— must register as money transmitters and comply with the full range of BSA obligations.[1837] As a result, these businesses became subject to extensive AML and CFT duties, comparable in scope, though not in prudential intensity, to those imposed on banks under the BSA.[1838]

Since then, FinCEN has issued further guidance clarifying what types of blockchain-based activities may trigger MSB

1836 31 C.F.R. § 1010.100(ff)(5)(A) ("The term 'money transmission services' means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.").

1837 Fin. Crimes Enf't Network, FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* 3, 5 (Mar. 18, 2013) [hereinafter 2013 FinCEN Guidance], https://www.fincen.gov/system/files/shared/FIN-2013-G001.pdf (explicitly referring to "de-centralized virtual currencies . . . that ha[ve] no central repository and no single administrator, and [] that persons may obtain by their own computing or manufacturing effort"). *See also* Fin. Crimes Enf't Network, FIN-2014-R001, *Application of FinCEN's Regulations to Virtual Currency Mining Operations* 3-4 (Jan. 30, 2014), https://www.fincen.gov/system/files/shared/FIN-2014-R001.pdf.

1838 *See* 31 C.F.R. § 1022.380 (2024), https://www.govinfo.gov/app/details/CFR-2024-title31-vol3/CFR-2024-title31-vol3-sec1022-380 (listing the regulatory requirements to register as a money transmitter in compliance with the BSA).

regulation.[1839] The agency's regulatory perimeter does not hinge on the legal classification of digital assets alone. Instead, it hinges on the combination of the characteristics of the value transferred and the nature of the activities conducted with those assets.[1840] FinCEN's regulations and guidance documents do not, therefore, govern the assets or markets directly; rather, they impose obligations on covered entities to monitor flows of value and mitigate the associated AML/CFT risks.[1841]

FIGURE 54.

FINCEN enforcement actions

FinCEN has actively enforced BSA/AML rules through significant penalties against non-compliant virtual currency exchanges. Early actions, like the $700,000 fine against Ripple Labs in 2015 for unregistered operations and inadequate AML programs, set the stage.[1842]

Subsequent enforcement targeted more severe and varied misconduct, including a $110 million penalty against BTC-e in 2017 for facilitating illicit transactions[1843] and a $60 million fine against the operator of Bitcoin mixers Helix and Coin Ninja in 2020.[1844] Similarly, Bittrex faced a penalty of over $29 million in 2022 for such things as processing transactions with entities sanctioned by the U.S. Treasury's Office of Foreign Assets Control and failing to file suspicious activity reports (SARs).[1845]

Penalties have escalated dramatically, as seen with BitMEX's $100 million fine in 2021 for unregistered operations and AML failures.[1846] They culminated in the landmark $3.4 billion FinCEN settlement with Binance in November 2023 for widespread violations of the BSA —part of a broader multi-agency resolution that also resulted in Binance's effective withdrawal from the U.S. market.[1847] These actions demonstrated FinCEN's increasing resolve to penalize failures in MSB registration, AML program implementation, customer due diligence, and suspicious activity reporting.

1839 *See, e.g.*, Fin. Crimes Enf't Network, FIN-2014-R011, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* 1-5 (Oct. 27, 2014), https://www.fincen.gov/system/files/shared/FIN-2014-R011.pdf (applying the MSB framework to crypto trading platforms); Fin. Crimes Enf't Network, FIN-2014-R012, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System* 1, 5 (Oct. 27, 2014), https://www.fincen.gov/system/files/shared/FIN-2014-R012.pdf (applying the MSB framework to a platform that accepts and processes cryptocurrency payments); Fin. Crimes Enf't Network, FIN-2015-R001, *Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals* 1, 4-5 (Aug. 14, 2015), https://www.fincen.gov/system/files/shared/FIN-2015-R001.pdf (applying the MSB framework to a company that trades in precious metals using cryptocurrency and issues digital proofs of custody) .

1840 Fin. Crimes Enf't Network, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* 12 (May 19, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. In fact, the legal treatment of virtual currencies such as cryptocurrency and the status of entities dealing with them are intertwined. FinCEN treats entities that work with "currency, funds, or other value that substitutes for currency"—the latter encompassing cryptocurrency business activity—as MSBs subject to a host of federal regulations. 2013 FinCEN Guidance, *supra* note 1837, at 3. *See also* 31 C.F.R. § 1010.100(ff)(5)(i)(A).

1841 U.S. Dep't of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* 50-51 (Sept. 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

1842 Press Release, Fin. Crimes Enf't Network, *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger* (May 5, 2015), https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual.

1843 Press Release, Fin. Crimes Enf't Network, *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales* (July 27, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransornware.

1844 Press Release, Fin. Crimes Enf't Network, *First Bitcoin Mixer Penalized by FinCEN for Violating Anti-Money Laundering Laws* (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

1845 Press Release, Fin. Crimes Enf't Network, *FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Systemic Violations of the Bank Secrecy Act* (Oct. 11, 2022), https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service. Suspicious activity reports (or SARs) are a mechanism to "report known or suspected violations of law or suspicious activity observed by financial institutions" that are subject to AML/CFT laws and regulations. Fin. Crimes Enf't Network, *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* 1 (2003), https://www.fincen.gov/system/files/shared/sarnarrcompletguidfinal_112003.pdf.

1846 Press Release, Fin. Crimes Enf't Network, *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act* (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.

1847 Press Release, Fin. Crimes Enf't Network, *FinCEN Announces Largest Settlement in U.S. Treasury Department History with a Virtual Asset Service Provider* (Nov. 21, 2023), https://www.fincen.gov/news/news-releases/fincen-announces-largest-settlement-us-treasury-department-history-virtual-asset.

At the state level, approaches to regulating virtual currency activities have diverged from focusing on the status of cryptocurrency and tokens to defining coverage based on the functional role of an entity in a transaction *(See Appendix 17)*. Certain states, such as Vermont,[1848] Washington,[1849] and Pennsylvania,[1850] have followed federal authority and integrated virtual currencies into their money transmission laws, requiring certain businesses dealing in cryptocurrency to obtain money transmission licenses. Others, such as Kansas,[1851] Wisconsin,[1852] and Wyoming,[1853] have concluded that virtual currencies do not constitute money under their respective money transmission laws. New York[1854] and California[1855] have created separate virtual currency license regimes *(See Appendix 17)*. Yet, other states, like Florida and Texas, now require a money transmitter license only in limited circumstances: in Florida, only for persons acting as intermediaries with the unilateral ability to control the execution of a transaction,[1856] and in Texas, only when fiat currency or a stablecoin is involved.[1857]

7.2.1.B. IRS: Crypto-assets as Property

In a separate regulatory sphere, the U.S. Internal Revenue Service (IRS) has long treated digital assets as "property" for purposes of federal taxation. This classification, first articulated in 2014, established that the disposition of crypto-assets —whether by sale, exchange, or conversion into fiat currency— constituted a taxable event, with gains or losses calculated against the taxpayer's cost basis.[1858] Unlike currency transactions, which may be exempt from recognition of gain in certain circumstances, the property classification ensures that even routine digital asset transactions may trigger reporting obligations.[1859]

Enforcement has reflected this approach. The IRS has conducted audits and pursued litigation against individuals and entities that failed to disclose cryptocurrency-related income. In 2024, for example, federal prosecutors charged Frank Richard Ahlgren III of Austin, Texas, with failing to report $4 million in sales of Bitcoin and related capital gains realized in 2017 and 2019.[1860] This matter was notable as one of the first criminal cases centered exclusively on the failure to report cryptocurrency-derived income, without accompanying charges of fraud or money laundering.[1861]

1848 Vt. Stat. Ann. tit. 8, §§ 2503(27)-(32) (2025).

1849 Wash. State Dep't of Fin. Insts., *Virtual Currency and Money Transmission Laws* 1-3 (2021), https://dfi.wa.gov/sites/default/files/virtual-currency-money-transmission-laws.pdf.

1850 Press Release, Penn. Dep't of Banking & Sec., *Pennsylvania Department of Banking and Securities to Begin Regulating Virtual Currency Transmitters Thanks to New Bipartisan Law Signed by Governor Shapiro* (June 28, 2025), https://www.pa.gov/agencies/dobs/newsroom/dobs-regulating-virtual-currency-transmitters-thanks-to-new-bipa.

1851 Kan. Off. of the State Bank Commn'r, CML Guidance MT 2014-01, *Cryptocurrency Guidance Document* 3 (June 6, 2014), https://www.osbckansas.gov/cml/mt_2014_01.pdf.

1852 *Money Transmitter Modernization Act*, Wis. Dep't of Fin. Insts., https://dfi.wi.gov/Pages/FinancialServices/LicensedFinancial/MoneyTransmitterModernizationAct.aspx (last visited Jan. 15, 2026).

1853 Wyo. Stat. Ann. § 40-22-104 (West 2024).

1854 N.Y. Fin. Serv. Law §§ 200.1(p)-(q), 200.3(a) (McKinney 2015) (New York's license for virtual currency businesses is colloquially called "BitLicense"). See, e.g., *Virtual Currency Business Licensing*, N.Y. Dep't of Fin. Servs., https://www.dfs.ny.gov/virtual_currency_businesses (last visited Jan. 15, 2026) (New York licensing regime for actors willing to enter virtual currency marketplaces).

1855 *Digital Financial Assets*, Cal. Dep't of Fin. Prot. & Innovation (Dec. 16, 2024), https://dfpi.ca.gov/regulated-industries/digital-financial-assets/ (explicitly referring to licensing of activity involving digital financial assets that include cryptocurrency); Digital Financial Assets, Cal. Dep't of Fin. Prot. & Innovation, https://dfpi.ca.gov/regulated-industries/digital-financial-assets/ (last visited Jan. 15, 2026) (California licensing regime for companies willing to engage in transactions involving digital assets).

1856 Fla. Stat. § 560.103(24) (2025).

1857 Tex. Dep't of Banking, *Supervisory Memorandum – 1037*, at 2-3 (Jan. 28, 2025), https://www.dob.texas.gov/public/uploads/files/Laws-Regulations/New-Actions/sm1037.pdf.

1858 *See* I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, 938-40 (Mar. 25, 2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

1859 For example, transactions with currency "could generate foreign currency gain or loss," with some exchange-rate gain exempt from tax or reporting. But since crypto is not "currency" but "property," every sale, purchase, or exchange generally constitutes a taxable event that must be reported. *See id.* at 2-4.

1860 Michelle Legge, *What Happens if You Don't Report Cryptocurrency on Taxes in 2025?*, Koinly, https://koinly.io/blog/crypto-tax-evasion/ (last visited Jan. 15, 2026).

1861 Press Release, Off. of Pub. Affs., U.S. Dep't of Just., *Early Bitcoin Investor Sentenced for Filing Tax Returns that Falsely Reported His Cryptocurrency Gains* (Dec. 12, 2024), https://www.justice.gov/archives/opa/pr/early-bitcoin-investor-sentenced-filing-tax-returns-falsely-reported-his-cryptocurrency.

The regulatory framework has continued to evolve. In June 2024, the IRS finalized its regulations implementing provisions of the bipartisan Infrastructure Investment and Jobs Act.[1862] These rules govern the reporting requirements that apply to brokers in digital assets. Specifically, starting in 2026, the IRS will require brokers dealing in such assets to report their gross proceeds from digital asset sales, covering all sales made in 2025. They will also have to report certain tax information in 2027 for sales in 2026.[1863] These rules not only reaffirm the property classification for digital assets, they also support tax compliance and move cryptocurrency into a similar reporting framework that exists for securities.[1864] In December 2024, the IRS issued a similar reporting requirement rule that applied to certain non-custodial or decentralized finance (DeFi) service providers.[1865] However, in spring 2025, the U.S. Congress passed a joint resolution disapproving of this rule, and the President signed it into law, citing impractically high compliance burdens for small businesses and non-custodial systems.[1866] The resolution effectively repealed the rule that applied to these decentralized exchanges.[1867] However, the reporting mandate from June 2024 that applies to brokers in digital assets remains in effect.[1868]

7.2.2. Regulation by Enforcement: The SEC and CFTC Approach

"Regulation by enforcement" refers to a regulatory strategy in which standards are developed and clarified ex post, through case-by-case enforcement actions, rather than ex ante, through detailed rulemaking or legislation.[1869] In the absence of active rulemaking, authorities apply existing legal norms to new or uncertain domains by initiating enforcement proceedings, thereby shaping expectations incrementally through precedential outcomes, rather than through formal legislative or administrative guidance.

Agencies such as the SEC and the CFTC delineated regulatory boundaries largely through selective enforcement actions, rather than by issuing clear rules in advance. Proponents argue that this strategy affords regulators flexibility to address novel challenges in a rapidly evolving technological landscape, while avoiding premature rules that may soon become obsolete.

7.2.2.A. The SEC: Crypto-assets as Securities

Few regulatory classifications are as contentious as the question of whether digital tokens should be deemed

1862 Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021).

1863 Press Release, U.S. Dep't of the Treasury, *IRS Release Final Regulations Implementing Bipartisan Tax Reporting Requirements for Sales and Exchanges of Digital Assets* (June 28, 2024), https://home.treasury.gov/news/press-releases/jy2438. *See also Digital Assets*, Internal Revenue Serv., https://www.irs.gov/filing/digital-assets (last visited Jan. 15, 2026).

1864 Press Release, U.S. Dep't of the Treasury, *Id.* (the final regulations are intended "to help taxpayers file accurate returns and pay taxes owed under current law"). Brokers trading in securities must file a tax form with similar information (e.g., gross proceeds). *See generally Instructions for Form 1099-B (2025)*, Internal Revenue Serv., https://www.irs.gov/instructions/i1099b (last visited Jan. 15, 2026).

1865 *See Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales*, 89 Fed. Reg. 106928, 106933-36 (Dec. 30, 2024), https://www.govinfo.gov/content/pkg/FR-2024-12-30/pdf/2024-30496.pdf.

1866 Press Release, U.S. H. Comm. on Ways & Means, *President Trump Signs Ways & Means Resolution Overturning Biden Administration's Burdensome IRS DeFi Broker Rule* (Apr. 10, 2025), https://waysandmeans.house.gov/2025/04/10/president-trump-signs-ways-means-resolution-overturning-biden-administrations-burdensome-irs-defi-broker-rule/.

1867 *See generally Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales*, 90 Fed. Reg. 30825 (July 11, 2025), https://www.federalregister.gov/documents/2025/07/11/2025-12967/gross-proceeds-reporting-by-brokers-that-regularly-provide-services-effectuating-digital-asset-sales.

1868 The June 2024 regulations (Treasury Decision 10000) requiring custodial digital asset brokers to file Form 1099-DA reporting gross proceeds (starting 2026 for 2025 sales) and basis information (starting 2027 for 2026 sales) remain in effect. Tim Shaw, *Preparing for New 1099 Digital Asset Reporting Rules*, Thomson Reuters Tax & Acct. (Nov. 20, 2025), https://tax.thomsonreuters.com/news/preparing-for-new-1099-digital-asset-reporting-rules/.

1869 *See* Cary Coglianese, *Rule Design: Defining the Regulator-Regulatee Relationship*, *in* The Regulator-Regulatee Relationship in High-Hazard Industry Sectors: New Actors and New Viewpoints in a Conservative Landscape 91-94 (Jean-Christophe Le Coze & Benoît Journé eds., 2024), https://link.springer.com/book/10.1007/978-3-031-49570-0 (suggesting different regulatory rule designs, including management-based regulation that involves rules "articulated in terms of broader principles" and internal rulemaking by regulatees). For an example of "regulation by enforcement" in the securities context, see generally Harvey L. Pitt & Karen L. Shapiro, *Securities Regulation by Enforcement: A Look Ahead at the Next Decade*, 7 Yale J. Regul. 149 (1990), https://openyls.law.yale.edu/server/api/core/bitstreams/9d351c25-3bfb-4f3c-bbd4-ce80e7b5d0c7/content.

securities. The U.S. Securities and Exchange Commission (SEC) has been at the forefront of this debate by invoking the *Howey* test, a judicially created standard originating from the 1946 Supreme Court decision in *SEC v. W.J. Howey Co.* The *Howey* decision set forth how to evaluate whether an arrangement or transaction constitutes an "investment contract" under the securities laws.[1870] The court defined an "investment contract" as any arrangement involving (1) an investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profits, (4) to be derived from the efforts of others.[1871]

Unlike FinCEN and the IRS, which provided relatively clear ex ante guidance about how existing regulations would apply to digital assets before pursuing enforcement *(See section 7.2.1)*, the SEC's approach to regulatory clarity differed significantly. The SEC early pursued actors involved in Ponzi schemes,[1872] bitcoin-related stock exchanges,[1873] and unregistered securities offerings that used Bitcoin.[1874] In July 2017, the SEC issued its Report of Investigation on The DAO,[1875] which applied the *Howey* test to conclude that certain digital tokens sold through initial coin offerings (ICOs) could constitute securities. While this report signaled the SEC's regulatory interest, it remained largely backward-looking and fact-specific, offering limited prospective guidance on which features would cause future token offerings to qualify as securities.

The SEC subsequently issued additional interpretive materials, most notably the 2019 Framework for "Investment Contract" Analysis of Digital Assets,[1876] which outlined factors the agency would consider when evaluating whether digital assets constitute investment contracts. However, this framework was released as nonbinding staff guidance rather than formal rulemaking. And it left substantial interpretive questions unanswered —particularly regarding how decentralization, secondary market sales, and the evolution of token functionality over time would affect securities classification. In a 2018 speech that prefigured some of these ambiguities, William Hinman, then Director of the SEC's Division of Corporate Finance, emphasized that digital assets are akin to the investment in citrus groves in *Howey:* They are merely the object of the investment contract. The circumstances of the offering transaction determine whether the token is part of an investment contract.[1877] More interestingly, Hinman contended that, "if the network on which the token or coin is to function is sufficiently decentralized," the asset

1870 *See generally U.S. Sec. & Exch. Comm'n v. W. J. Howey Co.*, 328 U.S. 293 (1946), https://tile.loc.gov/storage-services/service/ll/usrep/usrep328/usrep328293/usrep328293.pdf.

1871 *Id.* at 301. The original formulation in *SEC v. W.J. Howey Co.* referred to profits derived "solely from the efforts of others." Subsequent case law has relaxed this requirement, interpreting it more flexibly as requiring that profits be derived primarily or predominantly from the efforts of others.

1872 *Trendon T. Shavers & Bitcoin Sav. & Tr.*, Litigation Release No. 23090, No. 4:13-cv-16 (Sept. 22, 2014), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-23090; Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Bitcoin Mining Companies* (Dec. 1, 2015), https://www.sec.gov/newsroom/press-releases/2015-271.

1873 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations* (Dec. 8, 2014), https://www.sec.gov/newsroom/press-releases/2014-273.

1874 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Bitcoin Entrepreneur with Offering Unregistered Securities* (June 3, 2014), https://www.sec.gov/newsroom/press-releases/2014-111.

1875 *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Exchange Act Release No. 81207 (July 25, 2017), https://www.sec.gov/files/litigation/investreport/34-81207.pdf; *Investor Bulletin: Initial Coin Offerings*, U.S. Sec. & Exch. Comm'n (July 25, 2017), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-16. *But see* Antonita Madonna, *U.S. SEC Debates Relevance of Howey Test on Digital Assets; Investor Protection Worries Linger*, Thomson Reuters Regul. Intel. (Mar. 25, 2025), https://regintel-content.thomsonreuters.com/document/I1F84BAE0093E11F0869EF8E9AE1FF3F0 (noting that the current administration appears to be moving away from "the enforcement-heavy stance adopted by the previous administration," which includes revisiting the application of *Howey* to cryptocurrency).

1876 *Framework for "Investment Contract" Analysis of Digital Assets*, SEC (Apr. 3, 2019), https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets.

1877 William Hinman, Dir., Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n, *Remarks at the Yahoo Finance All Markets Summit: Crypto* (June 14, 2018), https://www.sec.gov/newsroom/speeches-statements/speech-hinman-061418.

may no longer represent an investment contract.[1878] Yet neither Hinman's speech nor the 2019 Framework provided clear criteria for determining when sufficient decentralization had been achieved. As SEC Commissioner Hester Peirce later observed, the Framework's multi-factor analysis provided little certainty about where the agency would draw regulatory lines.[1879]

This limited and interpretive approach to guidance left market participants uncertain about which tokens would be deemed securities until enforcement actions clarified the agency's position on specific fact patterns. Despite the issuance of these interpretive materials, enforcement actions rather than further guidance became the SEC's primary means of articulating securities law requirements for digital assets, a dynamic that came to characterize the "regulation by enforcement" strategy. Between 2017 and 2019, the SEC brought actions against issuers and intermediaries alike.[1880] It stressed that rebranding tokens as "utility tokens" did not remove them from the realm of securities law if investors expected profits based on the managerial efforts of the token issuers or third parties.[1881] Several ICO enforcement actions during this period further clarified the application of the Howey test to token offerings. In particular, federal courts confirmed the SEC's approach in SEC v. Kik Interactive Inc.[1882] and SEC v. Telegram Group Inc.,[1883] holding that token sales conducted as part of fundraising schemes constituted unregistered securities offerings when investors reasonably expected profits from the issuer's efforts.

From 2020 onward, the SEC expanded its enforcement agenda beyond ICOs, clarifying its intention to apply the federal securities laws more broadly to digital assets.[1884] The litigation against Ripple Labs, initiated in December 2020, is particularly illustrative *(See below Figure 55)*. The SEC also targeted major algorithmic stablecoin projects. In 2024, a federal jury found Terraform Labs and its founder Do Kwon liable for defrauding investors by making misleading claims about TerraUSD's stability and the broader Terraform ecosystem *(See above Figure 27)*.[1885] The verdict reinforced the SEC's jurisdiction over stablecoins and extended securities law principles to new categories of crypto-assets. Likewise, the Commission joined the Department of Justice in prosecuting SafeMoon executives for fraud and unregistered securities offerings.[1886]

Enforcement against digital asset intermediaries intensified during the same period. In 2023, the SEC targeted Kraken's operations twice: first, in an administrative action in which it alleged that Kraken offered and sold its crypto staking program to U.S. investors in violation of securities laws (Kraken settled those charges); second, in a federal court case in which the SEC argued that Kraken was an unregistered platform trading and conducting other activities in securities (the

1878 *Id.*

1879 Hester M. Peirce, Comm'r, SEC, *How We Howey*, Remarks at the Blockress Conference (May 9, 2019), https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

1880 *In re Munchee Inc.*, Securities Act Release No. 10445, 2017 WL 6374424 (Dec. 11, 2017), https://www.sec.gov/files/litigation/admin/2017/33-10445.pdf.

1881 Press Release, U.S. Sec. & Exch. Comm'n, *Company Halts ICO After SEC Raises Registration Concerns* (Dec. 11, 2017), https://www.sec.gov/newsroom/press-releases/2017-227. *See also* Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, *Statement on Cryptocurrencies and Initial Coin Offerings* (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

1882 *SEC v. Kik Interactive Inc.*, 492 F. Supp. 3d 169 (S.D.N.Y. 2020).

1883 *SEC v. Telegram Grp. Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020).

1884 Gary Gensler, Chairman, *Prepared Remarks on Crypto Markets at Penn Law Capital Markets Association Annual Conference,* U.S. Sec. & Exch. Comm'n (Apr. 4, 2022), https://www.sec.gov/newsroom/speeches-statements/gensler-remarks-crypto-markets-040422.

1885 *See* U.S. Sec. & Exch. Comm'n, *Statement on Jury's Verdict in Trial of Terraform Labs PTE Ltd. and Do Kwon* (Apr. 5, 2024), https://www.sec.gov/newsroom/speeches-statements/grewal-statement-040424 (statement regarding the Terraform litigation).

1886 *See* Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Crypto Company SafeMoon and its Executive Teams for Fraud and Unregistered Offering of Crypto Securities* (Nov. 1, 2023), https://www.sec.gov/newsroom/press-releases/2023-229.

SEC voluntarily dismissed the case).[1887] Likewise, SEC's enforcement actions against centralized exchanges, such as Coinbase or Binance,[1888] further highlighted the agency's determination to treat most crypto-assets as securities. It did so even as court decisions vacated other initiatives, such as rules extending to crypto trading businesses the registration requirement traditionally applied to "dealer" market participants only.[1889] These cases reflected a shift in enforcement attention from token issuers to trading and lending platforms.

Enforcement statistics underscore this evolution. In 2023, the SEC brought a record 46 crypto-related actions, most involving unregistered securities offerings or fraud.[1890] Although the number of cases decreased slightly in 2024, the financial impact of penalties increased dramatically, driven by the $4.5 billion settlement in *SEC v. Terraform Labs* (discussed in Figure 55). Collectively, these actions illustrated a transition from early ICO-focused enforcement toward a broader regulatory agenda that encompasses exchanges, stablecoins, and lending services. The actions also highlight the Commission's reliance on the *Howey* framework and its consistent message that relabeling tokens as "utility tokens" does not remove them from the scope of securities law. At the same time, securities regulators at the state level have brought their own enforcement actions under state securities laws (commonly known as "blue sky" laws), often coordinated through the North American Securities Administrators Association, reinforcing the application of securities regulation to crypto-assets at the state level.[1891]

1887 *See* Press Release, U.S. Sec. & Exch. Comm'n, *Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges* (Feb. 9, 2023), https://www.sec.gov/newsroom/press-releases/2023-25 (the inquiry ended with a multimillion dollar settlement and the termination of U.S. staking products); Payward, Inc. & Payward Ventures, Inc., Litigation Release No. 25896, No. 3:23-cv-06003 (Nov. 21, 2023), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-25896 (charging Kraken for operating "as an unregistered securities exchange, broker, dealer, and clearing agency"); Payward, Inc. & Payward Ventures, Inc., Litigation Release No. 26278, No. 3:23-cv-06003-WHO (Mar. 27, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26278 (noting that "the dismissal will facilitate the Commission's ongoing efforts to reform and renew its regulatory approach to the crypto industry").

1888 *See* Press Release, U.S. Sec. & Exch. Comm'n, *SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency* (June 6, 2023), https://www.sec.gov/newsroom/press-releases/2023-102 (charging Coinbase for the same violation of securities laws—unregistered national securities exchange, broker, and clearing agency—as Kraken); Press Release, U.S. Sec. & Exch. Comm'n, *SEC Announces Dismissal of Civil Enforcement Action Against Coinbase* (Feb. 27, 2025), https://www.sec.gov/newsroom/press-releases/2025-47 (dismissing the civil charges against Coinbase pending the newly created Crypto Task Force's "comprehensive and clear regulatory framework for crypto assets"); *Binance Must Face Bulk of US SEC Crypto Lawsuit, Judge Rules*, Reuters (June 29, 2024), https://www.reuters.com/legal/binance-must-face-bulk-us-sec-crypto-lawsuit-judge-rules-2024-06-29/.

1889 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Adopts Rules to Include Certain Significant Market Participants as "Dealers" or "Government Securities Dealers"* (Feb. 6, 2024), https://www.sec.gov/newsroom/press-releases/2024-14; Bruce H. Newman et al., *US District Court Vacates Controversial Dealer Rules*, WilmerHale (Dec. 13, 2024), https://www.wilmerhale.com/en/insights/client-alerts/20241213-us-district-court-vacates-controversial-dealer-rules (discussing the SEC rules and related litigation that struck them down). The SEC later decided not to proceed with its appeal of the district court's decision that vacated its "dealer" rules, see Stephen P. Wink, Naim Culhaci & Deric Behar, *SEC Withdraws Appeal of Court Decision to Vacate Its Dealer Rules*, Latham & Watkins LLP (Feb. 25, 2025), https://www.fintechanddigitalassets.com/2025/02/sec-withdraws-appeal-of-court-decision-to-vacate-its-dealer-rules.

1890 Cornerstone Rsch., SEC Cryptocurrency Enforcement: 2023 Update 1-2 (2024), https://www.cornerstone.com/insights/research/sec-cryptocurrency-enforcement-2025-update/.

1891 N. Am. Sec. Adm'rs Ass'n, *NASAA Enforcement Report and Top Threats for 2024* 6, 13 (2024), https://www.nasaa.org/wp-content/uploads/2024/10/FINAL_2024-Enforcement-Report.pdf.

FIGURE 55.

Applying the *Howey* Test to Crypto

Two landmark cases illustrate both the complexity and the divergent application of the U.S. Supreme Court's *Howey* test in the crypto asset context. In *SEC v. W.J. Howey Co.*, the Court held that a financial arrangement constitutes a security if it involves (1) an investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profits, (4) to be derived from the efforts of others. Applying a test articulated in 1946 to the novel features of blockchain-based technologies, however, has proven far from straightforward.[1892]

In the first case, *SEC v. Ripple Labs*,[1893] the U.S. District Court for the Southern District of New York adopted a transaction-specific approach to the application of U.S. securities law. It held there was a distinction between different categories of XRP (a digital token created by the financial technology firm Ripple Labs) sales. In its July 2023 summary-judgment decision, the court held that Ripple's *institutional sales* —direct, negotiated transactions with sophisticated or accredited investors pursuant to written contracts— constituted unregistered securities offerings. The judge held that institutional sales constituted securities offerings, while *programmatic sales* on secondary markets did not.[1894] The court reasoned that sophisticated buyers had a reasonable expectation of profits derived from Ripple's managerial and entrepreneurial efforts, thereby satisfying the *Howey* test.[1895] By contrast, Ripple's *programmatic sales* on digital asset exchanges did *not* constitute securities transactions since the sales occurred through automated, anonymous trading mechanisms in which retail purchasers transacted via blind bid-ask matching, without a direct relationship with Ripple.[1896] In that case, buyers could not reasonably be said to rely on Ripple's efforts to generate profits.

The decision, therefore, emphasized that XRP was not inherently a security; rather, its legal classification depended on the *specific circumstances* of *each* transaction. The legal reasoning was subject to significant debate within the legal community.[1897] In August 2024, the court entered a remedies order imposing injunctive relief and a $125 million civil penalty on Ripple Labs.[1898] In May 2025, the parties announced a proposed settlement framework under which Ripple would pay $50 million and the injunction against institutional XRP sales would be dissolved; the district court rejected this framework twice, refusing to reduce the penalty or lift the injunction. In August 2025, both parties dropped their appeals without obtaining those modifications, leaving the $125 million civil penalty and the injunction in place and formally closing the case.[1899]

Continued

1892 For the current version of the *Howey* framework for cryptocurrencies, see U.S. Sec. & Exch. Comm'n, *Framework for "Investment Contract" Analysis of Digital Assets*, https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets (last visited Jan. 15, 2026).

1893 *U.S. Sec. & Exch. Comm'n v. Ripple Labs*, Inc., 682 F. Supp. 3d 308, 324-30 (S.D.N.Y. 2023) [hereinafter *SEC* v. *Ripple Labs*].

1894 *See SEC* v. *Ripple Labs*, *motion to certify appeal denied*, 697 F. Supp. 3d 126 (S.D.N.Y. 2023) [hereinafter July 13, 2023 Ripple Order]. Institutional sales were essentially direct sales of XRP by Ripple to institutional buyers. Programmatic sales were indirect sales of XRP by Ripple to the general public via public digital-asset exchanges.

1895 *See* July 13, 2023 Ripple Order, *supra* note 1894, at 324-28. *See also* Jack Barber et al., *SEC v. Ripple: A Tale of Two Token Transaction Types*, FinTech and Digit. Assets Blog (July 2023), https://www.fintechanddigitalassets.com/2023/07/sec-v-ripple-a-tale-of-two-token-transaction-types/; Rachael Hashmall et al., *U.S. Federal Court Issues Mixed Ruling in Watershed SEC Action on Ripple's XRP*, Norton Rose Fulbright (July 2023), https://www.nortonrosefulbright.com/en-us/knowledge/publications/74133d3b/us-federal-court-issues-mixed-ruling-in-watershed-sec-action-on-ripples-xrp.

1896 *See* July 13, 2023 Ripple Order, *supra* note 1894, at 328-30.

1897 Joseph A. Castelluccio, Anna T. Pinedo & Steffen Hemmerich, *Defining Digital Asset Securities: US District Court Issues Summary Judgment Rulings In SEC v. Ripple Labs*, MAYER BROWN (July 24, 2023), https://www.mayerbrown.com/en/insights/publications/2023/07/defining-digital-asset-securities-us-district-court-issues-summary-judgment-rulings-in-sec-v-ripple-labs

1898 Michael W. Fakhoury et al., *Securities Enforcement Roundup – August 2024*, Morgan Lewis (Sept. 6, 2024), https://www.morganlewis.com/pubs/2024/09/securities-enforcement-roundup-august-2024.

1899 U.S. Sec. And Exc. Comm., Ripple Labs, Inc., Bradley Garlinghouse, & Christian A. Larsen, Litigation Release No. 26306, No. 1:20-cv-10832 (May 8, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26306; U.S. Sec. And Exc. Comm., Ripple Labs, Inc., Bradley Garlinghouse, & Christian A. Larsen, Litigation Release No. 26369, No. 1:20-cv-10832 (Aug. 7, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26369.

FIGURE 55. (continued)

Applying the *Howey* Test to Crypto (continued)

In the second case, *SEC v. Terraform Labs Pte. Ltd.*,[1900] a different judge in the same federal district court rejected a distinction between institutional and retail buyers in programmatic sales. Ruling on a motion to dismiss in July 2023, the judge held that retail purchasers could still form a reasonable expectation of profits based on the issuer's promotional efforts and ecosystem design, even in anonymous secondary market transactions.[1901] On subsequent summary judgment in December 2023, the court held that the defendant's tokens —LUNA, UST, and MIR— were securities because Terraform's active promotion and development efforts created a reasonable expectation of profits for all buyers, regardless of whether they purchased the tokens directly or via exchanges.[1902]

Both judges applied the *Howey* test; however, the *Ripple* court distinguished between the types of buyers and how the tokens were sold, while the *Terraform* court focused on the issuer's public representations and the overall scheme.[1903] The two decisions were also issued at different procedural postures. This split within one federal court district highlights the continued legal uncertainty in this area. While this uncertainty may justify the SEC's application of traditional securities regulation to cryptocurrencies, critics contend that this approach is too inflexible and punitive for novel, fast-moving technology.[1904]

7.2.2.B. The CFTC: Crypto-assets as Commodities

Citing the U.S. 1936 Commodity Exchange Act (CEA), the Commodity Futures Trading Commission (CFTC) has asserted jurisdiction over cryptocurrencies by classifying them as commodities —particularly in the context of derivatives regulation. In a seminal September 17, 2015, order, the CFTC affirmed that Bitcoin and other virtual currencies properly qualify as commodities, especially within the context of the derivatives market.[1905] Since then, the CFTC has stressed its intent to combat fraud and manipulation in digital-asset markets,[1906] applying the CEA to platforms that involve token-based derivatives or provide advisory services concerning token-based derivatives. Such platforms must register with the CFTC and are subject to regulation by the CFTC and/or the National Futures Association.[1907]

1900 *Sec. & Exch. Comm'n v. Terraform Labs Pte. Ltd.*, 684 F. Supp. 3d 170, 196-201 (S.D.N.Y. 2023) [hereinafter *SEC v. Terraform Labs.*]

1901 *See* Michael D. Birnbaum et al., *SEC v. Terraform Labs Pte. Ltd.: SDNY Judge Rakoff Denies Defendants' Motion to Dismiss SEC's Claims, Rejects the Ripple Court's Interpretation of the Howey Test*, Morrison Foerster LLP (Aug. 4, 2023), https://www.mofo.com/resources/insights/230803-sec-v-terraform-labs-pte-ltd-sdny-judge-rakoff.

1902 *SEC* v. *Terraform Labs*, *supra* note 1900, at 196-201.

1903 *Id.* at 197-98. Later, the court in *Ripple* also distinguished *Terraform* because that case was in a different procedural stage—motion to dismiss—where the SEC's allegations were taken as true, while *Ripple* decided on a full factual record that buyers in Ripple's programmatic sales had no reason to expect profits from Ripple's efforts. *See* U.S. Sec. & Exch. Comm'n v. Ripple Labs, Inc., 697 F. Supp. 3d 126, 135-37 (S.D.N.Y. 2023).

1904 *See* Akshay S. Ralhi, *Beyond Enforcement: The SEC's Shifting Playbook on Crypto Regulation*, Geo. L. Ctr. on Transnat'l Bus. & the L. (May 9, 2025), https://www.law.georgetown.edu/ctbl/blog/beyond-enforcement-the-secs-shifting-playbook-on-crypto-regulation; *see also Understanding the Howey Test for Digital Assets and Securities*, Merkle Science, (Sept. 9, 2024), https://www.merklescience.com/blog/understanding-the-howey-test-for-digital-assets-and-securities. Critics argue that the Howey Test, formulated in 1946 for a citrus grove investment scheme, is fundamentally ill-suited for decentralized blockchain networks where no central entity controls operations and profits may derive from network effects rather than managerial efforts.

1905 Press Release, U.S. Commodity Futures Trading Comm'n , *CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering* (Sept. 17, 2015), https://www.cftc.gov/PressRoom/PressReleases/7231-15.

1906 *See, e.g.*, Div. of Enf't, U.S. Commodity Futures Trading Comm'n, 2018 *Annual Report* 2 (2018), https://www.cftc.gov/sites/default/files/2018-11/ENFAnnualReport111418_0.pdf ("the [CFTC's Division of Enforcement] aggressively prosecuted fraud in . . . traditional areas, like precious metals, forex, and binary options. But the last Fiscal Year also saw some fraudsters evolve, as they sought to use new products or new technologies to target unsuspecting customers in markets like virtual currencies. We have worked hard to ensure that we are evolving with the bad actors—and indeed, staying one step ahead.").

1907 *See, e.g.*, In re Matter of Coinflip, Inc., CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). *See also* U.S. Commodity Futures Trading Comm'n, *Be Smart: Check Registration & Backgrounds Before You Trade*, , https://www.cftc.gov/check (last visited Jan. 15, 2026) (guidance on how to confirm a business is a registered trader in commodities).

Judicial precedent reinforces this jurisdictional framework. In *CFTC v. McDonnell*, the U.S. District Court for the Eastern District of New York held that virtual currencies are commodities subject to regulation —even when the SEC may also have jurisdiction. The court found Coin Drop Markets guilty of operating a deceptive virtual currency scheme that misappropriated investor funds.[1908] Likewise, in *CFTC v. My Big Coin Pay, Inc.,* the court held, at the motion to dismiss stage, that virtual currencies may qualify as commodities. The CFTC later obtained a final default judgment on June 5, 2025 which included findings of fraud and misappropriation of "virtually all the money solicited from customers" in connection with a purportedly fully functioning virtual currency called "My Big Coin." [1909] The action reinforced the CFTC's authority to combat fraud in spot markets without requiring evidence of broader market manipulation linked to futures contracts.

In fiscal year 2024, the CFTC brought 58 new enforcement actions, targeting unregistered trading platforms, fraudulent schemes, and novel misconduct in both traditional and decentralized markets.[1910] These included charges against Uniswap Labs, which resulted in a civil penalty of $175,000 and a cease-and-desist order for offering illegal leveraged or margined digital-asset transactions via DeFi. They also included charges against Falcon Labs, targeted in the agency's first action against an unregistered futures commission merchant with over $1.7 million in sanctions; and, KuCoin, charged for dealing in off-exchange digital-asset futures and swap transactions without registration and for supervisory failures.[1911]

7.2.3. Regulation by Prosecution: The DOJ Approach

Numerous criminal prosecutions exemplify the enforcement-driven approach referred to as "regulation by prosecution."[1912] Significant judicial rulings in these cases reflect efforts by courts and regulators to provide greater clarity in an otherwise uncertain legal landscape *(See section 6.2)*. While these decisions do not eliminate all ambiguities, they have established important precedents in the United States.

Federal prosecutors have targeted criminal uses of cryptocurrency mixing (See, for example, *section 6.5.3.* on Tornado Cash). In April 2024, the Department of Justice indicted the co-founders of Samourai Wallet on charges of conspiracy to commit money laundering and conspiracy to operate an unlicensed money-transmitting business. The indictment alleged that Samourai's mixing services facilitated the laundering of more than $100 million in criminal proceeds and processed over $2 billion in total transactions, linked to criminal activities such as dark web markets; various computer-fraud schemes, like spear phishing; and hacks and other cybercrimes. Prosecutors further contended that the co-founders knowingly engineered and promoted the software while being aware that it was being used to conceal the source of illicit funds, notably because the trail of transactions is obfuscated by routing transfers through intermediary wallets.[1913]

1908 *Commodity Futures Trading Comm'n v. McDonnell*, 332 F. Supp. 3d 641, 717-25 (E.D.N.Y. 2018).

1909 *See Commodity Futures Trading Comm'n v. My Big Coin Pay*, Inc., No. 18-CV-10077-DJC, 2025 WL 2202196, at 2–7 (D. Mass. June 5, 2025); Press Release, U.S. Commodity Futures Trading Comm'n, Federal Court Orders Michigan Man, California Man, and Two Nevada Companies to Pay Over $25 Million for Digital Asset Fraud (June 11, 2025), https://www.cftc.gov/PressRoom/PressReleases/9084-25.

1910 *2024 CFTC Enforcement: Agency Celebrates Record Monetary Relief*, BCLP (Dec. 6, 2024), https://www.bclplaw.com/en-US/events-insights-news/2024-cftc-enforcement-agency-celebrates-record-monetary-relief.html; James Field, *CFTC Records $17B Monetary Relief in 2024, Thanks to Digital Assets*, CoinGeek (Dec. 9, 2024), https://coingeek.com/cftc-records-17b-monetary-relief-in-2024-thanks-to-digital-assets/.

1911 *2024 CFTC Enforcement: Agency Celebrates Record Monetary Relief*, *supra* note 1910.

1912 The term "regulation by prosecution" or "regulation by prosecutor" has been used in both academic and government contexts. *See, e.g.*, Gregory M. Gilchrist, *Regulation by Prosecutor*, 56 Am. Crim. L. Rev. 315 (2019), https://www.law.georgetown.edu/american-criminal-law-review/wp-content/uploads/sites/15/2019/04/56-2-Regulation-by-Prosecutor.pdf; Todd Blanche, Deputy Att'y Gen., *Memorandum: Ending Regulation by Prosecution* (Apr. 7, 2025) https://www.justice.gov/dag/media/1395781/dl?inline [hereinafter Blanche Memo].

1913 Press Release, U.S. Att'y's Off., S.D.N.Y., *Founders and CEO of Cryptocurrency Mixing Service Arrested and Charged with Money Laundering* (Apr. 24, 2024), https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering.

However, many in the crypto industry have argued that the prosecution is difficult to reconcile with prior regulatory guidance by the Financial Crimes Enforcement Network (FinCEN). Filings by industry groups, such as the DeFi Education Fund and Blockchain Association, as well as the defense counsel have pointed to FinCEN's 2019 guidance, suggesting that non-custodial wallet software, standing alone, does not constitute a money services business and therefore is not subject to registration or AML obligations.[1914] Critics argued that, if FinCEN's own guidance suggests that such services are not money transmitters, then it was an incorrect application of the law to prosecute developers for "unlicensed money transmission." At the same time, however, the same FinCEN guidance also states that operators of anonymizing services—commonly understood to include cryptocurrency mixers—may qualify as money transmitters and thus fall within the scope of MSB regulation. The dispute therefore turns on how the activity is characterized: as the provision of software, or as the operation of a service facilitating the transfer and obfuscation of funds. For example, Coin Center, a crypto research and advocacy center, called the legal theory behind these cases "a massive overreach." It warned that, under this interpretation, "every functioning cryptocurrency wallet and smart contract" would be a money transmitter and, by extension, every developer would be an unlicensed transmitter.[1915]

In April 2025, the parties filed a joint status report indicating that they were discussing whether the case should proceed in light of the Justice Department's new policies on prosecutions involving digital assets, but no agreement was reached.[1916] In May 2025, the defendants moved to dismiss the indictment, citing FinCEN's guidance, with multiple crypto-industry groups expressing interest in filing amicus briefs making the same point.[1917] Ultimately, the case did not go to trial because both founders of Samourai Wallet pleaded guilty in July 2025 to operating an unlicensed money-transmitting business.[1918] The court sentenced one of the defendants to five years in prison and the other to four years in prison.[1919] Because the case ended with guilty pleas, the court did not resolve the broader question of how FinCEN's guidance applies to non-custodial wallets and cryptocurrency mixers, leaving that legal issue unsettled.

7.2.4. The Trump Administration's Policy Shift

With the change in U.S. presidential administrations in January 2025, the U.S. digital asset policy underwent a fundamental transformation. The second Trump administration began to move away from an enforcement-focused approach, shifting toward a strategy emphasizing forward-looking guidance, agency restructuring, and comprehensive federal legislation.

1914 *See* Letter from Defense Counsel to Judge Richard M. Berman, *United States v. Rodriguez*, No. 1:24-cr-00082-RMB (S.D.N.Y. May 5, 2025), ECF No. 86, https://bitcoinmagazine.com/wp-content/uploads/2025/05/https_dechert_my_sharepoint_com_personal_cflannery_dechert_com_Documents-1.pdf; Brief for DeFi Education Fund as Amici Curiae Supporting Defendants' Motion to Dismiss, *United States v. Rodriguez*, No. 1:24-cr-00082-RMB (S.D.N.Y. June 6, 2025), https://www.defieducationfund.org/docs/legal/litigation-contributions/defs-amicus-brief-in-u-s-v-rodriguez-and-hill/; *see also* Zack Cohen, Bitcoin Pol'y Inst., *The DOJ's Dangerous New Legal Theory* 1-2 (2024), https://cdn.prod.website-files.com/627aa615676bdd1d47ec97d4/67605a80af939bd2f92954b1_Samourai.pdf ("By implicating Samourai Wallet, the DOJ's case aims to expand the scope of money transmitter laws to include tools that simply facilitate peer-to-peer transactions. This would be analogous to regulating safe manufacturers as if they were banks.").

1915 Peter Van Valkenburgh, *DOJ's New Stance on Crypto Wallets is a Threat to Liberty and the Rule of Law*, Coin Ctr. (Apr. 29, 2024), https://www.coincenter.org/dojs-new-stance-on-crypto-wallets-is-a-threat-to-liberty-and-the-rule-of-law/.

1916 Joint Request at 1, *U.S. v. Rodriguez*, No. 1:24-cr-00082-RMB (Apr. 28, 2025), ECF No. 84.

1917 Memorandum of Law in Support of Defendants' Motion to Dismiss Indictment at 10, *U.S. v. Rodriguez*, No. 1:24-cr-00082-RMB (Apr. 28, 2025), ECF No. 95; Francisco Rodrigues, *Samourai Wallet Files to Dismiss DOJ Case, Citing FinCEN Guidance*, CoinDesk (May 30, 2025), https://finance.yahoo.com/news/samourai-wallet-files-dismiss-doj-084419326.html (summarizing the case).

1918 Press Release, U.S. Att'y's Off. S.D.N.Y., *Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty* (Aug. 6, 2025), https://www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty.

1919 Additionally, both defendants were sentenced to three years of supervised release, ordered to pay individual fines of $250,000, and required to forfeit approximately $237 million in criminal proceeds. Press Release, U.S. Att'y's Off. S.D.N.Y, *Founders Of Samourai Wallet Cryptocurrency Mixing Service Sentenced To Five And Four Years In Prison* (Nov. 19, 2025), https://www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-sentenced-five-and-four-years.

7.2.4.A. Critiques of "Regulation by Enforcement"

The reliance on enforcement as a regulatory tool has generated significant criticism. Because legal standards emerge only from individual cases, firms must extrapolate compliance obligations from enforcement actions against individual companies, many of which are very fact-specific.[1920] This dynamic creates legal uncertainty, stifles innovation, and fosters an unpredictable business environment. SEC Commissioner Hester Peirce warned that regulation by enforcement "allowed legal uncertainty to fester to the point that it is now 'a major deterrent to operating in the digital assets space in the United States.'"[1921] Under the current Trump administration, U.S. regulators have significantly recalibrated their reliance on a "regulation by enforcement" strategy in the domain of blockchain and cryptocurrencies, maintaining enforcement in cases involving fraud and market abuse while seeking to reduce its role as a primary tool of policy formation.

The advantages and disadvantages of "regulation by enforcement" have been thoroughly discussed by scholars. Most generally agree that it is within regulators' discretion to choose how to make policy and that doing so through litigation and enforcement allows for faster response to novel regulatory challenges. But scholars also note that this policy-making approach can be unfair and selective, politically motivated and undemocratic, or at least unpredictable and inconsistent.[1922] As for the latter, the above-mentioned examples of enforcement actions by U.S. government agencies demonstrate that the "regulation by enforcement" approach amplifies the inconvenience of institutional fragmentation across different regulatory regimes. The CFTC designates crypto-assets as commodities, the IRS treats them as property for tax purposes, and the SEC frequently characterizes them as securities under the *Howey* test. These differing classifications add to the legal uncertainty surrounding digital assets, especially questions regarding their status (what they are) and the applicable regime (which rules apply to transfers, ownership, bankruptcy, or theft recovery).[1923]

Within this context, President Biden in March 2022 signed Executive Order 14067 to impose a whole-of-government approach by directing coordinated reports from agencies,[1924] including the Department of Treasury (consumer protection and AML/CFT),[1925] the Department of Justice (law enforcement),[1926] and the Department of Commerce (competitiveness).[1927] However, enforcement authority was divided among the SEC, the CFTC, and

---

1920 Enforcement actions against Ripple are discussed in *infra* section 7.2.1.

1921 Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, Hobs and Hobbes: Wharton FinTech Lecture (Nov. 1, 2024) (quoting Jennifer J. Schulp, *Dazed and Confused: Breaking Down the SEC's Politicized Approach to Digital Assets*, Cato Inst. (Sept. 17, 2024), https://www.cato.org/testimony/dazed-confused-breaking-down-secs-politicized-approach-digital-assets#secs-jurisdiction-unclear).

1922 *See, e.g.*, Chris Brummer, Yesha Yadav & David Zaring, *Regulation by Enforcement*, 96 S. Cal. L. Rev. 1297 (2024), https://ssrn.com/abstract=4405036; Carol R. Goforth, *Critiquing the SEC's Ongoing Efforts to Regulate Crypto Exchanges*, 14 Wm. & Mary Bus. L. Rev. 305 (2023), https://scholarship.law.wm.edu/wmblr/vol14/iss2/3/; James J. Park & Howard H. Park, *Regulation by Selective Enforcement: The SEC and Initial Coin Offerings*, 61 Wash. U. J.L. & Pol'y 99 (2020), https://openscholarship.wustl.edu/law_journal_law_policy/vol61/iss1/11/.

1923 One of the fundamental questions regarding crypto-assets is the "Property Question"—whether (and how) established property rules apply to them. *See* Andrea Tosato & Christopher K. Odinet, *Digital Assets and the Property Question*, 78 Fla. L. Rev. (forthcoming 2026), https://ssrn.com/abstract=5151907.

1924 Exec. Order No. 14,067, 87 Fed. Reg. 14,143 (Mar. 9, 2022), https://www.govinfo.gov/app/details/FR-2022-03-14/2022-05471. *See also Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, White House (Sept. 16, 2022), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

1925 U.S. Dept. of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Sept. 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf

1926 The Department of Justice's September 2022 report advocated for significantly expanded powers to investigate and prosecute digital asset offenses. U.S. Dep't of Just., *The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* (Sept. 2022), https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf.

1927 U.S. Dep't of Com., *Responsible Advancement of U.S. Competitiveness in Digital Assets* (Sept. 2022), https://www.commerce.gov/sites/default/files/2022-09/Digital-Asset-Competitiveness-Report.pdf.

FinCEN, with each applying distinct statutory mandates to overlapping aspects of the digital-asset ecosystem.[1928]

This fragmented approach prompted calls —including from the chairman of the CFTC— for the designation of a single federal regulator to oversee digital assets.[1929] In 2024, CFTC Commissioner Summer K. Mersinger argued that relying on enforcement actions, rather than establishing clear, forward-looking rules, creates significant uncertainty for market participants. She said the Commodity Exchange Act and existing CFTC regulations, originally designed for centralized markets, fall short in addressing the unique challenges of decentralized finance and digital assets.[1930] Mersinger criticized this method as inconsistent with the agency's goal of fostering responsible innovation and market resilience, and she called for formal rulemaking to replace what she viewed as a temporary, "band-aid" solution.

7.2.4.B. Reassessment of "Regulation by Enforcement"

At the outset of his second term, President Trump issued an executive order entitled *Strengthening American Leadership in Digital Financial Technology*.[1931] The executive order represented the beginning of significant change in U.S. policy on digital assets and blockchain. President Trump's order revoked President Biden's digital asset Executive Order 14067 and the Treasury Department's July 2022 Framework for International Engagement on Digital Assets.[1932] Specifically, Trump's executive order directed federal agencies to protect and promote the ability to access and use open public blockchain networks "without persecution, including the ability to develop and deploy software, to participate in mining and validating, to transact with other persons without unlawful censorship, and to maintain self-custody of digital assets."[1933] It also directed the administration to

> provid[e] regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries, all of which are essential to supporting a vibrant and inclusive digital economy and innovation in digital assets, permissionless blockchains, and distributed ledger technologies.[1934]

President Trump's executive order also created a President's Working Group on Digital Asset Markets, comprising senior leaders of government. The order tasked the Working Group with recommending regulatory and legislative proposals that herald a new era in blockchain law and policy.[1935]

1. New SEC Policy

In connection with the change in administrations and a new executive order, the SEC launched a "Crypto Task

1928 But see an earlier attempt by the three agencies to coordinate their position on anti-money laundering and countering the financing of terrorism obligations for digital asset activities under the Bank Secrecy Act. Heath Tarbert, Chairman, U.S. Commodity Futures Trading Comm'n , Kenneth A. Blanco, Dir., Fin. Crimes Enf't Network, & Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* (Oct. 11, 2019), https://www.sec.gov/newsroom/speeches-statements/cftc-fincen-sec-jointstatementdigitalassets.

1929 Elizabeth Caires & Eric Forni, *Digital Assets Regulation in 2023: Is a New Regulatory Framework Needed?*, DLA Piper (Feb. 2, 2023), https://www.dlapiper.com/en/insights/publications/2023/01/the-cftc-and-a-congressional-framework-for-regulation-of-digital-assets; Rostin Behnam, Chairman, U.S. Commodity Futures Trading Comm'n, *Testimony Before the U.S. House Committee on Agriculture on The Future of Digital Assets: Providing Clarity for Digital Asset Spot Markets* (June 6, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam36.

1930 Summer K. Mersinger, Comm'r, U.S. Commodity Futures Trading Comm'n, *Dissenting Statement of Commissioner Summer K. Mersinger Regarding Settlement with Uniswap Labs* (Sept. 4, 2024), https://www.cftc.gov/PressRoom/SpeechesTestimony/mersingerstatement090424.

1931 Exec. Order No. 14102, *Strengthening American Leadership in Digital Financial Technology*, 90 Fed. Reg. 4567 (Jan. 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

1932 *Id.* § 3.

1933 *Id.* § 1.

1934 *Id.* § 1.

1935 *Id.* § 4.

Force" to clarify the application of securities laws to digital assets, encourage innovation, and protect investors.[1936] Its mandate emphasized guidance and collaboration with industry, rather than reliance on enforcement actions.[1937] On February 27, 2025, the SEC's Division of Corporation Finance issued a statement providing guidance that certain "meme coins" do not constitute securities under federal law, marking a departure from the previous administration's enforcement-focused approach.[1938] SEC Commissioner Hester Peirce, a Trump appointee during his first term, was tasked with developing a new regulatory framework for crypto-assets.[1939] She advised that the *Howey* test was too complex and applied too inconsistently to provide reliable guidance for digital assets.[1940]

More importantly, the SEC dismissed several high profile lawsuits that had been filed by the Biden administration against leading crypto firms.[1941] Verified dismissals include the SEC's civil enforcement action against Kraken (dismissed with prejudice on March 27, 2025).[1942] The SEC also filed a settlement agreement in *SEC v. Ripple* on May 8, 2025, proposing a framework that contemplated dismissal of the parties' appeals after further district-court proceedings.[1943] Subsequent proceedings later resulted in the parties dropping their appeals and the case ending.[1944] Separately, the SEC dismissed with prejudice its civil enforcement action against Coinbase (Feb. 27, 2025),[1945] Consensys (Mar. 27, 2025),[1946] and Binance (May 29, 2025).[1947] In the case of Robinhood, the SEC closed its investigation into Robinhood Crypto without enforcement action (announced Feb. 24, 2025).[1948]

2. New CFTC Policy

In April 2025, Acting Chair of the Commodity Futures Trading Commission (CFTC), Caroline Pham, announced a policy shift parallel with that of the SEC. She directed agency staff to move away from enforcement-led regulation and toward clearer regulatory guidance, while concentrating enforcement resources on core priorities, such as fraud and market manipulation.[1949] As part of this shift, Pham instructed staff not to pursue violations of licensing or registration requirements under the Commodity Exchange Act, "unless 'there is evidence that the defendant knew of the licensing or registration requirement at issue and violated such a

1936 *Crypto Task Force*, U.S. Sec. & Exch. Comm'n, https://www.sec.gov/about/crypto-task-force (last visited Jan. 15, 2026).

1937 Debevoise & Plimpton LLP, *Crypto Assets Under the Trump Administration* 12-13 (Feb. 2025), https://www.debevoise.com/-/media/files/insights/publications/2025/02/crypto-assets-under-the-trump-administration.pdf.

1938 Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n, *Staff Statement on Meme Coins* (Feb. 27, 2025), https://www.sec.gov/newsroom/speeches-statements/staff-statement-meme-coins.

1939 Ralhi, *supra* note 1904.

1940 Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, *There Must Be Some Way Out of Here* (Feb. 21, 2025), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125.

1941 Prashant Jha, *SEC Crypto Reversals: Every Case It Dropped in 2025 and the Legal Battles Still Ahead*, CCN (May 30, 2025), https://www.ccn.com/news/crypto/sec-crypto-reversals-2025-lawsuits/ (summarizing the status of most high-profile court cases against actors in the crypto industry).

1942 U.S. Sec. & Exch. Comm'n, Litigation Release No. LR-26278, Payward, Inc. and Payward Ventures, Inc. (d/b/a "Kraken") (Mar. 27, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26278.

1943 U.S. Sec. & Exch. Comm'n, Litigation Release No. LR-26306, Ripple Labs, Inc., Bradley Garlinghouse, and Christian Larsen (May 8, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26306

1944 Jonathan Stempel, *SEC Ends Lawsuit Against Ripple; Company to Pay $125 Million Fine*, Reuters (Aug. 8, 2025), https://www.reuters.com/legal/government/sec-ends-lawsuit-against-ripple-company-pay-125-million-fine-2025-08-08/.

1945 Press Release, U.S. Sec. & Exch. Comm'n, *SEC Announces Dismissal of Civil Enforcement Action Against Coinbase* (Feb. 27, 2025), https://www.sec.gov/newsroom/press-releases/2025-47

1946 Sec. & Exch. Comm'n, Litigation Release No. LR-26277, Consensys Software Inc. (Mar. 27, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26277.

1947 Jonathan Stempel, *US SEC Voluntarily Dismisses Lawsuit Against Binance*, Reuters (May 30, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/us-sec-voluntarily-dismisses-lawsuit-against-binance-2025-05-29/.

1948 Jaiveer Shekhawat, *US SEC Closes Investigation into Robinhood with No Action*, Reuters (Feb. 24, 2025), https://www.reuters.com/legal/us-sec-closes-investigation-into-robinhood-with-no-action-2025-02-24/

1949 Press Release, U.S. Commodity Futures Trading Comm'n, *Acting Chairman Pham Lauds DOJ Policy Ending Regulation by Prosecution of Digital Assets Industry and Directs CFTC Staff to Comply with Executive Orders* (Apr. 8, 2025), https://www.cftc.gov/PressRoom/PressReleases/9063-25.

requirement willfully.'"[1950] This recalibration was followed in September 2025 by a joint staff statement issued by the SEC and the CFTC, signaling a coordinated effort to promote regulatory clarity and support blockchain-based innovation within the United States. The statement expressed the view that "current law does not prohibit SEC- or CFTC-registered exchanges from facilitating trading of these spot crypto asset products."[1951]

7.2.4.C. Ending "Regulation by Prosecution": the Blanche Memo

The Department of Justice (DOJ) under President Trump's second term made its own changes. First, it dismantled the National Cryptocurrency Enforcement Team (NCET), formed under President Biden. Deputy Attorney General Todd Blanche issued a formal memorandum, *Ending Regulation By Prosecution*, known colloquially as the "Blanche Memo."[1952] The memo declared that the DOJ "is not a digital assets regulator" and that it would "no longer pursue litigation or enforcement actions that have the effect of superimposing regulatory frameworks on digital assets."[1953] It also directed prosecutors to close ongoing investigations inconsistent with this policy.[1954] It instructed them instead to avoid charging exchanges, mixers, and wallet providers for regulatory violations absent proof of willful intent.[1955]

Under the new framework, the DOJ is to prioritize prosecutions of entities that directly harm investors through fraud, embezzlement, scams, hacking, and rug pulls. The department is also to prioritize prosecutions of those who use digital assets for clearly defined criminal purposes, including terrorism financing, narcotics trafficking, and organized crime. Critically, the memorandum stipulated that prosecutors should not charge regulatory violations —such as unlicensed money transmitting or violations of the Bank Secrecy Act— unless there is evidence the defendant knew of the requirement and acted willfully.[1956]

7.2.4.D. New Federal Statutes

On July 30, 2025, the White House released a detailed report under the auspices of the President's Working Group on Digital Asset Markets.[1957] The report set out a comprehensive agenda for digital assets, including blockchain, stablecoins, tokenization, and related financial-technology infrastructure. It emphasized that the U.S. government should adopt a "pro-innovation mindset" toward crypto-assets and blockchain technologies, while addressing risks (such as illicit finance, national security, and investor protection). Among its recommendations, the report urged the SEC and the CFTC to exercise their existing authorities to provide regulatory clarity and facilitate the development of a federal framework for digital asset trading. The report also urged Congress to enact a comprehensive framework that clarifies regulatory jurisdiction; establishes fit-for-purpose requirements for registration, custody, trading, and tailored disclosure; and addresses other gaps in the current legal regime.

1950 *Id.* (quoting BLANCHE MEMO, *supra* note 1912, at 3).

1951 U.S. SEC AND EXC. COMM., Staff of SEC & CFTC, *SEC-CFTC Joint Staff Statement* (Project Crypto-Crypto Sprint) (Sept. 2, 2025), https://www.sec.gov/newsroom/speeches-statements/sec-cftc-project-crypto-090225. In this context, "spot" denotes cash-market trading in the underlying crypto-assets with immediate or near-immediate settlement, rather than futures, options, or other derivatives.

1952 BLANCHE MEMO, *supra* note 1912, at 3.

1953 *Id.* at 1.

1954 *Id.* at 2.

1955 *Id.* at 2-3.

1956 *Id.* Part II.

1957 WHITE HOUSE, *President's Working Grp. on Digit. Assets, Strengthening American Leadership in Digital Financial Technology* (2025), https://www.whitehouse.gov/crypto/. *See also* Hannah Lang, *White House in Crypto Policy Report Calls for SEC Action, New Legislation*, REUTERS (July 30, 2025), https://www.reuters.com/legal/government/white-house-crypto-policy-report-calls-sec-action-new-legislation-2025-07-30/.

1. The GENIUS Act

In July 2025, President Trump signed into law the Guiding and Establishing National Innovation for U.S. Stablecoins Act (aka GENIUS Act), creating a federal framework for stablecoins.[1958] The GENIUS Act established a comprehensive federal framework for the issuance and oversight of "payment stablecoins." A payment stablecoin is defined as a digital asset designed for use as a means of payment or settlement.[1959] The Act makes it generally unlawful for any person other than a permitted issuer to issue a payment stablecoin in the United States. In addition, digital asset service providers are prohibited from offering or selling payment stablecoins to U.S. persons unless the stablecoin is issued by a permitted issuer or falls within one of the statutory or regulatory safe harbors. The Act creates both federal and state pathways through which an entity may obtain authorization as a "permitted payment stablecoin issuer."

The Act directs federal and state regulators —including the Federal Reserve Board, the Office of the Comptroller of the Currency (OCC), the National Credit Union Administration (NCUA), and state payment-stablecoin supervisory agencies— to issue implementing rules governing capital, liquidity, and risk-management standards for permitted issuers.[1960] Under this framework, subsidiaries of insured depository institutions issuing payment stablecoins are supervised by their existing primary federal banking regulator — whether the OCC, the FDIC, the Federal Reserve, or the NCUA — while nonbank entities, uninsured national banks, and federal branches of foreign banks obtaining a federal license to issue payment stablecoins are supervised by the OCC. The Act also imposes strict reserve requirements to ensure full and timely redemption of outstanding payment stablecoins.

2. The CLARITY Act

Despite the adoption of the GENIUS Act, significant uncertainty remains. The bipartisan Digital Asset Market Clarity Act (CLARITY Act), which passed the House on July 17, 2025, seeks to establish a comprehensive statutory framework to allocate regulatory authority between the SEC and the CFTC and clarify the legal classification of digital assets.

The bill introduces a functional and status-based approach that distinguishes between different categories of digital assets and market participants. In particular, it introduces a certification regime for "mature blockchain systems." Where a blockchain is certified as "mature," certain tokens issued or transacted on that system may benefit from exemptions from SEC registration requirements. For systems that are not yet "mature," enhanced disclosure and reporting obligations would apply.[1961] The bill preserves the SEC's authority over investment contract assets and related intermediaries, while granting the CFTC "exclusive jurisdiction" over "digital commodity" spot markets and registered digital commodity exchanges and brokers. It would establish a registration regime for digital commodity exchanges, brokers, and dealers under the jurisdiction of the CFTC. The bill also provides for coordination mechanisms between the SEC and CFTC, including rulemaking authority to address hybrid or mixed transactions involving both digital commodities and securities, with the objective of avoiding duplicative or conflicting regulatory obligations across agencies.[1962]

1958 *See generally Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025* (GENIUS Act), Pub. L. No. 119-27, 139 Stat. 419 (2025), https://www.congress.gov/119/plaws/publ27/PLAW-119publ27.pdf.

1959 Payment stablecoins are digital assets that are, or are designed to be, "used as a means of payment or settlement . . . and the issuer of which . . . is obligated to convert, redeem, or repurchase for a fixed amount of monetary value . . . and represents that such issuer will maintain, or create the reasonable expectation that it will maintain, a stable value relative to the value of a fixed amount of monetary value." Stablecoins are neither national currencies, deposits, nor securities issued by an investment company. *Id.* at 421-22.

1960 On September 18, 2025, the U.S. Department of the Treasury began seeking public comments related to its implementation of the GENIUS Act, including the new framework that it proposed called Innovative Methods to Detect Illicit Activity Involving Digital Assets. Press Release, U.S. Dep't of Treasury, *Treasury Seeks Public Comment on Implementation of the GENIUS Act* (Sept. 18, 2025), https://home.treasury.gov/news/press-releases/sb0254.

1961 *See generally Digital Asset Market Clarity Act of 2025*, H.R. 3633, 119th Congress (2025), https://www.congress.gov/bill/119th-congress/house-bill/3633.

1962 *Id*., at § 502-03. *See also* Zachary Goldman et al., *Congress Set to Bring CLARITY to Digital Asset Market Structure*, WilmerHale (July 14, 2025), https://www.wilmerhale.com/en/insights/client-alerts/20250714-congress-set-to-bring-clarity-to-digital-asset-market-structure, for a summary of the main changes of the Act.

As the bill moved to the Senate, it underwent significant modification. The Senate Banking Committee released multiple discussion drafts throughout the second half of 2025, including a comprehensive 278 page draft on January 12, 2026.[1963] The Senate Agriculture Committee, which has jurisdiction over the CFTC-related provisions, released its own discussion draft in November 2025.[1964] These Senate versions introduced several controversial provisions that were not in the House-passed bill.

Most notably, the Senate Banking Committee draft prohibited digital asset service providers from offering passive interest or yield solely for holding stablecoin balances, though it allowed activity-based rewards tied to transactions, staking, liquidity provision, or other ecosystem participation.[1965] This stablecoin yield restriction, inserted after lobbying by the banking industry, sparked fierce opposition from major crypto firms, with Coinbase publicly withdrawing its support for the bill on January 14, 2026.[1966]

There are other critics of the CLARITY Act,[1967] including critics in the Senate who have argued that, despite regulatory clarity, this legislation weakens investor protection under longstanding securities laws. They also expressed concern that the Act opens the door for certain activity involving tokens to evade oversight, that it sets ambiguous criteria for decentralization, and that it fails to address money-laundering and sanctions risks.[1968] The CLARITY Act's fate remains uncertain. Although the bill passed the House in July 2025, the legislation faces significant obstacles including lack of bipartisan support and is still under review as of January 2026. It may undergo substantial revision before any potential enactment.

The policy shift underway in the United States introduces a significant new variable into the global regulatory landscape. By moving away from enforcement-driven oversight toward legislative clarity and institutional embrace of the crypto industry, the United States is repositioning itself as a more innovation-friendly jurisdiction —a development that is already reshaping the dynamics of international regulatory competition

7.3. PROACTIVE LEGISLATIVE FRAMEWORKS

Blockchain technology gives rise to new economic and social realities, along with unprecedented legal challenges. Applying traditional legal categories to innovations such as crypto-assets, smart contracts, and decentralized autonomous organizations (DAOs) remains difficult. The gradual emergence of judicial and administrative precedents sufficient to establish legal

1963 S. Comm. on Banking, Hous., & Urb. Affs., *119th Cong.,* Digital Asset Market Structure Discussion Draft (Comm. Print 2026) https://www.banking.senate.gov/imo/media/doc/market_structure_draft.pdf; *Senate Banking Committee Releases Amendment to 2025 Responsible Financial Innovation Act Draft*, Davis Wright Tremaine (Jan. 15, 2026), https://www.dwt.com/blogs/financial-services-law-advisor/2026/01/responsible-financial-innovation-act-amendment.

1964 Press Release, S. Comm. on Agric., Nutrition, & Forestry , *Boozman, Booker Release Bipartisan Market Structure Discussion Draft* (Nov. 21, 2025), https://www.agriculture.senate.gov/newsroom/rep/press/release/boozman-booker-release-bipartisan-market-structure-discussion-draft.

1965 S. Comm. on Banking, Hous., & Urb. Affs., *supra* note 1963, §702 (prohibiting passive yield on stablecoin holdings while allowing activity-based rewards); see *also Banks Push to Limit Stablecoin Rewards Ahead of Senate's CLARITY Act Markup*, Stocktwits (Jan. 10, 2026), https://stocktwits.com/news-articles/markets/cryptocurrency/banks-push-to-limit-stablecoin-rewards-ahead-of-senate-s-clarity-act-markup/cmU3mMER43e.

1966 Jason Brett, *Coinbase Pulls Support Night Before Senate Markup Of Market Structure*, Forbes (Jan. 14, 2026), https://www.forbes.com/sites/jasonbrett/2026/01/14/coinbase-pulls-support-night-before-senate-markup-of-market-structure/.

1967 For eg., in a five-page letter sent on January 13 2026 to the Senate Banking and Agriculture Committees, former SEC Chief Accountant Lynn Turner argues that the draft legislation lacks the transparency and financial disclosure standards necessary for effective oversight and informed investment decisions. Soyoung Ho, *Ex-SEC Chief Accountant Warns Senate Crypto Bill Could Trigger Next FTX*, Thomson Reuters Tax & Accounting News (Jan. 15, 2026), https://tax.thomsonreuters.com/news/ex-sec-chief-accountant-warns-senate-crypto-bill-could-trigger-next-ftx/.

1968 *See, e.g.*, Press Release, U.S. Sen. Comm. on Banking, Hous., & Urb. Affs., *At Hearing, Ranking Member Warren Releases Principles for Crypto Market Structure Legislation* (July 9, 2025), https://www.banking.senate.gov/newsroom/minority/at-hearing-ranking-member-warren-releases-principles-for-crypto-market-structure-legislation.

certainty will take time. In the meantime, technological development proceeds under conditions of substantial legal uncertainty. This uncertainty may constitute a barrier to adoption of blockchain technology, as market participants are reluctant to invest in technologies whose legal status is unclear or whose use may expose them to litigation. For example, smart contracts and DAOs require at least a minimal framework of legal recognition to be deployed and relied upon without undue legal risk.[1969]

In this context, regulation often appears necessary to facilitate mainstream adoption of technology by providing clarity and predictability. Yet, when technologies and industry practices evolve too rapidly, premature legislation can risk producing rules that quickly become obsolete or ineffective. Overly detailed or rigid regulatory measures may impose disproportionate burdens on the industry and hinder innovation. Nonetheless, many recent initiatives adopt a generally supportive stance toward blockchain technologies, with the stated objective of fostering innovation and enabling market development. Because they do not rely solely on piecemeal enforcement actions or non-binding interpretive guidance, these frameworks reduce uncertainty and are generally more durable.

The following section examines legal frameworks primarily designed to facilitate the development of blockchain technology by clarifying the legal status of its main applications and use cases: decentralized autonomous organizations (DAOs), smart contracts, digital identity, and crypto-assets. These frameworks integrate emerging technologies into existing legal systems and specify the conditions of their lawful operation. While they provide the legal basis for implementing and using blockchain-based solutions, they simultaneously introduce principles and rules that enable regulatory oversight and risk mitigation. This dual function is particularly evident in the regulation of crypto-assets, addressing a regulatory gap and establishing a comprehensive set of new rules and safeguards.

7.3.1. Designing a Legal Framework for DAOs

Case law illustrates that defining the legal nature of DAOs is particularly challenging, as they occupy an intermediate position between being a fully autonomous software system and a recognized legal person *(See above section 6.4.1.)*. DAOs display a pronounced contractual dimension: By acquiring governance tokens and participating in decision-making processes, users express their intention to collaborate within a framework established by the DAO's governing code. At the same time, DAOs operate as organized entities coordinating collective activity on decentralized networks.

Addressing the uncertainty surrounding the legal status of DAOs can give rise to divergent regulatory strategies. A first approach consists in the cautious, incremental adaptation of existing legal structures, an option that is often more politically and practically feasible than the creation of entirely novel and untested regimes. For example, in its 2024 report, the UK Law Commission recommended relying on established legal forms —such as partnerships and trusts—[1970] while clarifying the scope of participant liability.[1971] A more ambitious approach seeks to design a bespoke legal status for DAOs that takes into account their defining characteristics, including decentralization, automation, and, in some cases,

1969 *See, e.g.*, Aiden Slavin & Kevin Werbach, *Decentralized Autonomous Organizations Explained*, World Econ. F. (Jan. 17, 2023), https://www.weforum.org/stories/2023/01/everything-you-need-to-know-daos ("Without well-defined legal status, DAOs may not be able to benefit from legal frameworks, simplified tax arrangements and limited liability. [This legal uncertainty] could endanger users, facilitate financial crime and stymie innovation. A variety of recent policy efforts have sought to remedy this . . . Nonetheless, gaps remain.").

1970 The Law Comm'n, *Decentralised Autonomous Organisations* (DAOs): A Scoping Paper 144, 149-50 (July 2024), https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/.

1971 *Id.* at 44, 48, 51.

participant anonymity. The following section focuses on this latter approach, beginning with the COALA DAO Model Law, then examining the principal DAO-specific legal regimes adopted to date in the United States, Malta, and the Marshall Islands.

7.3.1.A. The COALA Model Law for DAOs

The Coalition of Automated Legal Applications (COALA) published a draft DAO Model Law on June 19, 2021.[1972] It represents one of the earliest and most ambitious efforts to articulate a harmonized legal framework specifically designed for DAOs. The COALA DAO Model Law was designed for international adoption, aiming to reduce legal uncertainty and regulatory fragmentation for DAOs operating across multiple jurisdictions.[1973] The Model Law's central objective is to allow DAOs to obtain legal personality and limited liability as DAOs, provided that certain technological conditions are met.[1974] And the Model Law would do so without requiring the DAOs to adopt or adapt a centralized legal entity form, such as an LLC, or subjecting them to traditional registration procedures.[1975] This approach not only legitimizes DAOs as legal entities but preserves their decentralized nature.[1976]

1. Key Provisions

The COALA DAO Model Law rests on the principles of *functional, regulatory* and *technological* equivalence. *(See section 1.3.2.)*[1977] It proceeds from two core premises: first, that existing legal frameworks can be extended to new technological contexts; and second, that technological architectures can, in certain cases, achieve the policy objectives that law traditionally secures through institutional or procedural mechanisms.

Within this perspective, DAOs may fulfill legal obligations through technological design rather than administrative procedures.[1978] Blockchain-based characteristics, such as transparency, immutability, and automated governance, are treated as functional substitutes for corporate law requirements, while smart contracts are regarded as the functional equivalent —expressed in computer code— of corporate bylaws or articles of association. This approach treats technological design as a functional substitute for certain legal mechanisms, while implicitly acknowledging that such substitution may be partial or imperfect.

- **Legal personality.** The Model Law does not rely on discretionary recognition by public authorities. Instead, its formation and legal-personhood provisions provide that a DAO is deemed to be a legal person by operation of law once it satisfies the statute's conditions.[1979] Recognition is thus conceived as automatic and rules-based, rather than constitutive in the traditional corporate-law sense.
- **Formation requirements**. Under the Model Law, a DAO benefits from legal personality if it fulfills eleven cumulative requirements, including, inter alia: deployment on a permissionless blockchain;[1980] publication of its full codebase in open-source format and subject to quality-assurance procedures

1972 Constance Choi et al., Coal. of Automated Legal Applications, *Model Law for Decentralized Autonomous Organizations* (DAOs) (2021) [hereinafter COALA DAO Model Law], https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf.

1973 *Id*. at 7.

1974 *Id*. at 18.

1975 *Id.* at 6.

1976 *Id*. at 4-5.

1977 *Id*. at 7-8.

1978 *Id*. at 11.

1979 *Id*. art. 2, at 11 and art.4(3) at 19.

1980 *Id*. art. 4(1)(a), at 18.

(such as security audits);[1981] the availability of user-friendly interfaces and a unique public address enabling third parties to monitor its operations;[1982] publicly accessible and comprehensible bylaws;[1983] a governance system that is technically decentralized;[1984] the continuous existence of at least one member;[1985] a publicly specified contact mechanism;[1986] and the designation of binding dispute-resolution mechanisms.[1987]

- **DAO members:** Under Article 7 of the Model Law, DAO members are, in principle, holders of governance tokens. Token ownership or acknowledgment of ownership through on-chain interaction suffices to establish membership, subject to bylaw-defined participation classes.
- **Limited liability**: DAO members enjoy limited liability: They are required to make only their committed on-chain contributions and are not personally liable for the DAO's obligations, including labor and tax debts, even if the DAO's assets are exhausted.[1988] An exception applies where a DAO refuses to comply with a binding judgment or award: Members who vote against compliance may be personally liable in proportion to their governance rights.[1989] Members remain personally liable for their own wrongful acts but not for those of other members.[1990]
- **Governance**. The COALA DAO Model Law enables DAOs to define different tiers of membership with varying voting rights and financial benefits. DAO members can appoint administrators or representatives to handle off-chain interactions,[1991] but DAOs are not required to have administrators. In the absence of administrators, DAO members run the DAO collectively as a class.[1992]
- **Taxation.** DAOs are treated as "transparent entities" in jurisdictions that adopt the COALA DAO Model Law,[1993] which can simplify tax compliance by passing tax obligations through to individual members or stakeholders.
- **Blockchain-specific risks**: In cases of hard forks — where a blockchain splits into two separate chains *(See above section 2.3.4.B.)*— the COALA DAO Model Law includes mechanisms to determine which version retains the DAO's legal personality.[1994] It calls for default to the "Majority Chain" after a hard fork, though the criteria for determining such a chain remain vague.[1995] The law also affirms continuity of legal personality despite technical failures, such as smart contract malfunctions or hacks.[1996] This offers

1981 *Id*. art. 4(1)(c)(d), at 18.

1982 *Id*. art. 4(1)(b), at 18.

1983 *Id*. art. 4(1)(f), at 18.

1984 *Id*. art. 4(1)(g), at 19.

1985 *Id*. art. 4(1)(h), at 19.

1986 *Id*. art. 4(1)(i), at 19.

1987 *Id*. art. 4(1)(j)(k), at 19.

1988 *Id*. art. 5(2), at 24. A member is "any person or DAO who has governance rights in a DAO." *Id.* art. 3(18), at 14.

1989 *Id*. art. 5(3), at 24.

1990 *Id*. art. 5(4), at 24.

1991 *Id*. art. 7-8, at 30-33.

1992 *Id*. art. 13-14, at 37-38.

1993 *Id*. art. 20, at 50.

1994 *Id*. art. 16, at 42-44.

1995 The commentary to the provision suggests that, if the Majority Chain is not readily apparent, one may look at security, the number of applications on the blockchain (widespread adoption), market capitalization, community recognition, and trademark. It is also not clear who exactly would apply this case-by-case framework. *Id.* at 45-46.

1996 *Id*. art. 18, at 48.

the DAOs an important level of resilience absent in many existing frameworks since, under traditional laws, entities lose legal standing if they cease functioning.

- **Dispute resolution**. Dispute resolution under the COALA DAO Model Law emphasizes the use of on-chain mechanisms to settle disagreements,[1997] but it does not exclude the possibility of accessing traditional legal systems when necessary.[1998] This dual-path approach to conflict resolution reflects an effort to preserve the autonomous operation of DAOs while ensuring access to legal remedies when required.

2. Influence and Challenges

The COALA DAO Model Law advances a bold proposal for a standardized, technology-specific framework tailored to DAOs. Although published in 2021, it remains a living project that continues to solicit input from legal scholars and blockchain developers,[1999] and it has already influenced several legislative initiatives. Some jurisdictions, including Utah and New Hampshire *(See below section 7.3.1.B.)*, have explicitly drawn inspiration from COALA's underlying principles.[2000]

No jurisdiction, however, has embraced the Model Law's most radical innovation: the rejection of any mandatory registration procedure or human-mediated formation requirement. Under the COALA DAO Model Law, the mere existence of a DAO and its compliance with the Model Law's substantive requirements are sufficient to automatically confer legal personality on the organization and limited liability on its members. This protocol-first approach to legal recognition departs sharply from traditional entity law, which is built around filings, registries, and identified accountable persons, even in limited-liability contexts. It is, therefore, unsurprising that regulators have thus far been reluctant to adopt such a model, particularly given concerns about supervision, jurisdiction, and the identification of responsible actors.

At the same time, the Model Law seeks to offset the absence of registration through demanding technical safeguards, including security audits and high-quality code requirements.[2001] While these mechanisms may enhance trust and reduce certain risks, they also raise concerns about cost and complexity,[2002] potentially deterring smaller projects or early-stage startups from relying on the framework.

Finally, the current version of the COALA DAO Model Law leaves areas of legal uncertainty, particularly regarding the status of smart contracts as constitutive legal instruments.[2003] Although Article 4(1)(f) requires the adoption of plain-language bylaws, the Model Law does not clearly specify whether the DAO's code or its bylaws prevail in the event of a conflict. This unresolved hierarchy between code and legal documentation illustrates the broader challenge of translating autonomous, software-based governance into coherent legal form.[2004]

1997 COALA DAO Model Law, *supra* note 1972, art. 4(1)(j)-(k), at 22, art. 3(9), at 13.

1998 *Id*. at 22.

1999 *Id*.

2000 Robert B. Lamb, *Utah Passes Innovative DAO Legislation*, Nat'l L. Rev. (Mar. 2, 2023), https://natlawreview.com/article/utah-passes-innovative-dao-legislation ("The Utah DAO Act adopted a version of the COALA Model law, which does more, goes further and achieves a level of "legal personality", limited liability protections, and avenues for decentralization and anonymity than the simple "LLC wrapper" approach.").

2001 COALA DAO Model Law, *supra* note 1972, art. 4(1)(d), at 18.

2002 *See* Mark Swiderski, *DAO – The Most Expensive Entity Structure Known to Man*, Campbell Teague (Jan. 20, 2023), https://campbellteague.com/dao-the-most-expensive-entity-structure-known-to-man/.

2003 "The deployment of a smart contract on a blockchain with relevant data about a DAO is not functionally equivalent to registration into a corporate registry, but the policy objectives of publicity and certainty are fully achieved." *Id.* at 3.

2004 Swiderski, *supra* note 2002 (suggesting that in common law jurisdictions this ambiguity could potentially be solved by reference to case law).

7.3.1.B. U.S. State Legal Frameworks for DAOs

While no action has been taken at the federal level, a growing number of U.S. states have experimented with providing legal recognition for DAOs.[2005] The first wave of state legislation has generally relied on a "wrapper" approach, integrating DAOs into existing entity forms —most notably into limited liability companies (LLCs). Laws adopted in states such as Wyoming and Tennessee allow DAOs to register as DAO-LLCs, thereby extending limited liability and a degree of regulatory certainty within a familiar corporate framework. However, while these regimes accommodate certain technological features, they often struggle to fully reflect DAOs' defining characteristics, particularly decentralized governance and smart-contract-based operations.

More recent frameworks move beyond the LLC and foundation models to design legal structures that more closely align with DAOs' decentralized and code-driven nature. The COALA DAO Model Law has strongly influenced this shift. Utah's DAO Act draws directly on COALA's proposals, while New Hampshire has enacted its own DAO-specific legislation that both incorporates and expands upon elements of the model. These developments signal a gradual transition from adapting DAOs to fit traditional corporate forms toward crafting bespoke legal regimes tailored to their unique characteristics.

1. Vermont (2018)

Vermont was among the earliest U.S. states to recognize "blockchain-based limited liability companies" (BBLLCs), integrating the use of blockchain technology within the traditional LLC framework, rather than creating a DAO-specific legal form or a distinct category of legal personhood.[2006] With the adoption of Senate Bill 269 (*An Act Relating to Blockchain Business Development*), signed into law on May 30, 2018, and effective July 1, 2018, Vermont expressly acknowledged that LLCs may use blockchain technology in their formation and governance.[2007]

Vermont law allows LLCs that "utilize blockchain technology for a material portion" of their operation to be registered as blockchain-based limited liability companies ("BBLLCs").[2008] These entities must file articles of organization indicating that status. In its formation documents, a BBLLC must include a summary of its mission or purpose, specify its degree of decentralization, identify the type of blockchain on which it operates, and describe the extent of participants' access to information as well as their read and write permissions with respect to the protocol.[2009] The statute also requires the company to specify how membership is acquired and what rights attach to membership.

The BBLLC must adopt voting procedures, which may rely on smart contracts. They must also establish protocols designed to respond to system security breaches or other unauthorized actions that compromise the integrity of the blockchain. The identification and governance details of any smart contracts are documented in the operating agreement rather than the articles of organization.[2010] This approach ensures that, while the entity's formation is formally recognized by the state, the technical and governance mechanisms —such as smart contracts that

2005 Matt Blaszczyk, *Decentralized Autonomous Organizations and Regulatory Competition: A Race Without a Cause*, 99 N.D. L. Rev. 107 (2024), https://ssrn.com/abstract=4509636.

2006 *Vermont Technology Company Creates First Blockchain-Based LLC*, Gravel & Shea PC (July 13, 2018), https://gravelshea.com/2018/07/vermont-technology-company-creates-first-blockchain-based-llc/.

2007 S. 269, 2017-18 Leg., Reg. Sess. (Vt. 2018).

2008 Vt. Stat. Ann. tit. 11, § 4172 (2024).

2009 *Id*. § 4173.

2010 Vt. Stat. Ann. tit. 11, §4172, 4173 (2024). An operating agreement is the LLC's internal governance contract, setting out how the entity is managed and how members' rights and obligations are defined; for BBLLCs, it also records how smart contracts operate and may be amended.

automate voting or management— are documented within the company's internal governance structure.

Vermont law does not require smart contracts to be capable of being amended; instead, it requires disclosure of procedures for upgrading or modifying smart contracts if such mechanisms exist.[2011] This means BBLLCs must have clear, internal mechanisms for how changes to their core blockchain systems are proposed, voted on, and implemented, ensuring both flexibility and resilience as technology advances.

Importantly, Vermont's law requires human involvement through an "administrative member," and it does not eliminate fiduciary duties by default. Overall, the BBLLC regime remains a conventional LLC framework that accommodates blockchain use, rather than a comprehensive legal regime tailored to fully autonomous or highly decentralized DAOs.

2. Wyoming (2021)

Wyoming also created a dedicated LLC form for DAOs. In 2021, it enacted the DAO Supplement to the LLC Act, becoming the first U.S. state to establish a legal framework specifically for DAOs.[2012] Under this law, DAOs enjoy the protections of limited liability while being partially relieved from traditional LLC governance constraints.

The Wyoming statute affirms the primacy of code over legal documents[2013] by providing that, "[w]here the underlying articles of organization and smart contract are in conflict, the smart contract shall preempt any conflicting provisions of the articles of organization."[2014] This principle, commonly referred to in the blockchain ecosystem as "code-deference," allows DAOs to define whether governance is conducted by human members or through autonomous algorithms.[2015] They can also designate whether the DAO is managed by human members or autonomous algorithms.[2016] While Wyoming's framework gives DAOs substantial autonomy to define and operate their internal governance mechanisms, state authorities and courts retain the power to intervene in cases of legal disputes or statutory violations, just as they would with any other LLC.[2017]

The Wyoming model originally required that, for a proposal to be valid, at least 50% of DAO members must participate in voting; but, a 2022 amendment subsequently allowed DAOs to define their own quorum requirements in their articles of organization.[2018] Additionally, Wyoming mandates that a DAO's articles of organization be amended whenever the underlying smart contracts are updated or changed, ensuring that the legal documentation reflects the operational reality and facilitates the entity's evolution over time.[2019]

2011 Vt. Stat. Ann. tit. 11, §4173 (2)(B) (2024).

2012 S. 73, 66th Leg., Gen. Sess. (Wyo. 2021). Amended in 2022, S. 16, 66th Leg., Budget Sess. (Wyo. 2022).

2013 *See* Sal Qadir, *DAOs: The Future of Organizing Communities Online*, Galaxy Digit. Rsch., 16 (2024), https://assets.ctfassets.net/h62aj7eo1csj/7161Cn2xibBNRmTvG5fpxQ/e739b9233e07d4c1d893d18c89f8dc71/GLXY_DAOs_Whitepaper.pdf.

2014 Except for specific requirements about the DAO's formation and the identification of its smart contracts in the articles of organization, where the articles and state law take priority. *See* Wyo. Stat. Ann. § 17-31-115 (2024) (as amended) ("Where the underlying articles of organization and smart contract are in conflict, the smart contract shall preempt any conflicting provisions of the articles of organization, except as it relates to W.S. 17-31-104 and 17-31-106(a) and (b).").

2015 *See generally* Andrew M. Hinkes, *The Limits of Code Deference*, 46 J. Corp. L. 869 (2021), https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Hinkes_Final_Web_0.pdf.

2016 Wyo. Stat. Ann. § 17-31-104(e) (2024) ("A statement in the articles of organization shall establish how the decentralized autonomous organization shall be managed by the members, including to what extent the management will be conducted algorithmically.").

2017 For example, the Wyoming Limited Liability Company Act applies to DAOs except where inconsistent with the DAO Supplement, subjecting DAOs to standard LLC judicial procedures for disputes. Wyo. Stat. Ann. § 17-31-103(a) (2024). courts may dissolve a DAO for statutory noncompliance, such as inactivity, unlawful purpose, or loss of human control. Wyo. Stat. Ann. § 17-31-114(c) (2024). While smart contracts generally preempt conflicting articles of organization, courts retain authority to resolve disputes involving statutory compliance. Wyo. Stat. Ann. § 17-31-115 (2024). Additionally, DAOs, like all Wyoming LLCs, are subject to state oversight for fraud, contractual breaches, or violations of fiduciary duties under the implied covenant of good faith and fair dealing. *See* Wyo. Stat. Ann. § 17-31-110 (2024).

2018 Wyo. Stat. Ann. § 17-31-102(a)(v) (2024).

2019 Wyo. Stat. Ann. § 17-31-107(a)(iii) (2024).

In March 2024, Wyoming went a step further by passing the *Decentralized Unincorporated Nonprofit Association Act* (DUNA Act), which was signed into law on March 7, 2024, and took effect July 1, 2024.[2020] The statute introduces a new, purpose-built legal entity for nonprofit, public-benefit DAOs, operating alongside Wyoming's earlier DAO-LLC framework.[2021] The DUNA framework addresses a critical gap left by the DAO LLC model: It provides a legal structure tailored for nonprofit, public-benefit DAOs —such as those governing blockchain protocols or managing open-source projects— which cannot operate as for-profit LLCs but need legal recognition and liability protection.[2022]

The DUNA Act recognizes DAOs as legal entities — specifically, as decentralized unincorporated nonprofit associations (DUNAs). This status confers legal personality, capacity to contract and hold property, and limited liability for participants.[2023] Eligibility is subject to statutory conditions, including a requirement that the DAO maintain at least 100 members. By carving out a dedicated nonprofit pathway for large, community-governed DAOs, the DUNA framework represents a significant step toward providing legal certainty for open and decentralized blockchain ecosystems. Wyoming thus operates two coexisting DAO regimes: the original 2021 DAO-LLC Supplement, which wraps DAOs within the LLC form and is primarily used by for-profit DAOs, and the 2024 DUNA Act, which introduces a dedicated unincorporated nonprofit structure for public-benefit DAOs.

3. Tennessee (2022)

Closely following on Wyoming's lead, Tennessee amended its Limited Liability Company Act in 2022 to permit the formation of decentralized organizations ("DO LLCs"), defined as limited liability companies whose articles of organization expressly state that the company is a decentralized organization.[2024] The statute specifies mandatory content for the articles of organization, including a conspicuous "Notice of Restrictions on Duties and Transfers"[2025] and DO LLCs may be organized as for-profit or nonprofit entities.

A DO LLC may be either member-managed or "smart-contract managed," the latter meaning that governance and voting mechanisms may be executed through smart contracts, provided that such smart contracts are capable of being amended.[2026] The framework requires DO LLCs to maintain a registered agent in the state, but the individual forming the entity need not be a member.[2027] Tennessee law also removes default fiduciary duties of members, subject to the implied covenant of good faith and fair dealing, unless otherwise modified by the operating agreement.[2028] Notably, it provides for automatic dissolution where the DAO fails to approve proposals or take actions for a period of one year.[2029]

Unlike the statutes adopted in Utah and New Hampshire, Tennessee's law does not establish a separate DAO registry, does not impose substantive requirements relating to open-source development or protocol quality assurance, and does not mandate operation on permissionless

2020 S. 50, 67th Leg., Gen. Sess. (Wyo. 2024).

2021 Hanna Brovenko, *Wyoming's DUNA Act: A New Dawn for DAOs in the Digital Dune*, Aurum L. (Sept. 26, 2024), https://aurum.law/newsroom/Wyoming%E2%80%99s-DUNA-Act-a-new-dawn-for-daos-web3.

2022 Wyo. Stat. Ann. § 17-32-102(a)(iii) (2024).

2023 Miles Jennings & David Kerr, *The DUNA: An Oasis for DAOs,* a16z Crypto (Mar. 7, 2024), https://a16zcrypto.com/posts/article/duna-for-daos/.

2024 Tenn. Code Ann. § 48-250-103(a) (2022).

2025 *Id*. § 48-250-103(c).

2026 *Id*. § 48-250-104(c).

2027 *Id*. § 48-250-104(a)-(b).

2028 *Id*. § 48-250-109(a).

2029 *Id*. § 48-250-113(a)(4).

blockchains.[2030] Tennessee law also prohibits the issuance of a certificate of authority for a decentralized organization based outside of the United States or its territories.[2031]

4. Utah (2023)

Unlike the LLC-based frameworks adopted in Tennessee, Vermont, and Wyoming, which adapted existing corporate forms to accommodate blockchain-based entities, Utah recognizes DAOs as an entirely separate legal entity. In 2023, it became the first U.S. state to enact a DAO-native statute: the Utah DAO Act.[2032] This framework represents a decisive break from the "wrapper" model used in Vermont, Tennessee, and Wyoming, where DAOs remained subtypes of LLCs notwithstanding accommodations for smart contracts and decentralized governance. By contrast, Utah's statute —directly inspired by the COALA DAO Model Law *(See above section 7.3.1.A.)*— creates a DAO-native limited-liability entity rather than adapting an existing corporate form, establishing DAOs as a standalone legal form.[2033]

The Utah DAO Act allows DAOs to register as Limited Liability Decentralized Autonomous Organizations (LLDs) —a new legal entity distinct from traditional LLCs.[2034] The Act aims to provide DAOs with legal personality,[2035] limited liability,[2036] and the ability to operate autonomously through smart contracts on a permissionless blockchain.[2037]

There are other ways the Utah DAO Act differs from Wyoming's DUNA Act, which allows certain DAOs to register as Decentralized Unincorporated Nonprofit Associations (DUNAs).[2038] While Wyoming's DUNA framework targets nonprofit, public-benefit DAOs with at least 100 members,[2039] Utah's LLD structure is designed for for-profit DAOs,[2040] imposes no minimum member requirement beyond a single member,[2041] and explicitly supports decentralized governance,[2042] anonymity protections,[2043] and operation on permissionless blockchains,[2044] a stark contrast to Wyoming's DUNA framework.

2030 *Compare* Tenn. Code Ann. § 48-250-101 *et seq.* (2025), *with* Utah Code Ann. § 48-5-201 *et seq.* (2025), *and* N.H. Rev. Stat. Ann. § 301-B:1 *et seq.* (2025).

2031 *Id*. § 48-250-115.

2032 H.B. 357, 2023 Gen. Sess. (Utah 2023) (enacted Mar. 13, 2023; effective Jan. 1, 2024), codified at Utah Code Ann. §§ 48-5-101 to -406 (2023).

2033 Joni Pirovich, a blockchain and digital assets tax adviser who worked with the Digital Innovation Taskforce, stated that the Utah DAO Act "is a huge step for DAO innovation as the Act is based on the @coalaglobal DAO Model Law, and will become effective from January 2024." *See* Amaka Nwaokocha, *DAO Gets Legal Recognition in the US as Utah DAO Act Passes*, Cointelegraph (Mar. 7, 2023), https://cointelegraph.com/news/dao-gets-legal-recognition-in-the-us-as-the-utah-dao-act-passes.

2034 Utah Code Ann. § 48-5-104 (2024) ("A decentralized autonomous organization that meets the requirements of this act: (1) shall be deemed a legal entity separate and distinct from the decentralized autonomous organization's members; (2) has the capacity to sue and be sued in the decentralized autonomous organization's own name and the power to do all things necessary or convenient to carry on the decentralized autonomous organization's activities and affairs; (3) shall meet the decentralized autonomous organization's liabilities through the decentralized autonomous organization's assets; (4) may have any lawful purpose; and (5) has perpetual duration.").

2035 Utah Code Ann. § 48-5-104(1) (2024).

2036 Utah Code Ann. § 48-5-202 (2024).

2037 To qualify as a Limited Liability Decentralized Autonomous Organization (LLD), the DAO must be "deployed on a permissionless blockchain." Utah Code Ann. § 48-5-201(3)(a) (2024).

2038 "Profits from any activities shall be used in furtherance of, or set aside for, the nonprofit association's common nonprofit purpose." Wyo. Stat. Ann. § 17-32-104(a) (2024).

2039 Wyo. Stat. Ann. § 17-32-102(a)(iii) (2024).

2040 *See* Utah Code Ann. § 48-5-104(4)(2024) ("may have any lawful purpose"); Utah Code Ann. § 48-5-406 (2024) (taxation options for LLDs). The statute does not restrict LLDs to nonprofit activities, and the legislative commentary and analysis confirm that the structure is intended to enable DAOs to operate as for-profit enterprises if they choose.

2041 "The decentralized autonomous organization has at least one member." Utah Code Ann. § 48-5-201(3)(g) (2024).

2042 Utah Code Ann. §§ 48-5-101(5), 48-5-201(3)(f) (2024) (defining "decentralized" as "decision-making [that] is distributed among multiple persons" and requiring that "the governance system of the decentralized autonomous organization is decentralized"). By contrast, Wyo. Stat. Ann. § 17-32-102(a) (2024) defines "governing principles" to include consensus algorithms and smart contracts; the DUNA Act presupposes decentralized governance but does not impose a strict statutory decentralization test.

2043 The Wyoming DUNA Act contains no provisions for anonymity or redaction of personal information in filings or bylaws. The Utah DAO Act explicitly protects anonymity by allowing organizers to request redaction of public filings and permitting DAOs to redact sensitive information from bylaws to safeguard member privacy. *See* Utah Code Ann. §§ 48-5-201(2)(b), 48-5-201(4) (2024).

2044 The Wyoming DUNA Act permits but does not require use of blockchain or distributed ledger technology; it allows DUNAs to operate on either public or private, permissioned or permissionless blockchains. *See* Wyo. Stat. Ann. §§ 17-32-102(a)(v), 17-32-121(b)(i). In contrast, the Utah DAO Act mandates deployment on a permissionless blockchain, defined as a publicly distributed ledger in which block validation is independent of user identity. *See* Utah Code Ann. §§ 48-5-101(23), 48-5-201(3)(a) (2024).

Unlike the statutes in Wyoming and Vermont, the Utah DAO Act does not require that the smart contracts governing a DAO be capable of amendment or upgrade. Instead, it places governance authority in member-adopted bylaws, with bylaws serving as the primary source of legal authority and smart contracts recognized as the operational implementation of those rules.[2045] Under the Act, DAOs must adopt bylaws[2046] —rather than traditional operating agreements— that establish governance structures,[2047] define the scope of limited liability,[2048] and set procedures for redacting personal information.[2049] The Act introduces a technology gatekeeping function to ensure that only organizations genuinely governed by code and consensus can qualify for LLD status.[2050] It also includes quality assurance requirements for DAO protocols[2051] and clarifies that no fiduciary duties are implied among participants unless explicitly stated in the bylaws.[2052]

Under the Utah DAO Act, members of an LLD are not personally liable for the organization's obligations solely by reason of participation, and liability is generally limited to their contributions,[2053] subject to specified statutory exceptions, including personal misconduct and voting against compliance with a court-ordered remedy.[2054] The Act permits proxy voting[2055] and requires that at least one natural person act as incorporator,[2056] thereby creating a minimal point of human accountability at formation while preserving the possibility of pseudonymous and decentralized participation thereafter.

While the Act has been praised for its innovation and its alignment with decentralized governance principles, concerns remain. One concern is the state law's compatibility with federal transparency obligations such as those that previously arose under the federal Corporate Transparency Act.[2057] Questions remain about how pseudonymous DAO structures interact with federal regulatory requirements, including anti-money laundering obligations and securities law disclosure rules. For example, a DAO whose participants wish to remain pseudonymous may still struggle to comply with certain regulatory requirements without compromising the privacy protections that attracted participants to a decentralized structure in the first place.

2045 *See, e.g.*, Utah Code Ann. § 48-5-101(6) (2024).

2046 Utah Code Ann. § 48-5-203(1) (2024).

2047 Utah Code Ann. § 48-5-301-304 (2024).

2048 Utah Code Ann. § 48-5-202 (2024).

2049 Utah Code Ann. § 48-5-201(4) (2024).

2050 For example, DAOs must be deployed on a permissionless blockchain, with all transactions recorded on-chain, Utah Code Ann. § 48-5-201(3)(a) (2024); a unique public address must allow anyone to monitor transactions, Utah Code Ann. § 48-5-201(3)(b) (2024); software code must be publicly available for review, Utah Code Ann. § 48-5-201(3)(c) (2024).

2051 Utah Code Ann. § 48-5-201(3)(d) (2024) requires DAOs to submit evidence that their software code has undergone "quality assurance," defined as a security review in accordance with industry standards; Utah Code Ann. § 48-5-103(2)(c) (2024) authorizes the Division of Corporations to establish rules identifying industry standards for these security reviews; Utah Code Ann. § 48-5-201(3)(c) (2024) further mandates that DAO software code be publicly available for review, ensuring transparency and accountability.

2052 Utah Code Ann. § 48-5-307 (2024) states that developers, members, participants, or legal representatives of a DAO "may not be imputed to have fiduciary duties... unless (1) [they] explicitly hold themselves out as a fiduciary; or (2) [this is] stipulated in the by-laws."

2053 Utah Code Ann. § 48-5-202(1)(a) (2024).

2054 Utah Code Ann. § 48-5-202(2) (2024).

2055 Utah Code Ann. § 48-5-303(1)-(3) (2024).

2056 Utah Code Ann. § 48-5-201(1)(b) (2024).

2057 31 U.S.C. § 5336. Until March 2025, the Corporate Transparency Act required the disclosure of beneficial ownership information for most U.S. entities, highlighting the tension between blockchain-based pseudonymity and federally mandated identification duties. The Act's anonymity provisions (allowing redaction of member identities) and decentralized governance made it difficult to identify and report beneficial owners as required by the Corporate Transparency Act, raising potential conflicts with federal disclosure rules. *See* Amy Sanderson, *Utah Grants DAO's Corporate Identity, Personhood Status*, Gamma L. (Aug. 2, 2023), https://gammalaw.com/utah-grants-daos-corporate-identity-personhood-status/. However, in March 2025, the Trump administration's Financial Crimes Enforcement Network (FinCEN) issued an interim final rule removing beneficial ownership reporting requirements for U.S. companies and U.S. persons, substantially eliminating this specific compliance conflict, *see also* Press Release, U.S. Dep't of the Treasury, *FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies and U.S. Persons, Sets New Deadlines for Foreign Companies* (Mar. 21, 2025), https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us.

5. New Hampshire (2024)

New Hampshire's Decentralized Autonomous Organization Act (H.B. 645) marks a major milestone in the legal recognition of DAOs in the United States.[2058] The New Hampshire DAO Act officially took effect in two phases: Provisions establishing the DAO registry and basic registration procedures (RSA 301-B:31) became effective immediately upon the bill's signing on July 26, 2024, enabling DAOs to begin registering without delay. The remainder of the Act —including detailed governance requirements and liability protections— became fully effective on July 1, 2025.

The law created a standalone legal entity for DAOs, distinct from the LLC-based structures used in other states and distinct from Utah's hybrid approach, which created a DAO-native entity while still anchoring legal authority primarily in off-chain bylaws. Drawing inspiration from the COALA DAO Model Law and the work of the New Hampshire Commission on Cryptocurrencies and Digital Assets,[2059] the New Hampshire law grants legal personhood and limited liability to DAOs registered in the state, extending these protections to developers, administrators, participants, and legal representatives.[2060]

A central feature of the Act is the establishment of a public DAO registry overseen by the Secretary of State.[2061] To be listed, a DAO must meet eleven requirements—a statutory transposition of the COALA DAO Model Law's "equivalence criteria"— including deployment on a permissionless blockchain, use of open-source software, adoption of public and plain-language bylaws that accurately reflect the rules encoded in the DAO's software, and evidence of quality assurance testing.[2062] While NH adopts COALA's standard for functional equivalence, it introduces a specific 20% control threshold to define a "decentralized network," providing a more granular metric than the Model Law.[2063] The Act also recognizes the legal roles of administrators, developers, participants, and legal representatives, allowing DAOs to designate individuals to perform off-chain functions.[2064]

Importantly, legal personality attaches only upon delivery of a notice of intent to register with the Secretary of State, which must be submitted by one or more authorized persons and must include, inter alia, the designation of a registered agent with a physical address in New Hampshire.[2065] An "authorized person" is any individual or entity empowered by the DAO's bylaws or governing software to submit filings and interact with public authorities on the DAO's behalf. As a result, a DAO cannot acquire legal status through purely autonomous or machine-initiated processes: A natural person (or a legally recognized entity acting through natural persons) must intervene at the moment of legal activation.

Governance under the New Hampshire Act is rooted in bylaws, which must specify the rules governing participants' rights and obligations.[2066] At the same time, the statute strongly embraces freedom of contract and

2058 N.H. Rev. Stat. Ann. § 301-B:1 et seq. (2024).

2059 Keith Ammon & Bill Ardinger, *New Hampshire Has a Better Approach to DAOs*, CoinDesk (Mar. 26, 2024), https://www.coindesk.com/opinion/2024/03/26/new-hampshire-has-a-better-approach-to-daos.

2060 N.H. Rev. Stat. Ann. §§ 301-B:7, 301-B:15 (2024).

2061 *Id.* §§ 301-B:14, 301-B:31 (2024).

2062 *Id.* § 301-B:15(I)(a)-(k) (2024); Fatemeh Fannizadeh, *Lawmakers In New Hampshire And Utah Recognize DAOs As Legal Persons*, Forbes (Mar. 8, 2023), https://www.forbes.com/sites/digital-assets/2023/03/07/-new-hampshire-utah-recognize-daos-as-legal-persons/

2063 N.H. Rev. Stat. Ann. §§ 301-B:5(IX).

2064 *Id.* § 301-B:14 (2024).

2065 *Id.* § 301-B:8(I) (notice of intent requirement); *Id.* § 301-B:9 (registered agent requirement with physical New Hampshire address).

2066 *Id.* § 301-B:16 (2024).

acknowledges that participants' rights and obligations may be determined by the governing software code, embracing the "intent of code is law" philosophy.[2067] This framework requires bylaws to align with the DAO's governing software code,[2068] ensuring that the legal documentation reflects the operational reality of the DAO's smart contracts. For example, if a DAO's code automates voting procedures or profit distribution, its bylaws must explicitly outline these processes in plain language to avoid discrepancies. This reflects an explicit endorsement of a "code-deference" approach,[2069] requiring that bylaws accurately describe and align with the DAO's operational smart contracts. In this respect, New Hampshire's regime represents one of the most explicit statutory attempts to reconcile legal formality with the operational realities of autonomous, code-based governance.

6. Conclusion

Taken together, these state-level initiatives illustrate a rapid evolution in the legal treatment of DAOs in the United States. Vermont's early experiment with blockchain-based LLCs represented an incremental step, adapting the familiar LLC framework to accommodate blockchain governance. Wyoming advanced further by creating a dedicated DAO LLC form and later by introducing the DUNA framework for nonprofit DAOs. Tennessee's conservative approach demonstrated that not all states sought to push the boundaries of DAO recognition, instead prioritizing regulatory familiarity and ease of compliance.

Utah marked a decisive departure by establishing DAOs as a standalone legal form through the DAO Act, directly inspired by the COALA DAO Model Law, and embedding governance authority in bylaws rather than smart contracts. New Hampshire has gone still further by adopting a comprehensive statutory framework that integrates principles of code-deference, open-source transparency, and quality assurance into a public registry of DAOs. This progression reflects a broader shift from tentative adaptations within existing corporate forms to the construction of bespoke legal regimes tailored to DAOs' decentralized, code-driven character.

At the same time, a significant common feature across all existing U.S. state frameworks is the retention of a mandatory human touchpoint at the moment of legal formation or registration. In Utah, the DAO Act expressly requires that at least one natural person act as incorporator of a Limited Liability Decentralized Autonomous Organization, even if the DAO's subsequent governance and membership remain pseudonymous or fully decentralized.[2070] In New Hampshire, while the statute does not foreground a named "incorporator" in the same formal sense, DAOs must be entered into a public registry maintained by the Secretary of State and must designate administrators, legal representatives, or other responsible persons to interact with public authorities.[2071] In both regimes, a DAO cannot acquire legal personality through purely autonomous or machine-initiated processes.

This persistent requirement of human-mediated legal activation marks an important departure from the more radical vision embodied in the COALA DAO Model Law,

2067 *Id.* §§ 301-B:2, 301-B:3, 301-B:16 (2024).

2068 N.H. Rev. Stat. Ann. § 301-B:16 (2024).

2069 The "code-deference" approach recognizes the primacy of code over legal documents, *see supra* note 2015.

2070 Utah Code Ann. § 48-5-201(1)(b) (2024).

2071 N.H. Rev. Stat. Ann. § 301-B:14 (establishing the "New Hampshire DAO registry"); *Id.* § 301-B:12(I) (requiring "one or more authorized persons, acting in the capacity of administrator or legal representative" to file the notice of intent), (defining "administrator"), *Id.* § 301-B:5(XXII) (defining "legal representative"); *Id.* § 301-B:19(I) (specifying that legal representation is for tasks "that cannot be achieved on-chain").

which contemplates the possibility of protocol-first or machine-initiated legal personhood. U.S. state law, by contrast, has embraced DAO-native entities only within the continued architecture of human-triggered legal recognition. While these innovations have positioned U.S. states at the forefront of DAO recognition,[2072] they also raise complex questions —of federal preemption, regulatory harmonization, and cross-jurisdictional enforceability— that remain to be resolved.

7.3.1.C. Malta

The Maltese Parliament adopted three significant legislative instruments on July 4, 2018, concerning so-called "technologically innovative arrangements." They were the Virtual Financial Assets Act,[2073] the Malta Digital Innovation Authority Act (MDIA Act),[2074] and the Innovative Technology Arrangements and Services Act (ITAS Act).[2075] The ITAS Act previously provided the statutory framework for the recognition and oversight of digital and decentralized structures. Those included distributed ledger technology (DLT) platforms and decentralized autonomous organizations (DAOs). Malta's current framework for the recognition and oversight of digital and decentralized structures is no longer grounded in a standalone ITAS statute but is instead administered through subsidiary regulations adopted under the MDIA Act. The ITAS Act was repealed in June 2024, and replaced by a revised, voluntary certification regime administered by the Malta Digital Innovation Authority (MDIA).[2076]

Under Malta's current regime, entities may apply to the Malta Digital Innovation Authority (MDIA) for voluntary certification as an Innovative Technology Arrangement (ITA).[2077] This process requires a technical audit of the arrangement's systems, including smart contracts and DLT platforms. A registered systems auditor verifies compliance with MDIA standards of legality, integrity, and accountability.[2078] Applicants must also appoint both a Maltese-resident legal representative and a registered technical administrator responsible for ongoing oversight and intervention capabilities.[2079]

The framework explicitly permits entities with or without legal personality to seek certification,[2080] aligning with Malta's broader policy of fostering innovation while ensuring regulatory oversight. As a result, DAOs that lack traditional corporate structures may still obtain certification, thereby benefiting from regulatory recognition and supervisory oversight within Malta's jurisdiction.

Certification itself does not create or confer legal personality; rather, it provides a regulatory seal of approval for technology arrangements that may or may not have independent legal status through other means. Consequently, certification does not by itself establish limited liability,[2081] meaning

2072 *See* Legal Nodes Team, *Wyoming LLC as a DAO Legal Wrapper: What You Need to Know*, Legal Nodes (Aug. 26, 2025), https://www.legalnodes.com/article/wyoming-dao-llc; N.H. Rev. Stat. Ann. §§ 301-B:2 (2024); Jason Finger & Peter Cramer, *Part I: With New DAO Law on the Books, Utah Joins Race with Wyoming and Tennessee to Become U.S. "Crypto Capital"*, Proskauer Rose LLP (May 25, 2023), https://www.blockchainandthelaw.com/2023/05/part-i-with-new-dao-law-on-the-books-utah-joins-race-with-wyoming-and-tennessee-to-become-u-s-crypto-capital. All three sources indicate that all states with DAO-related legal frameworks—Vermont, Wyoming, Utah, New Hampshire, and Tennessee (not discussed in this paper)—have passed these laws because they want to be jurisdictions of choice for cryptocurrency and blockchain businesses.

2073 Virtual Financial Assets Act, Cap. 590 (as amended through 2024) (Malta), https://legislation.mt/eli/cap/590/eng/pdf.

2074 Malta Digital Innovation Authority Act, Cap. 591 (as amended through 2024) (Malta), https://legislation.mt/eli/cap/591/eng/pdf.

2075 Innovative Technology Arrangements And Services Act, Cap. 592 (repealed 2024) (Malta), https://legislation.mt/eli/cap/592/eng/pdf.

2076 Innovative Technology Arrangements And Services (Itas) Certification Regulations, S.L. 591.01 (2024) (Malta), https://legislation.mt/eli/sl/591.01/eng/pdf [hereinafter ITAS Certification Regulations].

2077 ITAS Certification Regulations reg. 1(2), 3.

2078 ITAS Certification Regulations reg. 6(2), (10).

2079 ITAS Certification Regulations reg. 12(1), reg. 10(11).

2080 ITAS Certification Regulations reg. 10(2).

2081 ITAS Certification Regulations reg. 17.

members of uncertified or unincorporated DAOs may remain personally liable unless additional legal structures (e.g., a limited liability company) are adopted.

7.3.1.D. Marshall Islands

In December 2022, the Republic of the Marshall Islands (RMI) enacted the Decentralized Autonomous Organization Act (DAO Act), building on an earlier 2021 amendment to the Non-Profit Entities Act that had first extended legal recognition to certain DAO structures.[2082] The DAO Act amended and built upon the RMI's existing Non-Profit Entities Act, extending legal recognition to DAOs as a distinct organizational form.[2083] By adopting this legislation, the RMI became the first country to enact a dedicated statutory regime specifically tailored to DAOs. The Act explicitly recognizes DAOs as limited liability companies (DAO LLCs)[2084] and permits both for-profit and non-profit DAOs to incorporate.[2085] It also recognizes on-chain governance, token-based membership, and the use of smart contracts as legitimate mechanisms for organizational management.[2086]

The legislation enhances transparency and accountability by requiring DAOs to disclose certain information, including beneficial ownership,[2087] and establishes clear procedures for formation, management, withdrawal, and dissolution.[2088] Importantly, the RMI framework allows DAOs to elect their tax status, with for-profit DAO LLCs subject to a modest 3% gross revenue tax and non-profit DAO LLCs benefiting from tax-exempt status.[2089] In addition, Section 703(1)(c) of the Act incorporates Section 79 of the Limited Liability Company Act, allowing a DAO LLC to establish a series structure —effectively internal sub-entities— under which the debts and assets of one series are legally shielded from those of other series. The Act also clarifies that no additional reporting is required for each series beyond what is required for the DAO LLC as a whole.

Building on this statutory foundation, the RMI adopted further regulatory enhancements in 2023 subsequently introduced additional implementing regulations and adopted implementing regulations (the "DAO Regulations") to operationalize and supplement the 2022 DAO Act.[2090] Rather than repealing the original DAO Act,[2091] these measures supplemented and refined it by clarifying registration procedures,[2092] annual filing obligations, and compliance requirements,[2093] thereby streamlining

2082 Decentralized Autonomous Organization Act 2022, P.L. 2022-50, Bill No. 75ND2, 42d Const. Reg. Sess. (Marshall Is.), https://rmicourts.org/wp-content/uploads/2022/12/PL-2022-50-Decentralized-Autonomous.pdf [hereinafter Marshall Islands DAO Act].

2083 Non-Profit Entities (Amendment) Act 2021, P.L. 2021-39, Bill No. 53ND1, 42d Const. Reg. Sess. (Marshall Is.), https://rmicourts.org/wp-content/uploads/2021/12/P.L.-2021-39-NON-PROFIT-ENTITIES-AMENDMENT-ACT-2021.pdf.

2084 Marshall Islands DAO Act §§ 702(c), 704(1).

2085 Marshall Islands DAO Act §§ 705(3), 705(4).

2086 Marshall Islands DAO Act §§ 706(2), 710(1)(a), 715(1)–(2). These provisions collectively reflect the Act's recognition of on-chain governance, token-based membership, and the legal authority of smart contracts. Section 706(2) requires a DAO's formation documents to identify any smart contract directly used to manage its operations. Section 710(1)(a) provides that membership interests in a member-managed DAO are determined by governance token holdings at the time of a vote. Sections 715(1) and (2) confirm that a DAO's foundational documents and smart contracts serve as statements of authority and explicitly permit the use of blockchain, cryptocurrencies, and open-source code.

2087 Marshall Islands DAO Act § 712.

2088 Marshall Islands DAO Act §§ 705, 708, 713–714.

2089 Marshall Islands DAO Act § 703(3).

2090 Decentralized Autonomous Organization Regulations 2024, Republic of the Marshall Islands, 42d Const. Reg. Sess. (Marshall Is.), https://rmiparliament.org/cms/images/LEGISLATION/SUBORDINATE/2024/2024-0001/2024-0001_1.pdf [hereinafter Marshall Islands DAO Regulations].

2091 Marshall Islands DAO Regulations § 2(1).

2092 Marshall Islands DAO Regulations §§ 6, 8. Section 6 outlines the DAO formation process, requiring the registered agent to submit all formation documents—containing the information described in § 106(3) of the Act—via a secure upload portal or, if unavailable, by email in PDF format. Section 8 mandates the submission of a Beneficial Owner Information Report at formation and annually thereafter. This includes the data specified in § 112(2) of the Act and related verification documents, to be securely transmitted to the registered agent by each beneficial owner or, if none, an authorized representative member.

2093 Marshall Islands DAO Regulations § 15. This section grants the Registrar authority to enforce compliance with both the Act and the Regulations. Sanctions for violations may include a fine of up to $5,000 per violation, cancellation of the DAO's Certificate of Formation, or both—underscoring the legal weight of the regulatory framework and the consequences of noncompliance.

the overall regulatory environment.[2094] As a result, the Marshall Islands became one of the first jurisdictions to explicitly recognize DAOs as legal entities. This allowed DAOs to register as DAO LLCs. While the Marshall Islands' DAO LLC is technically a variant of the LLC form, it represents a more substantive adaptation than traditional "wrapper" approaches: the statute embeds core DAO features—such as on-chain governance, token-based membership, and smart contract execution—directly into the DAO LLC's legal framework, rather than simply layering blockchain elements onto a generic LLC structure. This approach gives DAOs legal personality, limited liability, and operational flexibility while preserving decentralized, on-chain governance.

7.3.1.E. Conclusion

Taken together, these legislative developments reveal a global trend toward the legal recognition of DAOs, though along divergent trajectories. In the United States, early state initiatives, such as Vermont's blockchain-based LLCs and Wyoming's DAO LLCs, relied on adapting the LLC form, while more recent statutes in Utah and New Hampshire introduced DAO-native legal structures directly inspired by the COALA DAO Model Law.[2095]

Parallel innovations abroad illustrate additional approaches. Malta initially adopted a comprehensive statutory framework through the Innovative Technology Arrangements and Services (ITAS) Act, but later shifted to a voluntary, administrative certification regime administered under the MDIA Act, emphasizing oversight, accountability, and technical audits without conferring legal personality or limited liability. By contrast, the Marshall Islands have created one of the most robust statutory regimes currently in force, explicitly recognizing DAOs as limited liability companies with on-chain governance, flexible tax treatment, and the possibility of series structures.[2096]

Collectively, these frameworks demonstrate both the opportunities and the fragmentation inherent in DAO regulation. While lawmakers increasingly seek to reconcile decentralized, code-driven governance with established legal principles, the diversity of approaches underscores the absence of harmonized standards. This patchwork leaves unresolved questions regarding interoperability, cross-border recognition, and the interaction of DAO-specific statutes with federal and international regulatory obligations. For instance, a DAO registered as a DUNA in Wyoming may face uncertainty when seeking to enforce contracts or hold assets in jurisdictions that do not recognize its legal status, while conflicting beneficial ownership requirements across U.S. state law and federal regulations like the Corporate Transparency Act create compliance challenges that no single jurisdiction has fully resolved.

Across both U.S. states and international jurisdictions, the influence of the Coalition of Automated Legal Applications (COALA) DAO Model Law is evident. Utah's DAO Act explicitly draws on COALA's proposals in designing a DAO-native entity form,[2097] while New Hampshire's DAO Act expands upon its principles by embedding quality assurance, transparency, and code

2094 Marshall Islands DAO Regulations § 14. This section modernizes the registration process by allowing all formation and related documents—including the Foreign Investment Business License (FIBL) application required under § 103(4) of the Act—to be submitted, signed, and delivered electronically. It further mandates that, by July 30, 2024, all relevant government agencies must accept digital payments (e.g., ACH, wire, credit card, or cryptocurrency), eliminating the need for in-person transactions during the DAO registration process.

2095 COALA DAO MODEL LAW, see *supra* note 1972.

2096 See Amaka Nwaokocha, *DAO Gets Legal Recognition in the US as Utah DAO Act Passes*, COINTELEGRAPH (Mar. 7, 2023), https://cointelegraph.com/news/dao-gets-legal-recognition-in-the-us-as-the-utah-dao-act-passes (noting Utah DAO Act "is based on the @coalaglobal DAO Model Law")

2097 UTAH CODE ANN. § 48-5-101 note (2024) (legislative findings); https://le.utah.gov/xcode/Title48/Chapter5/48-5-S101.html?v=C48-5-S101_2023050320240101; *see also* Jason Finger & Peter Cramer, *Part I: With New DAO Law on the Books, Utah Joins Race with Wyoming and Tennessee to Become U.S. "Crypto Capital"*, PROSKAUER ROSE LLP (May 25, 2023), https://www.blockchainandthelaw.com/2023/05/part-i-with-new-dao-law-on-the-books-utah-joins-race-with-wyoming-and-tennessee-to-become-u-s-crypto-capital/.

alignment requirements.[2098] Even where the Model Law is not expressly referenced, as in Wyoming and Vermont, its core themes —such as legal recognition of decentralized governance, limited liability for participants, and procedures for adapting smart contracts— resonate in legislative drafting.[2099] Malta's earlier ITAS Act and its successor certification regime likewise reflect themes later articulated in the COALA DAO Model Law, particularly the emphasis on accountability, oversight, and operational transparency. The Marshall Islands' DAO LLC framework closely parallels COALA's effort to integrate decentralized, on-chain governance within a purpose-built legal form. Taken together, these developments illustrate how the COALA DAO Model Law has served as a conceptual and practical blueprint, shaping diverse legislative experiments and encouraging policymakers to treat DAOs not merely as anomalous corporate variants but as organizations warranting bespoke legal recognition.

However, all enacted regimes have retained the requirement of a mandatory human-mediated gateway to legal recognition. Whether through an incorporator, organizer, filer, authorized person, or registered agent, a natural person (or a legally recognized entity acting through natural persons) must intervene at the moment a DAO acquires legal personality. No jurisdiction has adopted the COALA DAO Model Law's most radical feature: protocol-first legal existence without registration or human involvement. This structural choice reflects regulators' continued reliance on identifiable points of contact and accountability, even as they experiment with DAO-native entity forms.

7.3.2. Solving Conflict of Laws

Lawmakers and international organizations have begun addressing the complex issues of jurisdiction, forum, and applicable law in blockchain-related disputes.[2100] While questions of jurisdiction and forum determine which court may hear a dispute, conflict-of-laws rules address the distinct question of which substantive law should apply to transactions and proprietary relationships involving digital assets. Some states have amended existing statutes to enhance legal certainty, while others have pursued harmonization through soft-law instruments. The UNIDROIT *Principles of International Commercial Contracts* offers a neutral substantive framework that parties may expressly choose to govern their agreements.[2101] By selecting these principles, contracting parties can both reduce uncertainty about the applicable law and limit potential conflicts in cross-border transactions.

7.3.2.A. The Swiss Reform

Switzerland has opted for an early and detailed statutory approach, embedding blockchain-specific conflict-of-laws rules within its existing private international law framework. Switzerland offers one of the earliest and most detailed legislative models for resolving conflict-of-laws issues in digital-asset transactions. The 2020 reform of the Federal Act on Private International Law (PILA) introduced targeted provisions to clarify the treatment of distributed ledger-based assets:[2102]

2098 Keith Ammon & Bill Ardinger, *New Hampshire Has a Better Approach to DAOs,* COINDESK (Mar. 26, 2024), https://www.coindesk.com/opinion/2024/03/26/new-hampshire-has-a-better-approach-to-daos/.

2099 *See generally* Florence Guillaume & Sven Riva, DAO, *Code et Loi – Le Régime Technologique et Juridique de la Decentralized Autonomous Organization*, 10 Revue De Droit International D'assas (2021), https://ssrn.com/abstract=40137 (analyzing functional and regulatory equivalence principles in DAO legislation); Florence Guillaume & Sven Riva, *Model Law for DAOs – A Legal Regime Adapted to a New Type of Digital Company*, Lextech Inst. (Jan. 25, 2022), https://www.lextechinstitute.ch/model-law-for-decentralized-autonomous-organizations-daos/?lang=en.

2100 *See* Laila Metjahic, *Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*, 39 Cardozo L. Rev. 1533, 1536 (2018), https://cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf; Andrew W. Balthazor, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. Rev. 1207, 1209 (2019), https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1410&context=lawreview.

2101 Int'l Inst. For The Unification Of Priv. L. (UNIDROIT), Unidroit Principles Of International Commercial Contracts (2016).

2102 Bundesgesetz über das Internationale Privatrecht [Federal Act on Private International Law] Dec. 18, 1987, SR 291 (Switz.), https://www.fedlex.admin.ch/eli/cc/1988/1776_1776_1776/de.

- **Tokens representing claims (Article 145a PILA).** This article extends traditional conflict-of-laws rules on negotiable instruments to their digital equivalents, such as blockchain-based tokens. It applies to crypto-assets that represent claims (for example, certain asset-backed or claim-based stablecoins) or other tokens designed to place one or more receivables on a blockchain and render them tradable. It also applies to tokenized portfolios of mortgages, credit card receivables, or consumer loan claims. Under this provision, the issuer may designate the applicable law within the token itself.[2103] If no law is designated, the law of the statutory seat of the issuer —or if that cannot be determined, the issuer's principal place of business— governs.
- **Tokens representing goods (Article 106 PILA).** The same connecting factors apply to tokens representing physical goods, such as metals, diamonds, agricultural products, and other commodities. Thus, the applicable law is determined either by the choice of law expressed in the token or by reference to the issuer's statutory seat or principal place of business. However, this rule is subject to an important limitation: In the event of a priority dispute among multiple claimants asserting ownership over the underlying goods, the traditional *lex rei sitae* rule applies —that is, the law of the place where the goods are physically located prevails. This preserves classical property-law priorities where tangible assets are concerned.
- **Securities held with intermediaries (Article 108a PILA).** This provision clarifies the application of the *Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary*,[2104] (*Hague Securities Convention)*. It allows parties to select the governing law, provided the chosen jurisdiction is one in which the relevant intermediary maintains a branch. In the absence of such a choice, the applicable law defaults to the intermediary's principal place of business, reflecting the Place of the Relevant Intermediary Approach (PRIMA) established by the Convention. This approach preserves intermediary-based connecting factors that anchor legal relationships to identifiable market infrastructures.

These provisions collectively establish a coherent framework for tokenized assets within Swiss private international law. They recognize the technological specificities of digital tokens while preserving the hierarchy of traditional connecting factors where tangible assets or intermediated holdings are involved. Yet, as elsewhere, the broader question remains open: Are instruments such as the *Hague Securities Convention* adequate for digital assets? The Convention presumes the existence of identifiable intermediaries holding securities on behalf of clients, a model that sits uncomfortably with decentralized systems where assets are held directly on-chain without traditional custodial intermediaries. This tension between intermediary-based legal frameworks and disintermediated blockchain architectures remains a subject of ongoing scholarly debate.[2105]

2103 *Id.* at 205.

2104 Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary, July 5, 2006, Hague Conf. on Priv. Int'l L., https://finance.ec.europa.eu/publications/hague-convention-law-applicable-certain-rights-respect-securities-held-intermediary_en.

2105 *See generally* Florence Guillaume, *The Law Governing Blockchain-Based Intermediated Securities, in* Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law 269 (Andrea Bonomi, Matthias Lehmann & Shaheeza Lalani eds., 2019) (analyzing the compatibility of the Hague Securities Convention with DLT and arguing that the "relevant intermediary" concept may be difficult to apply in disintermediated blockchain networks).

7.3.2.B. The UNIDROIT Principles

Where Switzerland has pursued a national legislative solution, international organizations have instead promoted harmonization among countries through soft law. In 2023, the International Institute for the Unification of Private Law (UNIDROIT)[2106] adopted the *Principles on Digital Assets and Private Law* ("The *Principles*").[2107] Comprising 19 principles, the *Principles* are designed to be both technology-neutral and jurisdiction-neutral. They offer guidance to legislators, courts, and other stakeholders on transactions involving digital assets, including cryptocurrencies and non-fungible tokens (NFTs).[2108] The *Principles* also address core private law issues, such as control, transfer, custody, secured transactions, and insolvency.

Although the *Principles* constitute soft law, they may exert significant persuasive force. Legislatures may draw on their provisions when drafting national statutes; courts may rely on them to fill interpretative gaps; contracting parties may incorporate them into their agreements; arbitral institutions may use them as persuasive authority; and industry bodies may reference the *Principles* in guidelines, codes of conduct, or best practice standards.

1. Determining the Applicable Law

Principle 5, on Applicable Law, establishes a hierarchical ("waterfall") approach to identifying the governing law for digital assets that are inherently deterritorialized.[2109] It prioritizes party autonomy, allowing the applicable law to be expressly designated either within the digital asset itself (Principle 5(1)(a)) or in the system on which the asset is recorded (Principle 5(1)(b)). In the absence of such a designation, a default rule applies: The governing law is that of the statutory seat of the issuer, provided the seat is publicly and clearly ascertainable (Principle 5(1)(c)).

The "issuer" is narrowly defined as the person who introduces the asset "into the stream of commerce for value" and who publicly identifies both themselves and their statutory seat (Principle 5(2)(f)). This restrictive definition significantly limits the operation of the default rule, excluding, for instance, those who distribute digital assets through airdrops or those who fail to disclose a statutory seat, thereby deliberately reducing the practical reach of territorially anchored connecting factors.

Where no connecting factor can be identified, the *Principles* offer two fallback options:[2110]

- **Option A:** A legislature may specify the national law provisions that will govern proprietary issues regarding a digital asset, supplemented by the UNIDROIT *Principles* as gap-fillers; or
- **Option B:** A legislature may designate the UNIDROIT *Principles* as the governing law for such issues.

These options reflect a concerted effort to provide legal certainty, while acknowledging the limits of territorial connecting factors in situations where digital assets lack a clear link to any given jurisdiction.[2111]

2. Content of The *Principles*

The *Principles on Digital Assets and Private Law* apply only to digital assets capable of being placed under

2106 The International Institute for the Unification of Private Law (UNIDROIT) is an independent intergovernmental organization composed of 65 member states, with the mandate to harmonize and modernize private international law across its membership. The member states represent a diverse range of legal traditions and cultural backgrounds, reflecting a broad international consensus in its legal harmonization efforts.

2107 Int'l Inst. For The Unification Of Priv. L. (UNIDROIT), Digital Assets and Private Law Principles 2(2) (2023), https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf [hereinafter Digital Assets Principles].

2108 Digital Assets Principles Introduction paras. 16–20; *see also* Matthias Lehmann, *Digital Assets in the Conflict of Laws: A Comparative Search for the "Ideal Rule"*, Sing. J. Legal Stud. 1, 14 (2024), at 14, https://law.nus.edu.sg/sjls/wp-content/uploads/sites/14/2024/08/A0198_Matthias-Lehmann_1-26.pdf .

2109 Digital Assets Principles, *supra* note 2107, at princ. 5(1).

2110 *See* Digital Assets Principles princ. 5 cmt. 4; *see also* Digital Assets Principles Introduction paras. 28–33.

2111 Digital Assets Principles, *supra* note 2107, at 15-16.

"control."[2112] A person is deemed to have control when they can demonstrate the ability:

> a- to prevent others from obtaining substantially all of the benefits of the digital asset;
> b- to obtain substantially all of those benefits themselves; and
> c- to transfer control of the digital asset to another person.[2113]

The *Principles* recognize that digital assets may constitute the object of proprietary rights.[2114] This recognition implies that, in some jurisdictions, digital assets could be assimilated into existing categories of "property," while in other jurisdictions, legislative reform is needed to establish a distinct category capable of accommodating them. Such classification carries significant legal consequences, as it permits digital assets to be transferred, encumbered, and subjected to proprietary claims. The *Principles* deliberately refrain from imposing a uniform property classification, leaving this choice to national lawmakers.[2115]

The *Principles* further regulate two central commercial transactions: the transfer of proprietary rights[2116] and the creation of security rights. They specifically address both. First, the *Principles* establish an "innocent acquirer" rule: A transferee, acting in good faith, who meets certain conditions —including obtaining control of the asset— takes the asset free of competing proprietary claims.[2117] Second, the *Principles* provide that a secured creditor may perfect a security interest in a digital asset against third parties by obtaining control of that asset.[2118]

Taken together, Switzerland's Private International Law Act (PILA) and the International Institute for the Unification of Private Law (UNIDROIT) share a common goal: to provide legal certainty in transactions involving digital assets, while acknowledging the deterritorialized nature of distributed ledger technologies. They nevertheless embody distinct regulatory strategies: Switzerland integrates blockchain-specific rules into existing categories of private international law,[2119] while UNIDROIT promotes harmonization through specific principles.[2120] Each system attempts to balance party autonomy, legal certainty, and third-party protection, but their divergences highlight the continuing fragmentation of conflict-of-laws solutions in the digital asset space.[2121]

7.3.3. Frameworks for the Use of Technology

In certain jurisdictions, particularly within the European Union, new legal frameworks do not regulate blockchain technology *per se* but rather its principal use cases. The Data Act exemplifies this functional approach. Although it does not directly regulate smart contracts, it imposes specific technical and procedural requirements on their use in the context of data-sharing agreements. Likewise, the electronic Identification, Authentication and Trust Services (eIDAS) Regulation establishes a framework for electronic identification and trust services, including

2112 Digital Assets Principles, *supra* note 2107, at, princ. 2(2) (defining digital assets); Digital Assets Principles princ. 6 (defining control).

2113 Digital Assets Principles, *supra* note 2107, at princ. 6(1).

2114 Digital Assets Principle, *supra* note 2107, at princ. 3(1).

2115 Digital Assets Principles, *supra* note 2107, at princ. 3 cmt. 4.

2116 Digital Assets Principles, *supra* note 2107, at princ. 9(1).

2117 Digital Assets Principles, *supra* note 2107, at princ. 8(1).

2118 Digital Assets Principles, *supra* note 2107, at princ. 16(1).

2119 Bundesgesetz über das Internationale Privatrecht [IPRG] [Federal Act on Private International Law] Dec. 18, 1987, SR 291, art. 145a (Switz.), addressing the applicable law for digital assets by allowing a choice of law based on the text of the distributed ledger.

2120 Digital Assets Principles, supra note 2107, princ. 5.

2121 *See* Lehmann, *supra* note 2108, analyzing divergent approaches across jurisdictions and concluding that "a new gulf in the conflict of laws" has emerged.

digital identities that may be implemented through blockchain or other distributed-ledger technologies.

7.3.3.A. The Indirect Regulation of Smart Contracts: The EU Data Act

While some U.S. states have chosen to recognize smart contracts within existing electronic transactions frameworks *(See above section 6.5.2.A.1.)*, focusing primarily on their enforceability as private agreements, the European Union has taken a different regulatory path. The Data Act (Regulation (EU) 2023/2854)[2122] is not a smart contract law as such, but it nevertheless establishes specific requirements for their use when they are deployed in certain specific contexts (e.g. to automate data-sharing arrangements in the context of connected products and the Internet of Things).[2123]

The Data Act represents the European Union's effort to promote a competitive data economy in the context of connected devices and the Internet of Things. Manufacturers of industrial equipment, connected vehicles, smart home devices, agricultural machinery, and medical devices generate vast quantities of operational data through embedded sensors and connectivity features. Traditionally, these manufacturers retain exclusive control over device-generated data, preventing users —whether consumers or businesses— from accessing it or sharing it with competing service providers for repairs, maintenance, predictive analytics, or other value-added services. The Data Act seeks to rebalance control by granting users legally enforceable rights to access and share data generated through their use of connected products. Although the Act is not conceived as a dedicated framework for smart contracts, it expressly regulates their use when deployed as technical tools for automated data-sharing arrangements. It became fully applicable on September 12, 2025.

The Data Act imposes substantive obligations on manufacturers and data holders regarding what data must be made accessible to users, how data-sharing agreements must be structured, and what contractual terms are permissible. Moreover, and more importantly for this report, it imposes specific technical requirements on the design and operation of smart contracts used as technical tools to automate data-sharing arrangements.

1. Scope of the Data Act

The Data Act applies to manufacturers of connected products, such as the Internet of Things (IoT) devices, medical equipment, and connected vehicles. It also applies to providers of related services and to data processing service providers, including cloud and edge computing providers. And it covers public sector bodies in specific circumstances where access to data is required to respond to an exceptional need.

Within this framework, the technical requirements of the Data Act apply to actors whose activities involve the use or deployment of smart contracts for data-sharing purposes *(See section 4.4)*. This scope encompasses vendors and deployers of smart contracts insofar as those smart contracts are used to automate data-sharing arrangements.[2124] The regulatory burden thus falls on two categories of actors: (1) manufacturers and data holders

2122 The European Union Data Act (Regulation (EU) 2023/2854 entered into force on January 11, 2024, and became fully applicable on September 12, 2025. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023 O.J. (L 2023/2854), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854 [hereinafter Data Act]; Luca Olivieri et al., *European Union Data Act and Blockchain Technology: Challenges and New Directions*, *in* Proceedings of the 6th Italian Workshop on Blockchain and Distributed Ledger Technology 3 (2024), https://dlt2024.di.unito.it/wp-content/uploads/2024/05/DLT2024_paper_7.pdf; Gonzalo F. Gallego & Juan Ramon Robles, *EU Data Act (Part 8): Smart Contracts*, Hogan Lovells Engage (May 2, 2024), https://www.engage.hoganlovells.com/knowledgeservices/news/eu-data-act-part-8-smart-contracts.

2123 Luca Olivieri, et al., *European Union Data Act and Blockchain Technology: Challenges and New Directions*, 6th Distributed Ledger Technologies Workshop (DLT 2024) (2024), https://ceur-ws.org/Vol-3791/paper30.pdf; see *also* Sarah Legner & Anna Katharina Suzuki-Klasen, *Smart Contracts Under and Beyond the Data Act: Towards Legal Standards for Automated Contract Execution in Europe?* 14(5) Journal of European Consumer and Market Law, 225-234 (2025).

2124 Data Act, at art. 36(1) and recital 104.

who choose to automate their data-sharing obligations through smart contracts, and (2) the broader ecosystem of blockchain and software service providers who develop data-sharing automation tools for the internet of things (IoT) and connected products sector.[2125]

For example, if an automotive manufacturer develops an in-house smart contract system to automatically share vehicle diagnostic data with authorized repair shops when certain maintenance thresholds are reached, that manufacturer must ensure the system complies with the technical requirements. Similarly, a software company that sells a smart contract platform marketed to medical device manufacturers for automating patient data sharing must ensure its platform meets Article 36's technical standards. However, the Data Act does not extend to smart contracts used solely for internal purposes within a single organization, as such uses do not constitute data sharing within the meaning of the Act.

The Data Act defines a smart contract as a "computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering."[2126] The Regulation does not mandate any specific technological infrastructure for such programs. Instead, it adopts a technology-neutral approach encompassing any system capable of automatically executing the terms of a data-sharing agreement.[2127] Typical use cases involve connected products and automated data-sharing workflows and include Industrial IoT systems, connected vehicles, smart home devices, medical devices, and precision farming equipment. However, decentralized finance (DeFi) protocols, cryptocurrency transactions, and purely financial smart contracts generally fall outside the Regulation's material scope.

2. Regulatory Obligations Governing the Use of Smart Contracts

a. Substantive Obligations on Manufacturers and Data Holders

The Data Act requires data holders —typically manufacturers of connected products and providers of related services— to make accessible to users the data generated by the use of such products and services. The data must be made available to the users of the products and services and, under specified conditions, to third parties designated by the user.[2128] Products and services must be designed in a way that ensures data accessibility.[2129] Data sharing must be governed by a data-sharing agreement specifying key contractual terms, including confidentiality obligations, remuneration, the scope of data access, and other essential provisions. The tools used for automating data-sharing agreements, including smart contracts, must be interoperable.[2130]

b. Technical Requirements for Smart Contracts Under Article 36

When manufacturers, data holders, or third-party service providers choose to use smart contracts to automate the execution of data-sharing agreements, the Data Act

2125 Article 1(3)(g) explicitly brings within the scope of the EU Data Act "participants in data spaces and vendors of applications using smart contracts, and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement." Data Act, at art. 1(3)(g), 2023 O.J. (L 344) 1, 5; *also see* Data Act,, recital 104, 2023 O.J. (L 344) 1, 24.

2126 Data Act, at art. 2(39).

2127 *See* Data Act, recital 104 (stating that "the notion of 'smart contract' in this Regulation is technologically neutral").

2128 Gonzalo & Robles, *supra* note 2122.

2129 Data Act, at art 3(1) states "Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user".

2130 Data Act, at art 33(1)(d).

establishes a set of regulatory obligations governing the technical design of these smart contracts. Article 36 of the Data Act aims to ensure that automated data-sharing mechanisms are interoperable, reliable, equipped with appropriate access controls, and capable of being safely stopped or modified when necessary. Under Article 36(1), persons who use or deploy such smart contracts must ensure that they meet several essential requirements:[2131]

(1) Robustness and security: Smart contracts must be designed to operate reliably, prevent functional errors, and resist manipulation by third parties.[2132]
(2) Safe termination and interruption: Smart contracts must be equipped with safe termination and interruption mechanisms, allowing operations to be halted or reset when necessary to avoid unintended execution,[2133] including in cases of malfunction, legal disputes, cybersecurity risks, or revocation of consent.[2134]
(3) Data archiving and continuity: When a contract is terminated or deactivated, it must be possible to preserve transaction records, contract logic, and code to ensure auditability of past data processing.[2135]
(4) Access control: Strict governance-level and technical access controls must protect the smart contract from unauthorized use or modification. [2136]
(5) Consistency: The contract's execution must remain fully aligned with the terms of the underlying data-sharing agreement.[2137]

European standardization organizations have been developing harmonized technical standards specifying how these requirements should be implemented. As of January 2026, draft standards are under development through the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), with final adoption anticipated by late 2026. Once adopted, those who conform to these standards will benefit from a presumption of conformity with the essential requirements of the Data Act.[2138]

3. Challenges of Implementing the Data Act in the Blockchain Context

Scholars have discussed the definition of smart contracts adopted in the Data Act. This approach —which keeps the concept of a smart contract separate from that of a legal agreement— deviates from the path taken by several EU Member States, such as Malta.[2139] Legner and Suzuki-Klasen argue that this approach is preferable for any future, broader application of the notion of smart contracts beyond the Data Act.[2140] However, they note that recognizing smart contracts as potential legal agreements remains necessary —particularly in a consumer context— a step the Data Act does not take. According to the authors, this would require an EU-wide definition acknowledging the possibility that smart contracts may constitute legally binding agreements.

2131 Data Act, at art. 36(1).

2132 Data Act, at art. 36(1)(a).

2133 Data Act, at art. 36(1)(b).

2134 *See* Data Act, recital 104.

2135 Data Act, at art. 36(1)(c).

2136 Data Act, at art. 36(1)(d).

2137 Data Act, at art. 36(1)(e).

2138 Data Act, at art. 36(5).

2139 Art. 2(1) of the Malta Digital Innovation Authority Act, Cap. 591 (Malta), defines a "smart contract" as an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code. See Malta Digital Innovation Authority Act, Cap. 591, art. 2(1) (Malta), https://legislation.mt/eli/cap/591/eng/pdf; Christine Borg, *Understanding Smart Contracts: An Analysis of Their Nature, Effects and Enforcement in Terms of the Maltese Civil Code* 11, 14–15 (M.Sc. dissertation, Univ. of Malta 2020), https://www.um.edu.mt/library/oar/handle/123456789/73833.

2140 *See* Legner & Suzuki-Klasen, *supra* note 2123, at 234

Moreover, the implementation of the Data Act implies significant challenges, such as the interaction between smart contracts and data-erasure or revocation requests.[2141] The Act allows data holders, trade-secret holders, or users to request the erasure or disabling of data access when a data recipient has, for instance, obtained data through deceptive means, used it for unauthorized purposes, failed to maintain security safeguards, or altered technical protection measures.[2142] Designing smart contracts that can accommodate such reversibility requirements —without compromising data integrity or audit trails— is complex, particularly on immutable ledgers. The interaction between the Data Act and the General Data Protection Regulation (GDPR) creates additional complexity when personal data is involved.

An additional operational challenge is ensuring consistency between smart-contract logic and the evolving terms of data-sharing agreements.[2143] Smart contracts execute pre-programmed instructions automatically upon the occurrence of defined events, yet data-sharing relationships often require continuous adjustment and renegotiation. Translating dynamic contractual arrangements into code without loss of legal precision will therefore require robust governance and update mechanisms. Commentators have noted that, although vendors are responsible for ensuring such consistency, they cannot realistically meet this standard because they cannot anticipate in advance who will purchase or deploy their software.[2144] The consistency requirement should therefore be interpreted in a manner that accommodates this limitation.[2145]

Finally, the "kill-switch" requirement provided by Article 36(1)(b) implies that smart contracts must be equipped with a built-in mechanism which can "reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions."[2146] However, this requirement directly challenges blockchain immutability.[2147] Moreover, Recital 104 DA introduces an additional legal difficulty by conditioning termination on mutual consent —a requirement that may allow one party to block the activation of the kill switch and thereby force continued data sharing even where the legal basis for it has lapsed.[2148] Industry commentators and trade associations have expressed concern that the Data Act may conflict with the decentralized architecture and governance models of public blockchains.[2149]

4. The Proposed Repeal of the Data Act's Smart Contract Provisions

Recognizing these challenges, the EU Commission proposed in its Digital Omnibus package to repeal Article

2141 *See* Data Act, at art. 11(2)(a), Regulation (EU) No 2023/2854 (empowering data holders to request that a data recipient "erase the data made available" if the recipient provides false information, fails to implement security measures, or uses the data for unauthorized purposes).

2142 Data Act, at art. 11(3).

2143 *See* Data Act, at art. 36(1)(e), which requires smart contracts to possess "consistency" to ensure "consistency with the terms of the data sharing agreement."

2144 *See* Legner & Suzuki-Klasen, *supra* note 2123, at 228–229.

2145 *Id.* This challenge is compounded by the vendor-centric structure of Article 36. Vendors typically cannot foresee the specific data-sharing agreements for which their software will be used, meaning that the consistency requirement in Article 36(1)(e) can realistically only be satisfied with respect to standardized contractual clauses. Article 36(2) DA further complicates matters by leaving open when liability is triggered and which Member State's law applies, a gap that risks inconsistent national enforcement.

2146 Data Act, at art. 36(1)(b).

2147 Gonzalo & Robles, *supra* note 2122.

2148 *See* Legner & Suzuki-Klasen, *supra* note 2123, at 228.

2149 Gonzalo & Robles, *supra* note 2139; Veronika Renicker, *EU Data Act Smart Contract 'Kill Switch' Brings Uncertainty*, Cointelegraph (Aug. 23, 2023), https://cointelegraph.com/news/eu-data-act-smart-contract-kill-switch-brings-uncertainty; *EU Data Act Requires Smart Contracts to Have Kill Switch, Not Be Permissionless*, Ledger Insights (Mar. 14, 2023), https://www.ledgerinsights.com/eu-data-act-smart-contracts-immutability-permissionless/; Olivieri et al., *supra* note 2123; *Federico Casolari et al., How to Improve Smart Contracts in the European Union Data Act*, 2 Digit. Soc'y 9 (2023), https://www.researchgate.net/publication/371726750_How_to_Improve_Smart_Contracts_in_the_European_Union_Data_Act; Oshani Seneviratne, *The Feasibility of a Smart Contract "Kill Switch"*, Arxiv (July 14, 2024), https://arxiv.org/html/2407.10302v1.

36 of the Data Act.[2150] The Commission highlighted that industry stakeholders have raised concerns that Article 36's scope is unclear and may unintentionally capture a much wider range of DLT-based smart contracts, as well as ordinary software functionalities that merely automate data access but were not intended to fall within the Data Act's remit. A major criticism also relates to the core design of public blockchains, which rely on immutability, decentralization, and cryptographic transparency to ensure trust and security. Requiring built-in mechanisms to stop contracts or grant privileged access to specific actors would undermine these features, making permissionless blockchains harder to develop and potentially discouraging innovation. The Commission fears that imposing detailed regulatory requirements at the EU level risks locking in specific technological approaches and stifling innovation in a rapidly evolving field. As of January 2026, the proposed repeal of Article 36 remains under legislative consideration and has not yet been adopted.

Taken together, the adoption of the Data Act and the possible repeal of some of its provisions illustrate both the increasing legal recognition of blockchain technology and the persistent limits of regulating blockchain-based automation within existing regulatory paradigms. On the one hand, the Data Act expressly acknowledges smart contracts as a distinct technical object, defines their core characteristics, and subjects their deployment in specific contexts to detailed technical and governance requirements. On the other hand, the Commission's proposal to repeal Article 36 underscores the difficulty of drafting technically implementable obligations for decentralized infrastructures. The evolution of the Data Act thus suggests that blockchain technologies are regulable in principle, yet resistant to design-level mandates that conflict with foundational architectural features, such as immutability and decentralization. This tension complicates claims of blockchain alegality, while simultaneously revealing the practical constraints that continue to shape how far law can reach into the technical core of decentralized systems.

7.3.3.B. Recognizing Decentralized Identities (eIDAS)

Electronic identification and trust services in the European Union (EU) have been governed since 2014 by Regulation (EU) No 910/2014 on electronic identification, authentication, and trust services (eIDAS).[2151] In April 2024, the European Union substantially amended this framework through Regulation (EU) 2024/1183. Commonly referred to as "eIDAS 2.0." It established a more comprehensive and interoperable legal framework for digital identity and trust services across the EU.[2152] Its provisions apply progressively, with Member States required to make available at least one EUDI Wallet within 24 months of the entry into force of the relevant implementing acts (i.e., effectively by the end of 2026). Additional obligations, particularly for certain regulated private-sector relying parties, will apply at a later stage, notably from late 2027 onward.[2153]

While the core innovation of eIDAS 2.0 is the introduction of the EUDI Wallet, the Act also significantly expands the EU trust services framework by introducing electronic ledger services and granting "qualified electronic ledgers"

2150 *See* Commission Staff Working Document Accompanying the Documents Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), at 1.1.2.7, SWD(2024) 402 final (Nov. 27, 2024), https://data.consilium.europa.eu/doc/document/ST-15698-2025-ADD-2/en/pdf.

2151 Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 28.8.2014, pp. 73–114, http://data.europa.eu/eli/reg/2014/910/oj.

2152 The revised Regulation was published in the *Official Journal of the European Union* on April 30, 2024, and entered into force on May 20, 2024. Regulation (EU) 2024/1183 of the European Parliament and of the Council of Apr. 11, 2024, amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L (Apr. 30, 2024), http://data.europa.eu/eli/reg/2024/1183/oj.

2153 Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework, 2024 O.J. (L) 1183, https://eur-lex.europa.eu/eli/reg/2024/1183/oj [hereinafter eIDAS 2.0 Regulation]. eIDAS 2.0 Regulation, at arts. 5a(1), 5c, 5f.

a defined legal and evidentiary status. Together, these developments create new points of legal interface between EU digital identity policy and blockchain-based or distributed ledger technologies.

1. The European Union Digital Identity Wallet

The eIDAS 2.0 Regulation amends the original eIDAS framework to introduce the European Union Digital Identity (EUDI) Wallet, a tool designed to allow users to store and present a broad range of digital documents and attributes. The EUDI Wallet is designed to contain two categories of data. First, it includes a minimum set of Personal Identification Data (PID), defined as the core attributes necessary to uniquely identify a natural or legal person, issued by a competent authority designated by the Member State, such as national identity credentials. Second, the Wallet may also contain Electronic Attestations of Attributes (EAAs), which are cryptographically verifiable proofs of specific characteristics or entitlements, including driving licences, professional qualifications, academic diplomas, and other attestations issued by trusted public or private parties.[2154] These attestations function as "verifiable credentials" that enable selective disclosure of information.

The Wallet also supports the creation of qualified electronic signatures and seals, allowing users to sign documents and authenticate transactions with legal effect equivalent to handwritten signatures, where applicable.[2155] It is intended to function across borders and sectors, enabling access to both public services and private-sector applications.[2156]

a. The Provision of EU Digital Identity Wallets

Under Article 5a(1) of eIDAS 2.0, Member States must provide at least one EUDI Wallet free of charge to any citizen, resident, or business that requests one.[2157] Wallets may be issued directly by Member States or by certified private-sector entities authorized under national law. Such entities must comply with the harmonized requirements laid down in eIDAS 2.0 and its implementing acts.[2158] Several core implementing acts adopted in late 2024 set out high-level technical and security requirements[2159] and, in July 2025, additional acts addressed certification and conformity assessment.[2160] As a result, Member States must make a compliant wallet available by the end of 2026, with broader use expected to grow gradually thereafter. The European Commission will maintain a register of certified wallets and service providers to ensure transparency and cross-border recognition.[2161]

b. Acceptance obligations

One of the most significant provisions of eIDAS 2.0 is Article 5f,[2162] which establishes mandatory acceptance obligations for certain entities. Acceptance means that entities covered by the law must allow users to authenticate or identify themselves using the EUDI Wallet. If a user presents a valid wallet credential, the covered entity cannot require alternative identification methods.

2154 eIDAS 2.0 Regulation, recitals 6–8, 15; art. 5a(2).

2155 eIDAS 2.0 Regulation, at arts. 25, 26, 28, 35; *id*. recital 60.

2156 eIDAS 2.0 Regulation, recitals 7, 9, 46; arts. 5a(4), 6a.

2157 eIDAS 2.0 Regulation, at art. 5a(1).

2158 eIDAS 2.0 Regulation, at arts. 5a(3), 5c–5e.

2159 European Commission, *Implementing Regulation for European Digital Identity Wallets* (Dec. 4, 2024), https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-european-digital-identity-wallets (describing the Commission's adoption of five implementing regulations laying down rules for core functionalities and certification of European Digital Identity Wallets).

2160 eIDAS 2.0 Regulation, at arts. 5c(1), 5e(1); Commission Implementing Regs. (EU) 2024, OJ L (late 2024) (on technical and security requirements for EUDI Wallets); *see also* European Commission, *New Round of EU Digital Identity Wallet Implementing Regulations Adopted* (July 30, 2025), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/909706465/New+round+of+EU+Digital+Identity+Wallet+implementing+regulations+adopted.

2161 eIDAS 2.0 Regulation, at art. 5d(3).

2162 eIDAS 2.0 Regulation, at arts. 5c(f).

They must integrate the technical capability to read and verify wallet credentials and cannot discriminate against users choosing to authenticate via the Wallet.

The covered entities include:

- Member States that require electronic identification and authentication to access an online service provided by a public sector body,
- Private parties that rely on qualified trust services for identification or authentication purposes and are legally required under EU or national law to identify or authenticate users. This mandatory acceptance obligation, therefore, applies only where identification or strong authentication is required by law. It may cover entities such as banks and financial institutions (subject to anti-money laundering and know-your-customer requirements), healthcare providers (where patient identification is legally required), providers of age-restricted services (including alcohol sales, gambling platforms, and adult content websites), and crypto asset service providers authorized under MiCA *(See section 7.3.4.B.)*. Importantly, these sectors are covered only insofar as they are subject to binding legal identification requirements, rather than merely because they operate in a regulated sector.

Certain large online platforms regulated under the Digital Services Act (DSA) may also fall within the scope of Article 5f but only where EU law specifically requires user identification or strong authentication for access to particular services.

c. Privacy-Preserving Features and Selective Disclosure

A central feature of the EUDI Wallet is its emphasis on user control and privacy protection. The eIDAS regulation requires wallets be designed in accordance with privacy-by-design principle, enabling data minimization, selective disclosure of attributes, and protection against unnecessary linkability of transactions.[2163] According to the data minimization principles, the covered entities may request only the minimum attributes strictly necessary for their legitimate purposes. The regulation further recognizes that identification should not be required where it is not legally necessary, and it prohibits the systematic collection of full identity data in the absence of a legal obligation.[2164] Recital 60 explicitly provides that, unless required by other law, "accessing services by using a pseudonym should not be prohibited."[2165] The pseudonymity provisions, therefore, permit users to access services anonymously or pseudonymously unless specific legal obligations —such as anti-money laundering requirements in financial services— mandate identification.

The principle of selective disclosure allows users to share only the specific attributes necessary for a transaction, rather than revealing their complete identity profile. For example, when accessing age-restricted content, a user can present a cryptographic proof that they are over 18 years old without disclosing their exact birthdate, full name, address, or other identifying information. While eIDAS 2.0 itself does not mandate specific cryptographic techniques, its implementing acts, adopted in December 2024,[2166] establish technical specifications and explicitly reference international standards for wallet architecture and interoperability, including ISO/IEC 18013-5 (mobile driving license standard)[2167] and the W3C Verifiable

2163 eIDAS 2.0 Regulation, at art. 5a(4)(c)–(e); recitals 9, 12, 15, 59.

2164 eIDAS 2.0 Regulation, recital 60, 65; art. 5b(2)(d)

2165 eIDAS 2.0 Regulation, recital 60.

2166 Five implementing acts were adopted on November 28, 2024, and published in the *Official Journal* on December 4, 2024: Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 & 2024/2982, 2024 O.J. (L, 2024/2977) (Dec. 4, 2024).

2167 Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *ISO/IEC 18013-5:2021, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application* (2021).

Credentials data model.[2168] These standards are widely used within the self-sovereign identity (SSI) ecosystem and by decentralized identity projects *(See section 4.5)*, as they enable cryptographically verifiable credentials, selective disclosure, and decentralized trust frameworks.

While the EUDI Wallet features align closely with the SSI principles and decentralized identifier (DID) frameworks, eIDAS 2.0 maintains strict technological neutrality and does not mandate blockchain or distributed ledger technology as the underlying infrastructure.[2169] This leaves open whether the European digital identity ecosystem will evolve toward centralized state-operated systems, decentralized blockchain-based architectures, or hybrid models combining both.[2170]

2. Trust Services and Electronic Ledgers

The eIDAS framework establishes a harmonized regime for trust services that supports the security, integrity, and legal reliability of electronic transactions. Traditional trust services under eIDAS include qualified electronic signatures, qualified electronic seals for legal persons, qualified electronic timestamps, qualified website authentication certificates (QWACs), and qualified electronic registered delivery services.[2171] Trust service providers must obtain qualified status from a national supervisory authority, after which their services benefit from mutual recognition across the EU internal market.[2172]

The eIDAS 2.0 regulation expands this framework by introducing electronic ledger services as a new category of trust service. Recital 68 of the regulation defines electronic ledgers as "a sequence of electronic data records" that ensures data integrity and maintains a reliable chronological sequence, making the ledgers suitable for applications such as electronic voting and land registries.[2173] While the definition is technology neutral, it is widely understood to encompass certain blockchain-based or distributed ledger systems. Articles 45k and 45l of the regulation establish the legal effects of electronic ledgers. Article 45k(1) provides that records stored in an electronic ledger may not be denied legal effect or admissibility in legal proceedings solely on the grounds that they are in electronic form.[2174] Where the ledger qualifies as a *qualified electronic ledger* —that is, where it is operated by a Qualified Trust Service Provider (QTSP) in accordance with the requirements of eIDAS 2.0— entries recorded in the ledger benefit from a legal presumption of integrity and of accurate chronological ordering, according to Article 45k(2).[2175] Importantly, the legal presumption attached to qualified electronic ledgers concerns the integrity and ordering of records and does not extend to the substantive accuracy, legality, or lawfulness of the underlying data.[2176] As such, eIDAS 2.0 enhances evidentiary certainty for compliant ledger-based systems without displacing existing substantive legal rules.[2177]

Article 45l further sets out the conditions for qualified electronic ledgers by requiring that they "are created and managed by one or more qualified trust service

2168 *Verifiable Credentials Data Model v2.0*, W3C Recommendation (May 15, 2025), https://www.w3.org/TR/vc-data-model-2.0/.

2169 *See* eIDAS 2.0 Regulation, recitals 7, 9, 46 (emphasizing technological neutrality, interoperability, and flexibility of implementation and expressly avoiding the imposition of a single technical architecture).

2170 *Id*.

2171 Regulation (EU) No 910/2014 arts. 3, 25–44.

2172 Regulation (EU) No 910/2014 arts. 24–25, 30, 35, 40. A qualified trust service refers to a trust service that is compliant with the requirements of the eIDAS regulation.

2173 eIDAS 2.0 Regulation, recital 68.

2174 eIDAS 2.0 Regulation, at art. 45k(1).

2175 eIDAS 2.0 Regulation, at art. 45k(2); recital 56.

2176 eIDAS 2.0 Regulation, at 45k(2); recital 68.

2177 eIDAS 2.0 Regulation, recital 7; art. 45k.

providers;" "establish the origin of data records in the ledger;" "ensure the unique sequential chronological ordering of data records in the ledger;" and, "record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time."[2178] Compliance with these requirements is presumed where the ledger conforms to reference standards to be specified through implementing acts, as provided by Article 45l(3). In consultation with the European Committee for Standardization (CEN),[2179] the European Commission adopted Commission Implementing Regulation (EU) 2025/2531 on December 16, 2025.[2180] The Annex to this Regulation sets out the technical specifications and reference standards applicable to qualified distributed electronic ledgers.[2181] Qualified providers must document compliance in a publicly available "ledger practice statement." Together, these standards address blockchain-specific technical and governance requirements, including criteria for consensus mechanisms, node operation and governance, audit and logging obligations, and security specifications.

Qualified Trust Service Providers (QTSPs) wishing to operate qualified electronic ledgers must be legal entities established within the EU, employ reliable and technically competent persons in management positions, maintain sufficient financial resources to sustain operations and cover potential liabilities, and hold liability insurance or equivalent financial guarantees.[2182] Technical requirements include using trustworthy systems and products protected against unauthorized access and tampering, ensuring service continuity through redundancy and backup systems, implementing robust security measures to defend against cyberattacks, maintaining comprehensive audit logs of all system operations, and undergoing regular security audits by accredited conformity assessment bodies.[2183] Under Article 13 of eIDAS, QTSPs operating qualified electronic ledgers bear liability for damage caused by failure to comply with regulatory obligations. The burden of proof is on the QTSP, which must demonstrate either that it exercised due diligence and was not negligent or that the damage was caused by the actions of a third party beyond its control. This liability regime creates significant incentives for careful operation but also raises questions about insurance costs and the willingness of entities to assume QTSP status for blockchain-based ledgers.

Within this context, public permissionless blockchains such as Bitcoin and Ethereum may face structural obstacles to qualification because they lack identifiable operators who could serve as QTSPs and assume supervisory and liability obligations. The qualification model, therefore, structurally favors permissioned or consortium-based ledger architectures over fully decentralized networks. However, qualified status might be achieved through hybrid models

2178 eIDAS 2.0 Regulation, at art. 45l(1)–(2).

2179 *See* CEN/CENELEC JTC 19, *Blockchain and Distributed Ledger Technologies*, European Committee for Standardization, https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/emerging-technologies/.

2180 Commission Implementing Regulation 2025/2531, Laying Down Rules for the Application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as Regards Reference Standards and Specifications for Qualified Electronic Ledgers, 2025 O.J. (L 2531) (EU) https://eur-lex.europa.eu/eli/reg_impl/2025/2531/oj/eng. This Regulation entered into force on January 6, 2026.

2181 For all providers, the core applicable standard is ETSI EN 319 401 v3.1.1 (2024-06),which establishes general policy requirements for trust service providers, adapted to ledger services, ETSI, EN 319 401 v3.1.1, General Policy Requirements for Trust Service Providers (June 2024) https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf. This is complemented by ISO/IEC 15408:2022, Information Security, Cybersecurity and Privacy Protection – Evaluation Criteria for IT Security (2022), https://www.iso.org/obp/ui/en/#iso:std:iso-iec:15408:-1:ed-4:v1:en. and the EU Common Criteria–based cybersecurity certification scheme (EUCC), as implemented through Commission Implementing Regulations 2024/482 (Commission Implementing Regulation 2024/482, Laying Down Rules for the Application of Regulation (EU) 2019/881 of the European Parliament and of the Council as Regards the Adoption of the European Common Criteria-Based Cybersecurity Certification Scheme, 2024 O.J. (L 482) (EU), https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj/eng) and 2024/3144 (Commission Implementing Regulation 2024/3144, Amending Implementing Regulation (EU) 2024/482 as Regards Applicable International Standards and Correcting that Implementing Regulation, 2024 O.J. (L 3144) (EU) https://eur-lex.europa.eu/eli/reg_impl/2024/3144/oj/eng).

2182 eIDAS 2.0 Regulation, at art. 24(1)–(2).

2183 *Id.*

where a QTSP operates a notarization or anchoring service that references data in public blockchains while providing the qualified timestamp and certification layer.

3. European Blockchain Services Infrastructure (EBSI)

At the infrastructural level, the European Blockchain Services Infrastructure (EBSI)[2184] represents the European Union's flagship blockchain initiative. It provides a permissioned consortium blockchain infrastructure specifically designed for governmental and public-sector applications. It complements the eIDAS 2.0 framework by providing a pan-European, permissioned blockchain designed to support trusted digital public services. EBSI is operated through a decentralized network of nodes run by all EU Member States, the European Commission, and associated countries such as Norway and Liechtenstein.[2185] Governance is multi-stakeholder, with decision making distributed among participating government entities, ensuring that no single jurisdiction exercises unilateral control. The technical architecture is based on Hyperledger Besu,[2186] an enterprise-grade, Ethereum-compatible blockchain platform, utilizing a proof-of-authority consensus mechanism in which only pre-authorized validator nodes participate in block production and validation.

Institutionally, EBSI sits within Specific Objective 5 (Deployment and Best Use of Digital Capacities and Interoperability) of the Digital Europe Programme, which is a €8.16 billion strategic investment framework for digital infrastructure running through 2027.[2187]

The eIDAS 2.0 Regulation does not require the use of EBSI. However, EBSI has been developed with eIDAS 2.0 compliance as a design objective.[2188] Once technical standards for qualified electronic ledgers are fully adopted and stabilized, EBSI is a plausible candidate to apply for qualified status. Moreover, EBSI supports use cases closely aligned with eIDAS 2.0 objectives, including notarization services, verifiable credentials (such as digital diplomas), and secure cross-border data exchanges.

As of early 2026, EBSI has moved beyond purely experimental pilots and entered a phased deployment stage, with a limited number of services operating in controlled production environments while others remain in pilot form.[2189] Current use cases include:

- European Digital Credentials for Learning (Europass), through which universities issue digital diplomas as verifiable credentials anchored to EBSI, enabling instant verification by employers and other educational institutions without contacting the issuing university; participation has expanded to a growing number of universities across several Member States;[2190]
- notarization and timestamping services that provide cryptographic proof of the existence of documents at a given time, used for intellectual property protection, contract authentication, and evidentiary purposes;[2191]
- trusted data exchange between public authorities,

2184 European Commission, *European Blockchain Services Infrastructure (EBSI)* (2023), https://digital-strategy.ec.europa.eu.

2185 *Understanding EBSI's Blockchain Ecosystem*, EBSI Hub, https://hub.ebsi.eu/blockchain#:~:text=HyperLedger%20Besu,solution%20for%20the%20EBSI%20initiative (last visited Jan. 15, 2026).

2186 *Id*.

2187 European Commission, *Interim Evaluation of the Digital Europe Programme*, Commission Staff Working Document (Dec. 18, 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025SC0420.

2188 eIDAS 2.0 Regulation, at arts. 1, 45k–45l; recitals 6, 56.

2189 *See Eur. Comm'n: Digital Bldg. Blocks*, https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/474513483/About+us#:~:text=A%20new%20governance%20structure%20is,EBSI%20in%20its%20production%20phase (last visited Jan. 15, 2026), on formation of a new entity EUROPEUM-EDIC to support the deployment of successful EBSI pilots in its production phase.

2190 *European Digital Credentials*, EUROPASS, https://europass.europa.eu/en/european-digital-credentials (last visited Jan. 15, 2026).

2191 *Timestamp API*, EBSI Hub, https://hub.ebsi.eu/apis/pilot/timestamp (last visited Jan. 15, 2026).

notably in areas such as social security coordination,[2192] cross-border recognition of professional qualifications,[2193] and interconnection of business registries;[2194] and
- continued pilot projects on product traceability for medical devices and pharmaceuticals, primarily at proof-of-concept level.[2195]

EBSI remains controversial within parts of the blockchain community. Blockchain purists argue that EBSI is "not a real blockchain" because its permissioned architecture and governmental governance depart from the ideals of decentralization and censorship resistance that originally motivated public blockchain development.[2196] Privacy advocates also express concerns that a government-operated blockchain infrastructure could enable forms of surveillance or profiling, even where only metadata or cryptographic hashes — rather than full personal data — are recorded on-chain.[2197]

4. Assessment and Implications for Decentralized Identities

Rather than endorsing decentralization as a regulatory objective in itself, eIDAS 2.0 reflects a pragmatic governance approach: Decentralized technologies are legally recognized only to the extent that they can be integrated into a supervised, interoperable, and accountable framework for digital identity and trust services.

In practice, achieving qualified electronic ledger status requires the presence of an identifiable QTSP subject to regulatory supervision and liability. This institutional design appears structurally incompatible with genuinely decentralized, permissionless systems that lack any central operator capable of assuming legal responsibility. As a result, public blockchains such as Bitcoin or Ethereum are unlikely to qualify directly.

Finally, the interaction between mandatory EUDI Wallet acceptance and blockchain-based identity solutions remains uncertain. If the EUDI Wallet becomes the de facto standard for digital identity in the EU as a result of regulatory acceptance obligations, an important governance question arises: Will decentralized identity solutions based on public blockchain DIDs be able to coexist and compete on equal terms, or will they be structurally disadvantaged by the regulatory privileging of EUDI-compliant systems? The answer will significantly shape the future European digital identity ecosystem and the space available for private, open, and decentralized innovation.

Overall, under eIDAS 2.0, legal effects and evidentiary presumptions attach, not to decentralization as such but, to compliance with institutional requirements centered on qualified trust service providers, certification, and liability. eIDAS 2.0 thus confirms the difficulty of granting legal recognition to fully decentralized systems, while authorities tend to favor permissioned or

2192 *European Social Security Pass (ESSPASS)*, Eur. Comm'n: Emp., Soc. Affs. & Inclusion, https://employment-social-affairs.ec.europa.eu/policies-and-activities/moving-working-europe/eu-social-security-coordination/digitalisation-social-security-coordination/european-social-security-pass_en (last visited Jan. 15, 2026).

2193 *Resume Credentials Application*, Eur. Comm'n: Digital Building Blocks, https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/716149119/Resume+Credentials+Application (last visited Jan. 15, 2026).

2194 *Business Registers Interconnection System Dashboard*, Eur. Comm'n: Digital Building Blocks, https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/210798097/Business+Registers+Interconnection+System+dashboard (last visited Jan. 15, 2026).

2195 *Trace4EU: Battery Materials Traceability*, Eur. Comm'n: Digital Building Blocks, https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/716149466/Trace4EU+Battery+Materials+Traceability (last visited Jan. 15, 2026).

2196 *See Ethical Guidelines for Blockchain Systems*, Expert Grp. on Blockchain Ethics (EGBE), 3, 9 (May 2024), https://cryptoledgerlab.com/wp-content/uploads/2024/05/Ethical_Guidelines_for_Blockchain_Systems.pdf (distinguishing EBSI as a "private-permissioned" system).

2197 *See Scaling the EUDI Wallet: Lessons from the DC4EU Education and Social Security Pilots*, 3CL Found. (Jan. 20, 2026), https://www.3cl.org/beyond-dc4eu/ (acknowledging that while blockchain offers integrity, patterns in transactions can reveal sensitive metadata); *see also* Sarah Wynn, *SEC Chair Says Crypto Could Become "Powerful Financial Surveillance" Tool*, The Block (Dec. 15, 2025), https://www.theblock.co/post/382624/sec-chair-atkins-says-crypto-could-become-powerful-financial-surveillance-tool-sees-path-forward-without-giving-up-privacy (warning that if government steers blockchain architecture, it risks becoming a "financial panopticon" where every transaction is a reportable surveillance node).

hybrid configurations that can be aligned with existing governance and accountability structures.

7.3.4. Frameworks for the Regulation of Crypto-assets

While regulatory approaches to crypto-assets vary significantly across jurisdictions worldwide, some jurisdictions have adopted specific legislation to fill regulatory gaps, enhance legal certainty, and foster environments more conducive to technological development.[2198] In many of these jurisdictions, when a crypto-asset qualifies as a security or other recognized financial instrument, the existing framework applies; new rules are generally introduced only for assets that fall outside established categories.

The following sections examine Switzerland, the European Union, and South Korea. Switzerland illustrates a relatively light-touch approach: the Distributed Ledger Technology Act of 2021 ("DLT Act") was primarily confined to adapting existing financial frameworks to distributed ledger technology and crypto-assets. Other jurisdictions (presented in Appendices 17–21) have shown a similar tendency, modifying pre-existing securities or anti-money laundering legislation to accommodate digital assets. The European Union represents a more prescriptive model, having adopted the Markets in Crypto-Assets Regulation ("MiCA") in 2023 to establish a comprehensive framework for crypto-assets that are not already covered by financial law. South Korea, by contrast, demonstrates a more interventionist approach, with lawmakers acting rapidly to impose stricter oversight of crypto-asset markets in response to consumer protection concerns.[2199]

7.3.4.A. Switzerland

Like many countries, Switzerland does not have a comprehensive legislative framework that regulates crypto-assets (for a comprehensive presentation of the Swiss framework, *see Appendix 17*). A 2018 report by the Swiss Federal Council on the legal framework for blockchain and distributed ledger technology (DLT)[2200] concluded that the Swiss legal framework already addresses issues related to blockchain, although targeted legislative adjustments might be needed for legal certainty. As a result, various Swiss laws may apply. For instance, while the offering and sale of crypto-assets is not necessarily subject to Swiss financial market regulations, securities regulations apply where a crypto asset qualifies as a security.[2201]

1. Legal Categories

In 2018, faced with the need to determine which regulatory framework should apply to crypto-assets, the Swiss Financial Market Supervisory Authority (FINMA) issued its "Guidelines for enquiries regarding the regulatory framework for initial coin offerings."[2202] It remains a cornerstone of Swiss crypto regulation.[2203] This classification is indispensable for determining the

2198 For an overview of the jurisdiction-specific nature of crypto-asset regulation, see Atlantic Council GeoEconomics Center, *Crypto Regulation Tracker*, https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker/; *see also Markets in Crypto-Assets Regulation Tracker*, Latham & Watkins LLP, https://www.lw.com/en/markets-in-crypto-assets-regulation-tracker (last visited Jan. 15, 2026).

2199 Ella Fincken, *South Korea Pledges Tighter Crypto Regulations*, Global Legal Insights (Oct. 25, 2024), https://www.globallegalinsights.com/news/south-korea-pledges-tighter-crypto-regulations/

2200 Federal Council (Bern), *Legal framework for distributed ledger technology and blockchain in Switzerland - An overview with a focus on the financial sector*, (Dec 14, 2018), https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

2201 Under Swiss law, "securities" are defined as standardized instruments suitable for mass trading, including certificated or uncertificated securities, derivatives, and intermediated securities. The Federal Act on Financial Services (Financial Services Act, FinSA), art. 3(b), June 15, 2018, SR 950.1 (Switz.). Where a crypto asset qualifies as a security, its issuance or use may trigger regulatory requirements under Swiss financial market legislation, including the Financial Services Act (FinSA), the Financial Institutions Act (FinIA), and the Financial Market Infrastructure Act (FinMIA).

2202 Swiss Financial Mkt. Supervisory Auth. (FINMA), *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)* (Feb. 16, 2018), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf [hereinafter FINMA ICO Guidelines].

2203 For details on this categorization and the one in different financial markets acts, see Patrick Schärli, *Finanzmarktrechtliche Kategorisierung von Kryptowerten § 9, paras 9.04 et seq.*, *in* Kryptowerte (Corinne Zellweger Gutknecht, Dominik Tschudi & Kevin MacCabe eds., Helbing Lichtenhahn 2024).

applicable regulatory regime and for identifying possible gaps where existing legislation may not adequately address certain types of tokens.

FINMA distinguishes among several categories of crypto-assets and assesses whether they qualify as securities, based on their characteristics and functions:

- **Payment tokens,** such as bitcoin or ether, are meant to be used as a means of payment for acquiring goods or services or as a means for value transfer, either now or in the future.[2204] They are not treated as securities, since they do not grant holders any rights against an issuer or third party. Similarly, they are generally not considered financial instruments.[2205]
- **Utility tokens** grant digital access to a blockchain-based application or service.[2206] They are not considered securities if their only function is to provide such access and the utility is already usable at the time of issuance. However, if a utility token is also linked to investment purposes or capital market functions, it may take on the characteristics of an asset token and, therefore, fall within the scope of securities regulation.
- **Asset tokens** represent debt or equity claims against the issuer. They may entitle holders to future earnings or capital flows, similar to stocks, bonds, or derivatives. Tokens that enable trading of physical assets on a blockchain also fall into this category.[2207] They may be regarded as securities. This includes tokens representing uncertificated securities or derivatives that are standardized and suitable for mass trading. For instance, tokens that create future purchase claims in pre-financing scenarios could be treated as securities.[2208]
- **Stablecoins** may qualify as securities, depending on their structure. If a stablecoin is linked to underlying assets (such as commodities or securities) and grants holders contractual claims (redemption rights), it can be classified as a derivative or security under Swiss law.[2209] If a stablecoin merely serves as evidence of the token holder's ownership right, it generally does not qualify as a security. The key factor distinguishing stablecoins is that the underlying asset link primarily aims at price stabilization, rather than serving as an investment vehicle.[2210]
- **Hybrid tokens** combine characteristics of multiple categories, since these classifications are not mutually exclusive.[2211]

Swiss banking law uses the concept of "crypto-based assets" (*kryptobasierte Vermögenswerte*),[2212] as defined in the Federal Ordinance on Banks and Savings Institutions.[2213] These are assets that are *de facto* used (or intended by their issuer to be used) primarily as (i) payment instruments or (ii) instruments for money or

2204 *See* FINMA ICO Guidelines §3.1. Notable examples include Bitcoin, Bitcoin Cash, and Ether.

2205 For the definition of "financial instrument," *see* art. 3 lit. a FinSA; for the qualification, cf. FINMA ICO Guidelines §3.2.1.

2206 FINMA ICO Guidelines §3.2.2.

2207 FINMA ICO Guidelines §3.2.2

2208 FINMA ICO Guidelines §3.2.3.

2209 See the FINMA Supplement §2.2.

2210 FINMA Supplement §2.2.2.

2211 FINMA Supplement §2.2.2.

2212 Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV) [Ordinance on Banks and Savings Institutions], art. 5a, SR 952.02 (Switz.) (as amended Aug. 1, 2021) [hereinafter BO].

2213Verordnung über die Banken und Sparkassen (BankV) [Ordinance on Banks and Savings Institutions] of April 30, 2014, (SR 952.02), amendment in force as of August 1, 2021.

value transfer.[2214] This definition is particularly relevant in determining whether activities such as accepting, holding, or safeguarding such assets trigger licensing requirements under Swiss banking law.

On the whole, while Swiss law does not define terms such as "blockchain," "cryptocurrency," or "virtual currency,"[2215] it does rely on a functional, technology-neutral classification of crypto-assets grounded primarily in Swiss securities and financial market law. On October 22, 2025, the Swiss Federal Council launched a public consultation procedure in which it proposed the introduction of two new product categories: "crypto-based assets with a trading character" and "stable crypto-based means of payment."[2216]

2. The DLT Act

The legislative package commonly referred to as the "DLT Act," was adopted by the Swiss Federal Parliament on September 25, 2020, and entered into force in 2021.[2217] The Act introduced the new concept of "DLT securities" and a new licensing category called "DLT Trading Venue."[2218] The Act also provided clarifications on how crypto-based assets are treated in Swiss insolvency proceedings.[2219]

Overall, the DLT Act did not provide for a new framework for crypto-assets; it mostly aimed to modify existing laws to accommodate the characteristics of crypto-assets. The aim was to solve the most pressing issues raised by blockchain technology in the ambit of financial market law.[2220]

- **Ledger-Based Securities ("DLT Securities")**

A central innovation of the DLT Act was the introduction of ledger-based securities (often referred to in practice as "DLT securities") into the Swiss Code of Obligations.[2221] These securities constitute a fully electronic form of negotiable instrument designed to enable the tokenization of rights, claims, and financial instruments, such as shares, bonds, derivatives, and structured products, on distributed ledger systems.[2222] They provide a legal basis for the tokenization of assets.[2223] Because ledger-based securities may represent a wide range of underlying legal rights, certain asset tokens may be structured as ledger-based securities under Swiss law.[2224] By contrast, cryptocurrencies such as Bitcoin or *certain* stablecoins,[2225] which do not embody an underlying claim or membership right, cannot be issued as ledger-based securities.[2226]

2214 Art. 5a BO. Note that the category defined in Art. 5a BO represents a subcategory of "crypto-based assets in the broader sense," as the article itself explicitly states that it provides a definition of crypto-based assets in the sense of Art. 1b para. 1 lit. a Banking Act (Federal Act on Banks and Savings Institutions). *See* Bundesgesetz über die Banken und Sparkassen [Bankengesetz] [BankG] [Federal Act on Banks and Savings Institutions] Nov. 8, 1934, SR 952.0 (Switz.) (no official English translation available). Crypto-based assets that do not meet the requirements of Art. 5a BO trigger the authorization requirement under Art. 1a BO (the "normal" banking license).

2215 Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock, *Switzerland, in* GLI – Blockchain and Cryptocurrency Regulation 2025, 459 (Global Legal Grp. 2025).

2216 *See* Swiss Federal Council, *Federal Council moves forward with stablecoins and crypto: consultation launched*, (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY.

2217 Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act) of Sept. 25, 2020, AS 2021 33 (entered into force Aug. 1, 2021); *see also* Federal Council, *Der Bundesrat setzt DLT-Gesetz vollständig in Kraft und erlässt Verordnung* (June 18, 2021), https://www.news.admin.ch/de/nsb?id=84035.

2218 Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of June 19, 2015, (SR 958.1), arts. 73a–73o (as amended by the DLT Act).

2219 Federal Debt Enforcement and Bankruptcy Act (Bankruptcy Act) of April 11, 1889, (SR 281.1), arts. 242a–242b (as amended)

2220 For the reasoning behind this decision, see Federal Council, *supra* note 2217, 7–9, 45–47.

2221 Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of March 30, 1911, (SR 220), Art. 973d et seqq. CO.

2222 Dispatch to the DLT-Act, BBl 2020 233, at 309 et seqq.; furthermore, Haeberli, Oesterhelt & Wherlock, *supra* note 2215, at 461.

2223 Sandrine Chabbey, Stefan Kramer, *Switzerland paves the way for tokenisation of securities and introduces new DLT trading platforms*, IFLR (Sept. 14, 2021), https://www.iflr.com/article/2a63733ixysbvclr1awk3/switzerland-paves-the-way-for-tokenisation-of-securities-and-introduces-new-dlt-trading-platforms.

2224 Dispatch to the DLT-Act, BBl 2020 233, at 309 et seqq.

2225 However, stablecoins *can* be structured ledger-based securities, thereby certifying a directly transferable claim against the issuer.

2226 Dispatch to the DLT-Act, BBl 2020 233, at 309 et seq. Note, the Swiss Federal Council has opened consultation proceedings on a preliminary draft proposing the introduction of new statutory categories such as wertstabile kryptobasierte Zahlungsmittel (value-stable crypto-based means of payment), which would encompass certain types of stablecoins. See Swiss Federal Council, *Federal Council Moves Forward with Stablecoins and Crypto: Consultation Launched* (Oct. 22, 2025), https://www.sbfi.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY.

Ledger-based securities are recorded in a securities ledger that must meet statutory requirements,[2227] including ensuring that only the holders of the securities have control over their rights and that the integrity of the ledger is protected through appropriate technical and organizational measures. Issuers of DLT securities are responsible for ensuring that the register functions properly and that the protective measures remain effective.

- **DLT Trading Venues**

The DLT Act also amended the Financial Market Infrastructure Act (FinMIA) to introduce a new licensing category for DLT trading facilities.[2228] This regime allows trading venues to admit DLT-based securities and certain other crypto-based assets to multilateral trading, settlement, and custody within a single regulated infrastructure. In parallel, amendments to the Federal Debt Enforcement and Bankruptcy Act[2229] clarified the treatment of crypto-based assets in insolvency proceedings, including rules on segregation and access rights, thereby strengthening legal certainty for customers and custodians.

3. Sandbox Regulations

Switzerland has not adopted regulatory sandbox exemptions specifically tailored to distributed ledger technology or crypto-assets. Instead, it has pursued a technology-neutral, FinTech-friendly approach aimed at lowering barriers to market entry across the financial sector. This approach is commonly described as resting on three complementary pillars:

- **Public deposit:** Switzerland operates a limited "sandbox" exemption from banking licensing requirements. Under this regime, companies may accept public deposits without a banking license, provided that several strict conditions are met. Total deposits must not exceed CHF 1 million, must be non-interest-bearing, and must not be invested. Depositors must be explicitly informed in writing that the institution is not supervised by the Financial Market Supervisory Authority (FINMA) and that the deposits are not protected by deposit insurance.[2230] If the CHF 1 million threshold is exceeded, the institution must notify FINMA within ten days and apply for a banking license.[2231]
- **Settlement account exemption:** Swiss law provides an exemption for settlement accounts. Funds held by asset managers, securities firms, or comparable entities solely for the purpose of settling transactions are not treated as public deposits, provided that they are non-interest-bearing and transferred within 60 days.[2232] In the crypto asset context, FINMA has clarified that this exemption does not apply to cryptocurrency traders operating in a manner comparable to foreign-exchange dealers, thereby limiting its relevance for certain crypto-trading business models.[2233]
- **Simplified FinTech license:** Switzerland introduced a simplified FinTech banking license. This license allows institutions to accept up to CHF 100 million in public deposits,[2234] on the condition that the funds are

2227 See Art. 973d et seqq. CO, furthermore Art. 73d FinMIA, and Art. 58f et seqq. Ordinance on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Ordinance, FinMIO) of November 25, 2015 (SR 958.11).

2228 Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of June 19, 2015, (SR 958.1).

2229 Federal Debt Enforcement and Bankruptcy Act (Bankruptcy Act) of April 11, 1889 (SR 281.1) https://www.fedlex.admin.ch/eli/cc/11/529_488_529/de

2230 Art. 6 para. 2 BO.

2231 Art. 6 para. 4 BO.

2232 Art. 5 para. 3 lit. c BO.

2233 In detail, see Haeberli, Oesterhelt & Wherlock, *supra* note 2215, at 467.

2234 Art. 1b BA.

neither invested nor interest-bearing. License holders are prohibited from engaging in lending or mortgage activities, which has made the regime particularly suitable for certain payment and crowdfunding platforms.[2235] The Banking Ordinance (BO) provides for reduced requirements in areas such as capital, governance, and risk management to facilitate market entry.[2236] As this FinTech license has not been widely adopted, the Swiss Federal Council is proposing to introduce a bespoke license for "payment instrument institutions" that are stablecoin issuers.[2237]

4. Conclusion

Rather than introducing an entirely new regime for crypto-assets, Switzerland has selectively adapted existing laws to address the most pressing issues, such as securities tokenization, market infrastructure, and insolvency treatment.[2238] By building upon FINMA's token classification guidelines and adopting the DLT Act, Switzerland has adopted a functional framework for the issuance and trading of crypto-assets, particularly through the introduction of DLT securities and new licensing categories. Complementary FinTech-friendly measures —such as the sandbox exemption, settlement account exemption, and simplified FinTech license— further support innovation and reduce barriers to entry, even if they are not specifically tailored to DLT.

Beyond crypto-assets regulation, Switzerland lacks a specific legal framework for decentralized autonomous organizations (DAOs). The absence of DAO-specific legislation leaves significant gaps in legal certainty, compelling founders to rely on existing corporate forms or "legal wrappers" to mitigate liability risks. In practice, DAO founders risk classification as a *simple partnership* (*einfache Gesellschaft*),[2239] which entails joint and several liability that is personal, direct, and unlimited.[2240] To mitigate this risk, many Swiss founders rely on "legal wrappers," such as foundations or associations.[2241]

7.3.4.B. In the EU: Markets in Crypto-Assets Regulation (MiCA)

In the European Union, Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA)[2242] established a harmonized regulatory regime for crypto-assets and crypto-asset service providers. Compared with Switzerland —where lawmakers opted to adapt existing financial-market legislation (including through the Swiss DLT Act) rather than enact an entirely new and

2235 Haeberli, Oesterhelt & Wherlock, *supra* note 2215, at 467.

2236 Art. 7a, 8a, 14a et seqq. BO.

2237 See Swiss Federal Council, *Federal Council moves forward with stablecoins and crypto: consultation launched*, (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY, and the explanatory report (in German) https://cms.news.admin.ch/dam/en/der-schweizerische-bundesrat/bqoaKNhbpGcb/finig-erlaeuternder-bericht-de.pdf.

2238 Also see Haeberli, Oesterhelt & Wherlock, *supra* note 2215, at 458.

2239 *See* Swiss Code of Obligations (CO) of Mar. 30, 1911, SR 220, art. 530 (providing that a simple partnership (*einfache Gesellschaft*) arises where two or more persons combine their efforts or resources to achieve a common purpose, absent the formation of another legally recognized entity).

2240 *See* Swiss Code of Obligations (CO) of Mar. 30, 1911, SR 220, arts. 530, 544(3) (providing that partners in a simple partnership are jointly and severally liable with their entire personal assets); *see also* Andreas Furrer, *Privatrechtliche Haftungsfragen,* 6.58 et seqq, KRYPTOWERTE (Corinne Zellweger Gutknecht, Dominik Tschudi & Kevin MacCabe eds., Helbing Lichtenhahn 2024).; Eleonor Gyr, *Dezentrale Autonome Organisation DAO, Eine juristische Betrachtungsweise*, JUSLETTER (Dec. 4, 2017), https://jusletter.weblaw.ch/juslissues/2017/917/dezentrale-autonome-_ad06f55b2f.html__ONCE&login=false; Stephan D. Meyer, *Dezentrale autonome Organisationen (DAOs) und das Gesellschaftsrecht der Zukunft, 2013* AKTUELLE JURISTISCHE PRAXIS 319; Nina Reiser & Basil Wächli, *Rechtliche Erfassung von Dezentralen Autonomen Organisationen (Teil 1)*, 120 SCHWEIZERISCHE JURISTEN-ZEITUNG, 755, 757–60 (2024), https://www.sjz.ch/de/artikel/2504-0650-2024-0253/rechtliche-erfassung-von-dezentralen-autonomen-organisationen-teil-1; Benedikt Schuppli & Golnaz A. Jafari, *Piercing the Digital Veil: A Case Study for a DAO Legal Framework under Swiss Law* (Oct. 28, 2021) forthcoming J. INTELL. PROP., INFO. TECH. & E-COM. L. (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951804.

2241 See Rolf H. Weber, *Is there a need for regulation of DAOs in Switzerland?* in DECENTRALIZED AUTONOMOUS ORGANIZATIONS IN THE LEGAL LANDSCAPE 143 (Florence Guillaume & Sven Riva eds., Edward Elgar 2015).

2242 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance) OJ L 150, 40–205 (June 9, 2023), http://data.europa.eu/eli/reg/2023/1114/oj [hereinafter MiCA Regulation (EU) 2023/1114].

comprehensive regime— MiCA represents a more far-reaching and systematic regulatory approach.[2243]

While the following paragraphs primarily focus on MiCA, it is important to emphasize from the outset that MiCA constitutes only one component of a broader and multi-layered EU regulatory framework applicable to crypto-assets and distributed ledger technologies.[2244] In particular, crypto-asset activities are subject to the European Union's anti-money laundering and counter-terrorist financing framework. This framework includes the recast Transfer of Funds Regulation (EU) 2023/1113, which extended the "travel rule" to crypto-asset transfers,[2245] as well as the wider EU AML package.[2246] Regulation (EU) 2022/858[2247] established a pilot regime for market infrastructures based on distributed ledger technology (the DLT Pilot Regime) and provides a framework for the trading and settlement of financial instruments using DLT.[2248] Finally, the Digital Operational Resilience Act (DORA) established a harmonized and comprehensive regime for digital operational resilience within the European financial sector and applies to crypto-asset service providers.[2249]

MiCA itself applies to the issuance, public offering, and admission to trading of crypto-assets that fall

2243 In 2023, the United Kingdom took initial steps toward bringing stablecoin transactions within a regulatory framework through the Financial Services and Markets Act 2023. The Act grants the Treasury the power to designate digital settlement assets—including stablecoins used as a means of payment—as subject to regulatory oversight, and empowers the FCA and, for systemically important stablecoins, the Bank of England to supervise relevant firms once the assets are formally recognised. *See generally* Financial Services and Markets Act 2023, c. 29 (Eng.), https://www.legislation.gov.uk/ukpga/2023/29/contents. Building on this framework, on 15 December 2025 the Treasury laid before Parliament the draft *Financial Services and Markets Act 2000 (Crypto-assets) Regulations 2025*, which would bring a broad range of crypto-asset activities—including issuing qualifying stablecoins, operating trading platforms, and safeguarding crypto-assets—within the FCA's authorisation and supervision regime. As of the date of this report, the draft regulations had been laid before Parliament but had not yet been formally enacted; the regime is expected to come into force in October 2027. *See* The Financial Services and Markets Act 2000 (Crypto-assets) Regulations 2025 (draft), https://www.legislation.gov.uk/ukdsi/2025/9780348277586/contents. Finally, the *Property (Digital Assets etc) Act 2025*, which received Royal Assent on 2 December 2025, confirms the existence of a third category of personal property distinct from things in possession and things in action, into which crypto-tokens, NFTs, and potentially other digital assets may fall, while leaving the development of the boundaries and associated rights to the courts. *See* Property (Digital Assets etc) Act 2025, c. 19 (Eng.), https://www.legislation.gov.uk/ukpga/2025/29/enacted.

2244 The Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation, 2023 O.J. (L 2023/2226) 1, https://eur-lex.europa.eu/eli/dir/2023/2226/oj/eng [hereinafter DAC8] may also be noted as relevant here. This EU directive implements the OECD's Crypto-Asset Reporting Framework (CARF) from January 1, 2026, requiring Reporting Crypto-Asset Service Providers (RCASPs)—exchanges, brokers, wallet providers, and digital asset platforms—to collect, verify, and report crypto-asset transaction data, user tax residency information, and wallet addresses to EU tax authorities. As part of a broader global initiative endorsed by over 75 jurisdictions (including the UK, Canada, Australia, Singapore, and New Zealand), DAC8 and CARF establish an international crypto tax reporting framework aimed at enhancing transparency, enabling cross-border monitoring, and combating tax evasion in the crypto-asset sector.

2245 The EU's Recast Second Wire Transfer Regulation (EU) 2023/1113 (Recast WTR2) on information accompanying transfers of funds and certain crypto-assets is also known as the Recast Second Funds Transfer Regulation (Recast FTR2). It is in effect since June 29, 2023, and applies since 30 December 2024. It replaced the Second Wire Transfer Regulation (EU) 2015/847 (EU WTR2) to align with updated international standards published by the Financial Action Task Force (FATF), the global anti-money laundering AML/CTF regulation-setting body. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance), PE/53/2022/REV/1, OJ L 150, 9.6.2023, pp. 1–39, http://data.europa.eu/eli/reg/2023/1113/oj.

2246 In May 2024, the new EU AML package was formally adopted. It was published in the Official Journal of the EU on 19 June 2024, https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en It includes: Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, 2024 O.J. (L 2024/1620) [hereinafter AMLAR], https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 2024 O.J. (L 2024/1624) [hereinafter AMLR], https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng. Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, 2024 O.J. (L 2024/1640) [hereinafter 6AMLD], https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng; Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, 2023 O.J. (L 150) 1, https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng. After entering into force on July 9, 2024, the AML Regulation will apply directly from July 10, 2027. The Member states must transpose the directive by the same date.

2247 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R0858 [hereinafter DLT Pilot Regime].

2248 It creates a regulatory "sandbox," temporarily relaxing certain EU financial markets rules to allow firms to experiment with blockchain-based trading and settlement systems in a controlled environment. See DLT Pilot Regime, at arts 4-8.

2249 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act), 2022 O.J. (L 333) 1 [hereinafter DORA]. DORA imposes detailed obligations concerning the management of information and communication technology (ICT) risks, including internal governance and control mechanisms, incident detection and response, testing of digital resilience, and the oversight of third-party ICT service providers. See DORA, arts. 5–16 (ICT risk management and internal governance), arts. 17–23 (incident detection and reporting), arts. 24–27 (digital operational resilience testing), arts. 28–44 (ICT third-party risk management and oversight), https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

outside the scope of existing EU financial-services legislation,[2250] as well as to the provision of associated crypto-asset services. Its core objectives include closing regulatory gaps, enhancing investor and consumer protection, safeguarding the stability of the financial system, fostering innovation, and avoiding regulatory fragmentation across the internal market. MiCA entered into force on June 29, 2023. Its provisions on asset-referenced tokens and electronic money tokens have applied since June 30, 2024, while the remaining provisions, including the authorization and supervision of crypto-asset service providers, became applicable on December 30, 2024. Member States were required to establish authorization frameworks by these dates, and existing service providers benefited from transitional provisions allowing them to continue operations under pre-existing national licenses while applying for MiCA authorization. This grandfathering period extends until July 1, 2026, at the latest, subject to Member State discretion to shorten this period.

1. Scope

a. Crypto-assets that Do Not Qualify as Financial Instruments

MiCA defines crypto-assets as "digital representations of value or of rights that are able to be transferred and stored electronically using distributed ledger technology or other similar technology."[2251] It provides that regulators should adopt a "substance over form approach"[2252] when classifying crypto-assets. This means that they should be classified based on their features, not on the designation that their issuer assigns to them."[2253] MiCA also defines important notions, such as distributed ledger technology,[2254] asset-referenced tokens (ARTs, commonly referred to as "stablecoins"),[2255] which reference multiple assets or currencies, and e-money tokens (EMTs),[2256] which reference a single official currency. Most widely used fiat-backed stablecoins on the market (such as USDC and USDT) fall under the EMT category. Both categories are sometimes referred to collectively as 'stablecoins'.

MiCA applies only to crypto-assets that do *not* qualify as financial instruments governed by existing EU financial services legislation, including the revised Markets in Financial Instruments Directive (MiFID II).[2257] Implementing these provisions will be difficult: The determination of crypto-assets as financial instruments —particularly in relation to whether a token qualifies as a derivative— will require complex, case-specific analysis.[2258] The European Securities and Markets Authority (ESMA) is required to "issue guidelines on the

2250 Such as: Council Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU (Markets in Financial Instruments Directive II), 2014 O.J. (L 173) 349 [hereinafter MiFID II], https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng; Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the Prospectus to Be Published When Securities Are Offered to the Public or Admitted to Trading on a Regulated Market, and Repealing Directive 2003/71/EC, 2017 O.J. (L 168) 12 [hereinafter Prospectus Regulation], https://eur-lex.europa.eu/eli/reg/2017/1129/oj/eng; Council Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions, Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, 2009 O.J. (L 267) 7 [hereinafter Electronic Money Directive], https://eur-lex.europa.eu/eli/dir/2009/110/oj/eng.

2251 MiCA Regulation (EU) 2023/1114, art.3(1)(5).

2252 "When assessing and classifying crypto-assets, competent authorities should adopt a substance over form approach whereby the features of the crypto-asset in question determine the classification and not its designation by the issuer." MiCA Regulation (EU) 2023/1114, recital 11.

2253 *See* MiCA Regulation (EU) 2023/1114, recitals 8–9.

2254 'Distributed ledger technology' or 'DLT' means a technology that enables the operation and use of distributed ledgers; MiCA Regulation (EU) 2023/1114, art. 3(1)(1).

2255 'Asset-referenced token' means a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies. MiCA Regulation (EU) 2023/1114, art. 3(1)(6).

2256 'Electronic money token' or 'e-money token' means a type of crypto asset that purports to maintain a stable value by referencing the value of one official currency; MiCA Regulation (EU) 2023/1114, art. 3(1)(7). Electronic money tokens are included within MiCA's scope, but MiCA does not apply to central bank digital currencies.

2257MiCA Regulation (EU) 2023/1114, art. 2(4); *see also id.* recital 9.

2258 *See* MiCA Regulation (EU) 2023/1114, recital 9.

criteria and conditions for the qualification of crypto-assets as financial instruments" *(See below at 3)*.[2259]

b. Exclusion of NFTs

Although the European Commission's original proposal did not include non-fungible tokens (NFTs) within the scope of MiCA, the Commission engaged in extensive debate during the legislative process over the possible inclusion of NFTs.[2260] The final version of MiCA confirms that NFTs are not included, except where their features or intended uses effectively render them fungible or functionally equivalent to other crypto-assets.[2261] In such cases, competent authorities may need to assess, on a case-by-case basis, whether the NFTs in question are truly non-fungible.[2262]

c. Exclusion of Fully Decentralized Services

MiCA covers providers of services involving crypto-assets, as well as persons seeking to offer crypto-assets to the public in or targeting the European Union (EU) market. It also applies to persons seeking admission of such assets to trading on a crypto asset trading platform established in the EU or authorized as a crypto asset service provider (CASP) in a Member State.[2263] Services involving crypto-assets include but are not limited to custody of crypto-assets; operation of trading platforms; exchange services between crypto-assets and fiat currencies or other crypto-assets; execution of client orders; placement, reception, and transmission of orders; advisory services; portfolio management; and transfer services on behalf of clients.[2264]

Importantly, MiCA excludes from its scope crypto-asset services provided "in a fully decentralized manner without any intermediary."[2265] This exclusion is coherent with MiCA's design: MiCA is built around obligations imposed on crypto-asset service providers (CASPs), meaning legal or natural persons who can be *identified, supervised, and sanctioned*.[2266] It is designed to regulate the provision of services that resemble those offered by financial intermediaries —such as custody, trading platforms, or exchange services.[2267] Where no intermediary exists, the regulatory logic largely disappears. Above all, in a system that is genuinely decentralized —with no intermediary operating, controlling, or administering the service— there is no identifiable actor who could realistically be licensed, monitored, or held liable.[2268]

Without an intermediary, traditional supervisory mechanisms cannot function. It would be legally and practically inappropriate to extend licensing and compliance obligations to software code itself or to diffuse collectives of pseudonymous users. Legislators, therefore, sought to avoid creating obligations that could unintentionally criminalize or stifle open-source development, innovation, or the mere publication of code.[2269] By excluding "fully decentralized" systems, MiCA

2259 MiCA Regulation (EU) 2023/1114, art. 2a(3); *see also* ESMA, *Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments*, ESMA Doc. No. ESMA75453128700-1323 (Dec. 17, 2024), https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf

2260 MiCA Regulation (EU) 2023/1114, recital 10.

2261 MiCA Regulation (EU) 2023/1114, article 2(3).

2262 Jack Schickler, *MiCA, EU's Comprehensive New Crypto Regulation, Explained*, CoinDesk (2023), https://www.coindesk.com/learn/mica-eus-comprehensive-new-crypto-regulation-explained/ (last visited May 6, 2024).

2263 MiCA Regulation (EU) 2023/1114, arts. 2(1), 4, 59.

2264 MiCA Regulation (EU) 2023/1114, art. 3(1)(16).

2265 MiCA Regulation (EU) 2023/1114, recital 22.

2266 MiCA Regulation (EU) 2023/1114, arts. 3(1)(15), 59–60; recital 22.

2267 MiCA Regulation (EU) 2023/1114, recital 7; arts. 59–66.

2268 MiCA Regulation (EU) 2023/1114, recital 22.

2269 MiCA Regulation (EU) 2023/1114, recital 22.

draws a conceptual boundary between *regulated service provision by identifiable actors* and *protocols that operate autonomously*. In other words, MiCA is built to regulate *intermediaries*, not *software*.[2270]

At the same time, Recital 22 of MiCA makes clear that this exclusion is intended to be narrow and exceptional: If *any part* of the service is organized, controlled, or operated by a person or entity, MiCA applies. The interpretation and implications of this exclusion remain to be determined.[2271] Commentators emphasize that the exclusion is vague and difficult to apply in practice:[2272] What constitutes "fully decentralized"? Must a protocol exhibit zero human governance, no upgrade mechanisms, and no associated legal entity? What about decentralized autonomous organizations (DAOs) or token-based governance structures? What qualifies as an "intermediary" for MiCA purposes?

In practice, the threshold for "full decentralization" may be set so high that very few DeFi or smart-contract-based systems will qualify.[2273] Even protocols that present themselves as "decentralized" often retain upgrade keys, governance tokens, front-end interfaces, or other forms of de facto human control. Because of these hybrid architectures, many projects may fail to satisfy the "fully decentralized, no intermediary" criterion and may, therefore, fall within MiCA's scope or or require a crypto asset service provider license. For example, a system relying on a decentralized smart-contract backend but coupled with centralized governance structures or upgrade mechanisms would likely not benefit from the exclusion.

Rather than attempting to regulate blockchain protocols, supervisory authorities may concentrate on identifiable actors and operators, such as token issuers, governance administrators, or custodians. In practice, many protocols, such as Uniswap *(See Figure 28)* or MakerDAO *(See Figure 33)*, continue to rely on identifiable governance structures even if their core functions are executed through decentralized smart contracts. Only the most basic blockchain protocols —such as Bitcoin's base layer— might plausibly qualify for the exclusion, though even this remains uncertain given the presence of development communities and coordinated upgrade processes.

This exclusion could create a false sense of regulatory safety for DeFi actors. Project developers or governance participants may assume that building on autonomous smart contracts places them outside MiCA's reach, when in practice regulators may adopt a functional interpretation of "intermediary." Moreover, although MiCA is a harmonized EU regulation, national competent authorities —and potentially ESMA through guidance or supervisory convergence tools— will play a key role in interpreting whether a given protocol qualifies for the decentralization exclusion. Divergent interpretations during the early implementation phase could, therefore, generate legal uncertainty or temporary fragmentation across Member States.

2270 MiCA Regulation (EU) 2023/1114, recitals 7, 22; arts. 3(1)(15), 59.

2271 *See generally* Huseyin Oguz Genc, *Constructing an Evaluation Framework for Full Decentralization: A Case Study on DeFi's Stable Currency Issuance Services – CDP Protocols*, Stan. J. Blockchain L. & Pol'y (2023), https://stanford-jblp.pubpub.org/pub/cdp-protocols/release/1.

2272 António Garcia Rolo, *Out of scope, out of mind, and don't say decentralisation: brief remarks on the new MiCA regulation*, European Law Blog, (May 23, 2023), https://www.europeanlawblog.eu/pub/out-of-scope-out-of-mind-and-dont-say-decentralisation-brief-remarks-on-the-new-mica-regulation/release/1; Mikołaj Barczentewicz & André Gomes, *Crypto-Asset Market Abuse Under EU MiCA,* Eur. J. Risk Reg., 1-18 (2024), https://www.researchgate.net/publication/386105123_Crypto-Asset_Market_Abuse_Under_EU_MiCA; Dario Majorana, *UBI DAO IBI IUS?*, *in* Decentralized Autonomous Organizations—Governance, Technology, and Legal Perspectives: DAWO 2025143 (Michele Lustenberger, Florian Spychiger & Lukas Küng eds., Springer Proc. in Bus. & Econ. 2026), https://doi.org/10.1007/978-3-032-03273-7_9; PwC Legal, *Demystifying DeFi in MiCAR* (Oct. 8, 2024), https://legal.pwc.de/en/news/articles/demystifying-defi-in-micar (highlighting ESMA's view that the exact scope of the fully-decentralized exemption is uncertain and must be assessed on a case-by-case basis); BCAS, *Decentralisation under MiCA: the definitive handbook for DeFi* (Sept. 3, 2024), https://blog.bcas.io/decentralisation-under-mica-the-definitive-handbook-for-defi (discussing the indeterminate boundary between fully and partially decentralized arrangements and the implications for DAOs and governance tokens); Merkle Science, *Is DeFi truly exempt from MiCA regulations?* (June 19, 2024), https://www.merklescience.com/blog/is-defi-truly-exempt-from-mica-regulations (analysing the challenges of defining decentralisation and intermediaries under Recital 22).

2273 CMS Law, *DeFi and MiCA: How Much Decentralisation Is Enough?* (May 24, 2023), https://cms.law/en/prt/publication/legal-experts-on-markets-in-crypto-assets-mica-regulation/defi-and-mica-how-much-decentralisation-is-enough.

2. Requirements

a. Offering to the Public and Trading of Crypto-assets in the EU

Under MiCA, public offering of crypto-assets and their admission to trading on crypto-asset trading platforms within the European Union are subject to specific legal requirements.[2274] These requirements include the mandatory publication of a white paper that provides a detailed description of the offering or the request for admission to trading.[2275] MiCA also imposes conduct obligations on issuers of crypto-assets, requiring them to act honestly, fairly, and professionally.[2276]

b. Asset-References Tokens (ARTs)

Issuers of asset-referenced tokens must be legal entities established in the European Union,[2277] obtain authorization from a national competent authority of a Member State and publish a white paper that has been approved by the relevant authority.[2278]

To obtain MiCA authorization, ART issuers must also comply with a range of obligations, including requirements related to owning funds, governance structures, transparency, management of conflicts-of-interest, complaint handling mechanisms, the custody and investment of reserve assets, and business continuity planning.[2279]

The use of ARTs as a means of exchange is subject to quantitative restrictions. Where the quarterly average daily number of transactions exceeds one million Euros and the average daily value exceeds €200 million within a single currency area, issuers must suspend issuance and submit a remediation plan.[2280]

When ARTs are classified as "significant,"[2281] issuers are subject to more stringent obligations. ARTs may be classified as "significant" only where at least three criteria listed in Article 43(1) are met. Those include user base, reserve size, transaction volumes, cross-border usage, and systemic importance. Significant ARTs are subject to enhanced supervision by the European Banking Authority (EBA), higher capital requirements, more frequent reporting, and interoperability obligations.

c. Electronic Money Tokens (EMTs)

Issuers of electronic money tokens (EMTs)[2282] must be authorized as either credit institutions or electronic money institutions (with limited exceptions). They must comply with the applicable sectoral legislation,[2283] publish a white paper, and notify the relevant national authority.[2284] USD-denominated stablecoins, such as USDT and USDC, are typically classified as EMTs as they reference a single official currency.

EMTs may also be designated as "significant" under Article 43(1). "Significant" EMTs are also subject to enhanced supervisory and compliance obligations.[2285] Significant

2274 MiCA Regulation (EU) 2023/1114, arts. 4, 5, 16.

2275 MiCA Regulation (EU) 2023/1114 art. 4.

2276 MiCA Regulation (EU) 2023/1114, art. 14(1)(a).

2277 MiCA Regulation (EU) 2023/1114, art. 16(1)(a).

2278 MiCA Regulation (EU) 2023/1114 arts. 16(1), 17, 19.

2279 MiCA Regulation (EU) 2023/1114, art. 18.

2280 MiCA Regulation (EU) 2023/1114, art. 23(1)–(4).

2281 MiCA Regulation (EU) 2023/1114, arts. 43–45. The criteria for significance include, inter alia, whether the issuer is designated as a gatekeeper under the Digital Markets Act (Regulation (EU) 2022/1925), https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.

2282 MiCA Regulation (EU), 2023/1114 art. 16 et seqq.

2283 MiCA Regulation (EU), 2023/1114 art. 48(1)(a).

2284 MiCA Regulation (EU), 2023/1114 arts. 51–53.

2285 MiCA Regulation (EU) 2023/1114 arts. 56–58.

EMTs are supervised primarily at EU level by the European Banking Authority, with involvement of the European Central Bank (ECB) and relevant central banks, rather than by national central banks alone.

d. Crypto-assets Service Providers (CASPs)

Crypto-asset Service Providers (CASPs) must be authorized legal persons. Once authorized, they may operate across the EU without the need for additional authorizations.[2286] Authorized CASPs are subject to an extensive set of regulatory obligations, including organizational requirements, conduct of business rules, safekeeping of client funds, outsourcing controls, disclosure obligations, and prudential requirements, such as maintaining an adequate amount of their own funds and holding appropriate insurance coverage.[2287]

A "significant" crypto asset service provider is defined as one with a minimum of 15 million active users in the EU on an annual basis.[2288] Significant providers are supervised at the national level, but national competent authorities are required to report material supervisory developments to the European Securities and Markets Authority (ESMA).

e. Market Abuse Provisions

MiCA introduced a dedicated market abuse framework inspired by the EU Market Abuse Regulation (MAR).[2289] Unlike MAR, which applies only to financial instruments, MiCA extends market abuse rules to all crypto-assets within its scope, even when they do not qualify as securities. For crypto-assets admitted to trading on a crypto-asset trading platform, MiCA establishes specific safeguards. These include obligations to disclose inside information and prohibitions against insider dealing, unlawful disclosure of inside information, and market manipulation. Together, these rules aim to preserve market integrity and protect investors in crypto-asset markets.[2290]

f. Marketing Communications

MiCA imposed strict rules on marketing communications. Materials must be clearly identifiable, fair, balanced, and not misleading. Required disclosures include risk warnings, issuer identity, references to white papers, and fee transparency. These rules extend to social media, influencer campaigns, and online advertising.

3. Implementation

MiCA entered into force in June 2023 and became fully applicable on December 30, 2024. On February 13, 2025, several Delegated Regulations supplementing MiCA were published in the *Official Journal of the European Union.*[2291] Meanwhile, ESMA released two reports in March and July 2024 on MiCA technical standards.[2292] There, it noted that "ascertaining whether a service is provided in a partially decentralised manner or in a fully decentralised manner is not straightforward," while adding that "the risk of

2286 MiCA Regulation (EU) 2023/1114 art. 61.

2287 MiCA Regulation (EU) 2023/1114 arts. 59–60.

2288 MiCA Regulation (EU) 2023/1114 art. 85(1).

2289 Council Regulation 596/2014, 2014 O.J. (L 173) 1 (EU).

2290 MiCA Regulation (EU) 2023/1114, arts. 86–92.

2291 These include Regulatory Technical Standards ("RTS") specifying a number of requirements for white paper approvals and complaints handling. *See* Commission Delegated Regulation (EU) 2025/296, 2025 O.J. (L 296) (approvals), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0296; Commission Delegated Regulation (EU) 2025/294, 2025 O.J. (L 294) (complaints), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0294. In addition, on February 20, 2025, the RTS and Implementing Technical Standards ("ITS") concerning the obligation of certain financial entities to notify competent authorities of their intention to provide crypto-asset services, were published in the *Official Journal*. See Commission Delegated Regulation (EU) 2025/303, 2025 O.J. (L 303), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0303; Commission Implementing Regulation (EU) 2025/304, 2025 O.J. (L 304), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0304.

2292 ESMA, *Final Report– Draft technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – first package*, ESMA18-72330276-1634, (Mar. 25, 2024); https://www.esma.europa.eu/sites/default/files/2024-03/ESMA18-72330276-1634_Final_Report_on_certain_technical_standards_under_MiCA_First_Package.pdf; ESMA, *Final Report – Second Consultation Package under MiCA*, ESMA75-453128700-1229, (July 3, 2024), https://www.esma.europa.eu/sites/default/files/2024-07/ESMA75-453128700-1229_Final_Report_MiCA_CP2.pdf

malpractices is present with decentralisation as well."[2293] ESMA published its final guidelines on December 17, 2024, addressing key criteria, including whether crypto-assets constitute transferable securities, derivatives, or other financial instruments under MiFID II.[2294]

In July 2025, ESMA published the final version of its guidelines on supervisory practices to prevent and detect market abuse.[2295] The guidelines are intended for National Competent Authorities (NCAs) and include general principles for effective supervision and specific practices for detecting and preventing market abuse in crypto-assets. The European Union now plans to transfer supervision of cryptocurrency companies to ESMA as part of a set of measures to "fully integrate" financial markets.[2296]

Further implementation challenges stem from the necessity of aligning MiCA with other regulatory frameworks. The Digital Operational Resilience Act (DORA), which establishes a harmonized and comprehensive regime for digital operational resilience within the European financial sector, applies to crypto-asset service providers authorized under MiCA.[2297] The recast Transfer of Funds Regulation (EU) 2023/1113 incorporates into European Union law the Financial Action Task Force (FATF) "travel rule,"[2298] extending it to crypto-asset transfers.[2299] In force from December 30, 2024, it requires crypto-asset service providers to obtain, verify, and make accessible specific information concerning the originators and beneficiaries of crypto-asset transfers, irrespective of the transfer amount. It also mandates the implementation of effective procedures to identify and address missing or incomplete information and establishes particular rules for transfers involving unhosted wallets. Finally, the Pilot Regime Regulation (EU) 2022/858[2300] allows authorized DLT multilateral trading facilities, DLT settlement systems, and DLT trading-and-settlement systems —subject to predefined thresholds and scope limitations— to benefit from targeted exemptions or derogations from certain provisions of existing financial services legislation.

4. Conclusion

MiCA establishes a coherent and comprehensive regulatory framework for crypto-assets and related services. While it successfully integrates crypto-

2293 *Id*., *Final Report – Second Consultation Package under MiCA*, at 48. https://www.esma.europa.eu/sites/default/files/2024-07/ESMA75-453128700-1229_Final_Report_MiCA_CP2.pdf

2294 ESMA, *Final Report – Guidelines specifying Union standards on the maintenance of systems and security access protocols for offerors and persons seeking admission to trading of crypto-assets other than asset referenced tokens and e- money tokens*, (Dec. 17, 2024); https://www.esma.europa.eu/sites/default/files/2024-03/ESMA18-72330276-1634_Final_Report_on_certain_technical_standards_under_MiCA_First_Package.pdf.

2295 ESMA, *Final Report: Guidelines on supervisory practices to prevent and detect market abuse under the Markets in Crypto-Assets Regulation (MiCA)* (Apr. 29, 2025), https://www.esma.europa.eu/sites/default/files/2025-04/ESMA75-453128700-1408_Final_Report_MiCA_Guidelines_on_prevention_and_detection_of_market_abuse.pdf

2296 ESMA, *ESMA Welcomes Commission's Ambitious Proposal on Market Integration* (Dec. 4, 2025), https://www.esma.europa.eu/press-news/esma-news/esma-welcomes-commissions-ambitious-proposal-market-integration

2297 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("DORA") imposes detailed obligations concerning the management of information and communication technology (ICT) risks, including internal governance and control mechanisms, incident detection and response, testing of digital resilience, and the oversight of third-party ICT service providers.

2298 The "Travel Rule" is included in Recommendation 16 of the Financial Action Task Force (FATF), an international AML standards-setting body traditionally applicable to banks and wire transfers. It obliges covered intermediaries to collect, retain, and transmit identifying information about the originator and beneficiary of a transaction. In 2019, the FATF extended it to virtual assets and Virtual Asset Service Providers (VASPs). *See* Fin. Action Task Force, https://www.fatf-gafi.org/en/home.html (last visited Jan. 15, 2026); Financial Action Task Force Fin. Action Task Force, *FATF Recommendations* (as amended Oct. 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html

2299 The EU's Recast Second Wire Transfer Regulation (EU) 2023/1113 (Recast WTR2) on information accompanying transfers of funds and certain crypto-assets is also known as the Recast Second Funds Transfer Regulation (Recast FTR2). It has been in effect since June 29, 2023, and applied since December 30, 2024. It replaced the Second Wire Transfer Regulation (EU) 2015/847 (EU WTR2) to align with updated international standards published by the Financial Action Task Force (FATF), the global anti-money laundering AML/CTF regulation-setting body. See Regulation (EU) 2023/1113 of the European Parliament and of the Council of May 31, 2023, on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance), PE/53/2022/REV/1, OJ L 150, 9.6.2023, pp. 1–39, http://data.europa.eu/eli/reg/2023/1113/oj.

2300 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (DLT Pilot Regime), https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng.

asset activities that resemble traditional financial intermediation, it also exposes the limits of a regulatory model premised on the existence of identifiable intermediaries. By excluding crypto-asset services provided "in a fully decentralized manner without any intermediary," MiCA deliberately leaves genuinely permissionless and autonomous systems outside its core regulatory perimeter. Protocols that operate through self-executing smart contracts, without a controlling entity or operator, cannot be readily subjected to licensing, supervisory, or sanctioning mechanisms designed for legal or natural persons. As a result, the most innovative forms of decentralized finance (DeFi) do not fit neatly within MiCA's framework and continue to operate amid significant legal uncertainty at the EU level.

For the protocols and entities within its scope, MiCA promotes investor protection, market integrity, financial stability, and consumer transparency. It imposes detailed disclosure obligations on issuers and crypto-asset service providers, including requirements to specify governance arrangements and token allocations. By mandating transparency regarding governance structures and token distributions, MiCA may help to mitigate the excessive concentration of control that can arise within blockchain protocols *(See above section 6.2.1.B.)*. In this sense, the regulation can be understood as contributing —albeit incidentally— to the preservation of viable forms of decentralized governance in blockchain ecosystems.[2301]

Finally, like other European tech regulations, MiCA is implemented through standards and guidelines adopted by European Standardization Organizations, (CEN, CENELEC, ETSI),[2302] European regulators (EBA, ESMA, ECB),[2303] and by national regulators.[2304] These standards and guidelines are developed together with operators, using tools such as sandboxes and pilots.

7.3.4.C. Strict Oversight: South Korea

South Korea represents a model of stringent supervision: Rather than prohibiting crypto-assets outright or liberalizing market access, it has subjected the sector to stringent ex ante oversight while progressively channeling participation through regulated institutional pathways. Notably, it prohibited initial coin offerings (ICO) primarily through supervisory guidance and administrative measures, rather than through comprehensive primary legislation.

South Korea's regulatory oversight of crypto-assets began in earnest in 2017, when the Financial Services Commission (FSC) prohibited domestic ICOs and warned that cryptocurrency exchanges could face closure for failures to protect investors. [2305] From 2017 to 2025, the country has combined a restrictive approach to token issuance with a progressively more detailed supervisory regime for crypto-asset service providers. Simultaneously, it has supported blockchain innovation through public sector pilot programs and private sector initiatives.[2306]

In January 2026, the FSC finalized guidelines lifting the nine-year ban on corporate cryptocurrency investments,

2301 See MiCA Regulation (EU) 2023/1114, recital 7; *see also* Hanna Halaburda, *The Hidden Danger of Re-Centralization in Blockchain Platforms*, Brookings, (Apr. 10, 2025), https://www.brookings.edu/articles/the-hidden-danger-of-re-centralization-in-blockchain-platforms/.

2302 European Committee for Standardization, European Committee for Electrotechnical Standardization, European Telecommunications Standards Institute

2303 European Banking Authority, European Securities and Markets Authority, European Central Bank

2304 F. Bassan, *Digital Platforms and Blockchains: The Age of Participatory Regulation*, 34 Eur. Bus. L. Rev 7, 1103-1132 (2023), https://www-sciencedirect-com.stanford.idm.oclc.org/topics/computer-science/digital-platform.

2305 Arjun Kharpal, *South Korea Bans All New Cryptocurrency Sales*, CNBC (Sept. 28, 2017), https://www.cnbc.com/2017/09/28/south-korea-bans-all-new-cryptocurrency-sales.html.

2306 Ministry of Science and ICT, *Korea Plans to Adopt Blockchain in Seven Sectors with a Goal to Promote Decentralized Identifiers (DIDs)* (June 24, 2020), https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=441&se.

allowing listed companies and professional investors to allocate up to 5% of equity capital to approved digital assets, provided transactions are routed through regulated domestic exchanges.[2307] The FSC has also endorsed self-regulatory efforts, such as the Digital Asset Protection Foundation, and published roadmaps for stablecoins and spot-crypto exchange-traded funds (ETFs), and it has expanded venture support for crypto startups.[2308] Together, these initiatives form part of South Korea's broader "digital-assets roadmap" which, as of early 2026, aims to transition to a proactive "institutional integration" phase.

1. Regulation of ICOs, Cryptocurrencies, and Exchanges

Following the 2017 blanket ban on initial coin offerings, the FSC, in January 2018, introduced a real-name verification system for cryptocurrency trading.[2309] This system prohibits anonymous transactions and requires all trading accounts to be linked to verified bank accounts, thereby reinforcing anti-money-laundering (AML) and know-your-customer (KYC) obligations.[2310] By requiring exchanges to secure formal partnerships with domestic commercial banks, the real-name system effectively integrated crypto trading platforms into the traditional financial sector, while significantly narrowing the number of exchanges able to operate lawfully.

Retail cryptocurrency trading remains lawful but is restricted to exchanges operating under strict regulatory supervision. Registered exchanges must comply with enhanced AML/KYC requirements, maintain transactional monitoring systems, and cooperate closely with financial authorities. In addition, regulators adopted a cautious stance toward exchange conduct: Exchanges are prohibited from trading their own tokens or affiliated tokens and remain subject to limits on proprietary activities.[2311] Regulatory authorities also began, through guidance rather than statute, to allow certain tightly circumscribed transactions involving crypto-assets. One example is the limited conversion ("cash-out") of crypto holdings into fiat currency by eligible entities for operational or liquidation purposes, subject to stringent conditions relating to liquidity, transparency, and conflict-of-interest avoidance.[2312]

2-.The South Korean "crypto law"

In July 2023, South Korea's National Assembly enacted the *Act on the Protection of Virtual Asset Users (VAUPA)*, which entered into force in July 2024.[2313] The Act constitutes South Korea's first dedicated statutory framework governing crypto-assets and applies to all registered virtual asset service providers (VASPs). Rather than regulating token issuance or specific asset categories, the Act focuses on user protection, market integrity, and supervisory enforcement. Crypto-assets that qualify as securities fall within the scope of the Financial Investment Services and Capital Markets Act (FSCMA), while other virtual assets are governed by VAUPA. Certain categories, such as non-fungible tokens

2307 James Field, *South Korea sets 5% cap on corporate digital asset investments*, CoinGeek (Jan. 15, 2026), https://coingeek.com/south-korea-sets-5-cap-on-corporate-digital-asset-investments/.

2308 Fin. Servs. Comm'n (S. Kor.), *Virtual Asset User Protection Act Enforcement and Future Roadmap* (July 17, 2024) (outlining the next phases of regulation including stablecoins), https://www.fsc.go.kr/eng/pr010101/81217; *see also* Lee & Ko, *Phased Corporate Access to Virtual Asset Markets: FSC Announces Roadmap for Corporate Participation in Crypto Markets* (Feb. 13, 2025), https://www.lexology.com/library/detail.aspx?g=3b205962-9319-40dd-bed0-534c3d3102fb&utm_source.

2309 *See* Fin. Servs. Comm'n (S. Kor.), *Measures to Curb Speculative Cryptocurrency Trading* (Sept. 2017) (announcing ICO ban); Fin. Servs. Comm'n (S. Kor.), *Introduction of Real-Name Verification System for Virtual Asset Trading* (Jan. 2018); *see also* Reuters, *South Korea to Ban Cryptocurrency Traders from Using Anonymous Bank Accounts*, CNBC (Jan. 22, 2018), https://www.cnbc.com/2018/01/22/cryptocurrencies--south-korea-announces-real-name-account-rules.html.

2310 *See* Act on Reporting and Using Specified Financial Transaction Information, Act No. 15571, arts. 5–6 (S. Kor.), as amended (applying AML/KYC obligations to virtual asset transactions); *see also* Fin. Servs. Comm'n (S. Kor.), *Guidelines on Real-Name Accounts for Virtual Asset Trading* (2018).

2311 Fin. Servs. Comm'n (S. Kor.), *Guidelines for Virtual Asset Disposal by Virtual Asset Exchanges*, (May 2025), https://www.fsc.go.kr/eng/pr010101/84489?srchCtgry=&curPage=3&srchKey=&srchText=&srchBeginDt=&srchEndDt=. (implemented June 2025).

2312 *Id.*; *see also* Fin. Servs. Comm'n (S. Kor.), *Digital Asset Protection Foundation to be Set Up to Ensure Safe Return of User Funds from Closed Down VASPs* (Sept. 25, 2024), https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=83126&type=N&insttCode=A260302.

2313 Act on the Protection of Virtual Asset Users, Act No. 19563, July 18, 2023, (S. Kor.), https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=63752&type=part&key=23.

(NFTs), may fall outside the regime where they do not exhibit investment characteristics, although this remains subject to case-by-case recharacterization. Stablecoins, for their part, occupy a more ambiguous position, with regulators adopting a case-by-case approach pending further regulatory clarification.

VAUPA grants explicit supervisory and investigative powers to the Financial Services Commission and imposes a set of core obligations on VASPs,[2314] including:

- segregation of customer assets from proprietary funds, with fiat deposits held at regulated financial institutions;
- robust custody and safekeeping obligations for customer virtual assets, including requirements — elaborated through enforcement guidance— that a substantial portion of such assets be held offline in secure custody arrangements;
- the adoption of measures, such as insurance or reserve mechanisms, to cover liabilities arising from cybersecurity incidents;
- record-keeping and transaction-monitoring obligations; and,
- mandatory reporting of abnormal or suspicious transactions.

The Act also establishes a statutory basis for the supervision and sanctioning of unfair trading practices, including insider trading, market manipulation, and the misuse of non-public information. The FSC is empowered to impose administrative sanctions, conduct on-site inspections, and refer cases for criminal investigation where appropriate.

3. Institutional Participation and Proposed Reforms (2025 roadmap)

In parallel with the implementation of the 2023 Act, South Korean authorities have signaled their intention to expand institutional participation in cryptocurrency markets through a gradual, risk-based approach. In early 2025, the FSC announced a phased roadmap under which corporate real-name accounts would initially be permitted for narrowly defined purposes, particularly liquidation or conversion of crypto-assets into fiat currency.

Phase 1 of this roadmap covers certain law-enforcement and public agencies, non-profit organizations, universities, and virtual-asset exchanges. A subsequent phase is envisaged to extend participation to listed companies and other "professional investors," subject to reinforced internal-control and compliance requirements. As part of Phase 1, the FSC's Virtual Asset Committee finalized guidelines in May 2025 (implemented beginning in June 2025)[2315] that allow eligible non-profit organizations to receive and dispose of donated virtual assets under strict conditions.[2316] These include: an operating history of at least five years; external audits with appropriate audit opinions for the past three years; the establishment of an internal pre-review or compliance committee; and a policy of converting donated crypto into fiat currency without undue delay. The donated virtual assets must be those traded in at least three Won-denominated exchanges.[2317]

These conditions are designed to ensure liquidity, mitigate reputational and governance risks, and prevent speculative or opaque asset exposure. In January 2026, amendments were made to South Korea's capital markets legislation to institutionalize "Security Tokens" (ST) by recognizing

2314 *Id*. arts. 6–9.

2315 Fin. Servs. Comm'n (S. Kor.), *Guidelines for Virtual Asset Disposal by Virtual Asset Exchanges*, (May 2, 2025), https://www.fsc.go.kr/eng/pr010101/84489?srchCtgry=&curPage=3&srchKey=&srchText=&srchBeginDt=&srchEndDt=.

2316 Fin. Servs. Comm'n (S. Kor.), *Sale of Virtual Assets by Non-profit Corporations and Exchanges Will Be Allowed From June* (May 2, 2025), https://www.fsc.go.kr/eng/pr010101/84489.

2317 Lee Yeon-woo, *Nonprofits, crypto exchanges allowed to sell crypto from June 1*, The Korea Times (May 1, 2025), https://www.koreatimes.co.kr/economy/cryptocurrency/20250501/nonprofits-crypto-exchanges-allowed-to-sell-crypto-from-june-1

distributed ledgers as legally valid securities registries and authorizing qualified entities to act as "Issuance Account Management Institutions."[2318] These amendments further illustrate South Korea's strategy of embedding tokenized finance within existing capital-markets law, rather than creating a fully autonomous digital-asset regime.

4. Conclusion

South Korea has established one of the most strictly supervised crypto-asset regulatory regimes among advanced economies. It reflects a model of intensive financial supervision: Authorities impose stringent anti-money-laundering controls, tightly regulate exchanges, and permit institutional participation only gradually, while progressively embedding these safeguards in statutory law. The framework deliberately curbs speculative excesses and conflicts of interest. At the same time, policymakers have avoided a general prohibition on blockchain innovation, opting instead for an incremental and tightly managed regulatory strategy. More ambitious reforms —such as the introduction of a comprehensive digital-asset framework law, dedicated regulation of stablecoins, or the approval of spot-crypto exchange-traded funds— remain under discussion or at the roadmap stage. Recent measures indicate, however, a calibrated shift from defensive supervision toward structured market integration, while maintaining a high degree of regulatory control.

7.4. PROHIBITIONS AND RESTRICTIONS

Some countries have adopted a prohibition-based approach to cryptocurrencies while not necessarily prohibiting blockchain technology itself. These jurisdictions generally prioritize centralized monetary control, strict capital flow management, and concerns related to financial stability and illicit finance over the promotion of cryptocurrency markets.

7.4.1. The Prohibition of Decentralized Cryptocurrencies: China

China exemplifies one of the most restrictive regulatory models for blockchain technology. In 2021, it implemented a sweeping ban on all cryptocurrency mining and trading activities,[2319] effectively outlawing key decentralized blockchain applications and prompting a large-scale relocation of mining operations, primarily to the United States, Canada, Kazakhstan, and Russia[2320] (though some operations have subsequently relocated again due to regulatory changes in those jurisdictions).[2321] This prohibitive stance is driven by multiple concerns, including risks to financial stability, the potential for capital flight, fraud prevention, and high energy consumption.[2322] It also reflects the Chinese government's broader commitment to centralized control over both financial and technological infrastructures.

Despite these restrictions, China continues to advance its

2318 Fin. Servs. Comm'n (S. Kor.), *Amended Legislation Establishes Legal Ground for Introducing and Circulating Security Tokens* (Jan. 15, 2026), https://www.fsc.go.kr/eng/pr010101/86076.

2319 People's Bank of China, Notice on Further Preventing and Disposing of Risks of Virtual Currency Trading Hype (Sept. 30, 2021), https://xining.pbc.gov.cn/en/3688110/3688172/4157443/2025080817510285458/index.html; Nat'l Dev. & Reform Comm'n, *Notice on Regulating Virtual Currency "Mining" Activities* (Sept. 24, 2021) as reported in Alun John et al., China's top regulators ban crypto trading and mining, sending bitcoin tumbling, Reuters (Sept. 24, 2021), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

2320 Samuel Shen & Andrew Galbraith, *China's Ban Forces Some Bitcoin Miners to Flee Overseas, Others Sell Out,* Reuters (June 25, 2021), https://www.reuters.com/technology/chinas-ban-forces-some-bitcoin-miners-flee-overseas-others-sell-out-2021-06-25/

2321 *See e.g.* Grady McGregor, *Kazakhstan Was the Second-Largest Bitcoin Miner in the World. Now Its Energy Crisis Is Forcing Miners to Shut Down*, Fortune (Nov. 24, 2021) https://fortune.com/2021/11/24/kazakhstan-bitcoin-crypto-mining-energy-power-crisis-china-xive-shuts-down/, describing how the migration of Chinese miners to Kazakhstan triggered a localized power crisis and subsequent clampdown on the industry.

2322 Notice on Regulating Virtual Currency "Mining" Activities, *supra* note 2319, at 1.

own state-directed blockchain initiatives, most notably the development of a central bank digital currency —the digital yuan. This approach underscores how certain governments perceive decentralized blockchain technologies as fundamentally misaligned with their institutional frameworks and economic objectives, leading them to opt for prohibition rather than regulatory accommodation.

Overall, Mainland China's regulatory framework draws a clear distinction: decentralized cryptocurrencies are largely prohibited as sources of financial and systemic risk, while blockchain—in forms that are compatible with state oversight and control—is actively promoted as a tool of digital governance and industrial modernization. At the same time, the legal framework combines prohibitions on commercial cryptocurrency activities (including exchanges, mining, and ICOs) with judicial recognition of individual crypto holdings as virtual property protected under civil law. Chinese courts have generally treated cryptocurrencies as legally protectable property while holding transactions inconsistent with public policy as unenforceable.

7.4.1.A. The Ban of Decentralized Cryptocurrencies

Regulatory control in China began in 2013 when the People's Bank of China (PBoC), along with other financial authorities, issued a joint notice prohibiting financial institutions from engaging in Bitcoin transactions, although individual ownership was not criminalized.[2323] In 2017, regulators banned initial coin offerings (ICOs) and domestic cryptocurrency exchanges, citing financial risks and illegal fundraising concerns.[2324] Platforms for token financing and trading were prohibited from (1) exchanging legal tender to token, "virtual currency," or vice versa, (2) buying or selling of, or acting as central counterparty for, token or "virtual currency," or (3) providing pricing or information services for token or "virtual currency." Websites and mobile apps of unlawful token financing and trading platforms were to be closed or removed from app stores. However, this measure did not extend to banning the ownership or mining of cryptocurrency. According to data from Chainalysis, over $50 billion in cryptocurrency flowed out of East Asia between 2019 and 2020, much of it likely originating from China, often facilitated through stablecoins, such as USDT in over-the-counter transactions or through offshore exchanges.[2325]

This framework was significantly tightened in 2021, when the People's Bank of China and the National Development and Reform Commission (NDRC) imposed a complete ban on cryptocurrency transactions[2326] and mining,[2327] citing risks to financial stability, capital controls, and energy consumption. In 2024, the Supreme People's Court and the Supreme People's Procuratorate included "virtual asset" transactions in the legal definition of money laundering under Article 191 of the Criminal Law.[2328]

2323 People's Bank of China et al., *Notice on Precautions Against the Risks of Bitcoins*, Yin Fa [2013] No. 289 (Dec. 3, 2013), https://www.gov.cn/gzdt/2013-12/05/content_2542751.htm (China).

2324 People's Bank of China et al., *Announcement on Preventing Financing Risks of Token Offerings* (Sept. 4, 2017), http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html.

2325 Chainalysis Team, *East Asia: Pro Traders and Stablecoins Drive World's Biggest Cryptocurrency Market*, Chainalysis Blog (Aug. 20, 2020), https://www.chainalysis.com/blog/east-asia-cryptocurrency-market-2020/.

2326 People's Bank of China et al., *Notice on Further Preventing and Disposing of the Risks of Virtual Currency Trading and Speculation*, Yin Fa [2021] No. 237 (Sept. 15, 2021), https://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm.

2327 National Development and Reform Commission et al., *Notice on Rectifying Virtual Currency "Mining" Activities*, Fa Gai Yun Xing [2021] No. 1283 (Sept. 3, 2021), https://www.gov.cn/zhengce/zhengceku/2021-09/25/content_5639225.htm.

2328 Supreme People's Court, Supreme People's Procuratorate & Ministry of Public Security, *Opinions (II) on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Telecommunications and Internet Fraud* (June 22, 2021), https://www.spp.gov.cn/spp/xwfbh/wsfbt/202106/t20210622_522041.shtml.

7.4.1.B. Blockchain Innovation Under Centralized State Control

China's prohibition of cryptocurrencies tells only half the story. China has pursued an ambitious and highly centralized blockchain development policy. The 2019 Blockchain Information Service Regulation, issued by the Cyberspace Administration of China, imposed content controls, real-name registration, and mandatory filing requirements for blockchain service providers.[2329] In August 2019, the *PBoC's FinTech Development Plan* (2019–2021) emphasized the strategic use of distributed ledger technology in secure databases, financial infrastructure, and digital identity systems.[2330] The *2020 Cryptography Law* codified encryption management practices critical for secure blockchain applications and national cybersecurity.[2331] The *14th Five-Year Plan (2021–2025)* identified blockchain as one of several key digital infrastructure technologies, alongside artificial intelligence and big data, with wide applications in logistics, manufacturing, and governance.[2332]

Official policy documents articulate a consistent, state-centered vision of blockchain. The *2021 Guiding Opinions on Accelerating Blockchain Technology Application* defined blockchain as a "new-generation information technology" that integrates distributed networks, cryptographic tools, and smart contracts into a tamper-resistant and traceable database system. The intention of the technology is to address cybersecurity challenges and transform the internet from "information transmission to value transmission."[2333] This vision was reaffirmed in the *2023 Blockchain and Distributed Ledger Technology Standards System Guide*, which positioned blockchain as foundational infrastructure for emerging sectors like Web3 and the metaverse.[2334]

However, despite adopting the language of decentralization, China's actual implementation has diverged sharply from the public, permissionless architecture that is foundational to Web3. In practice, China promotes tightly controlled, permissioned systems —commonly referred to as "alliance chains"— where participation, data management, and consensus are tightly regulated by state-approved organizations. The Chang'an Chain (ChainMaker) exemplifies this model: It is a domestically developed blockchain infrastructure led by prominent research institutes and major technology companies, designed to be "autonomous and controllable," with a focus on high performance, security, and compliance with national standards.[2335]

Overall, blockchain applications are now deeply embedded in China's domestic systems. Permissioned blockchain platforms support supply chain tracking, judicial evidence preservation, tax monitoring, and public record authentication. The e-CNY, China's central bank digital currency (CBDC), represents a key instrument in

2329 Cyberspace Admin. of China, *Regulation on the Management of Blockchain Information Service*s (Jan. 10, 2019, effective Feb. 15, 2019), available at https://www.gov.cn/gongbao/content/2019/content_5392298.htm.

2330 People's Bank of China, *Notice of the People's Bank of China on Issuing the FinTech Development Plan (2019–2021)* (Sept. 6, 2019), http://www.pbc.gov.cn/zhengwugongkai/4081330/4406346/4693549/4085169/index.html.

2331 Standing Comm. Nat'l People's Cong., *Cryptography Law of the People's Republic of China* (Oct. 26, 2019, effective Jan. 1, 2020), https://www.gov.cn/xinwen/2019-10/27/content_5445395.htm.

2332 People's Bank of China, *Notice on Issuing the FinTech Development Plan (2022–2025)*, Yin Fa [2021] No. 335 (Jan. 21, 2022), http://www.pbc.gov.cn/zhengwugongkai/4081330/4406346/4693549/4470403/index.html.

2333 Ministry of Industry and Information Technology & Office of the Central Cyberspace Affairs Commission, *Guiding Opinions on Accelerating the Application of Blockchain Technology and Industrial Development*, Gong Xin Bu Lian Xin Fa [2021] No. 62 (June 7, 2021), https://www.cac.gov.cn/2021-06/07/c_1624629407537785.htm.

2334 Ministry of Industry and Information Technology, Cyberspace Administration of China & National Standardization Administration, *Notice on Issuing the Blockchain and Distributed Ledger Technology Standards System Guide*, Gong Xin Bu Lian Ke [2023] No. 260 (Dec. 28, 2023), https://www.gov.cn/zhengce/zhengceku/202401/content_6925774.htm.

2335 ChainMaker, *Introduction to the ChainMaker Underlying Technology Platform*, ChainMaker Docs v1.2.0, https://docs.chainmaker.org.cn/v1.2.0/html/intro/%E5%B9%B3%E5%8F%B0%E7%AE%80%E4%BB%8B.html (last visited Jan. 15, 2026).

this strategy. According to the People's Bank of China 2021 White Paper, the e-CNY is a retail-level digital currency equivalent to physical cash, issued through a two-tier system involving the central bank and commercial banks.[2336] Pilot programs have expanded to regions such as Hong Kong and Hainan, integrating the e-CNY with trade finance and cross-border identity systems.[2337]

7.4.2. Prohibition of Cryptocurrencies as Means of Payment: Russia

In Russia, the ownership and trading of digital assets are permitted, and mining is legal, although the use of crypto-assets as a means of payment is expressly prohibited.

The principal legal framework is Federal Law No. 259-FZ of July 31, 2020, *On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation*, which entered into force on January 1, 2021.[2338] This statute distinguishes between digital financial assets (DFAs) and digital currency. DFAs are defined as digital rights which may include monetary claims, equity rights, or other property rights that are created, recorded, and transferred using distributed ledger or similar technologies. They are classified as property rights and regulated with respect to issuance, circulation, and accounting. By contrast, "digital currency" (*tsifrovaya valuta*) refers to digital data that may be used or offered as a means of payment that is not denominated in the legal currency of the Russian Federation, a foreign state, or an international monetary unit. While individuals and entities may lawfully acquire, hold, trade, and mine digital currencies, their use as a means of payment for goods or services within Russia is explicitly prohibited, and the dissemination of information about such use is likewise restricted.

Mining is recognized as a lawful entrepreneurial activity under Federal Law No. 221-FZ of August 8, 2024, which formally legalizes cryptocurrency mining and entered into force on November 1, 2024. The law establishes a mandatory national register of miners administered by the Ministry of Digital Development, with registration required for industrial-scale operations. Miners are required to report income and to pay taxes on earnings derived from the sale or exchange of mined assets under the general provisions of the Tax Code.[2339] Industrial-scale mining operations are subject to registration requirements, and authorities have periodically discussed the possible introduction of licensing obligations.

Separate reporting and disclosure obligations apply to digital financial assets and to digital currencies, with thresholds and procedures having evolved through subsequent tax-law amendments and regulatory guidance. Certain transactions exceeding statutory thresholds may trigger reporting obligations, and residents are required to declare holdings of digital currencies and DFAs in accordance with applicable tax rules.

Although the domestic use of digital currency as a means of payment has remained prohibited,[2340] recent legislative developments signal a cautious opening toward international applications. In February 2024, the State Duma approved a draft law authorizing the use of

2336 People's Bank of China, *White Paper on the Progress of Research & Development of E-CNY in China* (July 16, 2021), https://www.gov.cn/xinwen/2021-07/16/content_5625569.htm.

2337 Hong Kong Monetary Auth., *Expansion of Cross-Boundary Pilot for e-CNY in Hong Kong* (May 17, 2024), https://www.hkma.gov.hk/gb_chi/news-and-media/press-releases/2024/05/20240517-3/; *Bank of China Hainan Branch Embraces Digital Finance to Build e-CNY Ecosystem*, XinhuaNet (Dec. 7, 2023), http://hq.xinhuanet.com/20231207/cedaebe9171d419b9cf764302d026577/c.html.

2338 Federal Law No. 259-FZ of July 31, 2020, *On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation* (as amended Oct. 25, 2024), SZRF 2020, No. 31, Item 5023 (Russ.), https://cis-legislation.com/document.fwx?rgn=126432.

2339 Law on Digital Financial Assets, Federal Law No. 259-FZ (Russ.), arts. 1(1), 3.1–3.5.

2340 Law on Digital Financial Assets, Federal Law No. 259-FZ (Russ.), arts. 1(3), 14(5).

digital financial assets and, within experimental legal regimes, certain forms of digital currency, in cross-border trade and payments.[2341] The legal mechanism relies on "experimental legal regimes" established under Federal Law No. 258-FZ, which enables approved entities to conduct international settlements using both Russian and foreign digital currencies under the supervision of the Bank of Russia and the Ministry of Finance.[2342] In January 2025, a ruble-pegged stablecoin known as A7A5 was launched by private actors and has been widely reported as being used in cross-border settlement structures designed to mitigate sanctions-related constraints.[2343] Public reporting suggests that such instruments are intended to facilitate access to international liquidity while limiting prolonged exposure to counterparty and asset-freezing risks, although they do not alter the domestic prohibition on crypto-payments.[2344] These initiatives aim to facilitate trade finance and external settlements while maintaining the prohibition on the use of digital currency for domestic payments.

In December 2025, the Bank of Russia published a regulatory concept proposing to allow both qualified and non-qualified investors to purchase cryptocurrencies and stablecoins as "currency values" for investment purposes only, while reaffirming the long-standing prohibition on their use as a means of payment within Russia.[2345] Under the proposal, digital currencies and stablecoins would be treated as monetary assets that Russian residents may buy and sell exclusively through licensed intermediaries. Public summaries of the concept indicate that non-qualified investors would gain limited access subject to quantitative caps and asset-eligibility restrictions, while qualified investors would benefit from broader access, potentially excluding anonymity-enhancing or privacy-focused tokens. The concept also contemplates cross-border transactions, including purchases on foreign exchanges using foreign bank accounts, subject to disclosure and tax-reporting obligations. The Bank of Russia expects lawmakers to establish the necessary legislative framework by July 1, 2026, with criminal or administrative liability for unlicensed crypto intermediation taking effect one year later, on July 1, 2027. On December 15, 2025, the chair of the State Duma's financial markets committee reiterated that cryptocurrencies would "never become money" in Russia and would function only as investment instruments.[2346]

In parallel, Russia continues to promote distributed ledger technologies for state-managed applications — including e-government services, judicial recordkeeping, and supply-chain oversight— within the framework of its national "Digital Economy of the Russian Federation" program.[2347] However, these deployments must comply with strict data localization and cybersecurity regulations —particularly under Federal Law No. 152-

2341 See Federal Law of the Russian Federation No. 45-FZ of Mar. 11, 2024 on Amending Certain Legislative Acts of the Russian Federation], art. 1 (Rus.), https://cis-legislation.com/document.fwx?rgn=157172 (authorizing the use of digital financial assets for foreign trade settlements).

2342 *Id.*

2343 *Legislated Sanctions Evasion: How the Garantex Rebrand, Grinex, and the Ruble-Backed Token, A7A5 Have Shaped Russia's Shadow Crypto Economy*, Chainanalysis (Aug. 14, 2025), https://www.chainalysis.com/blog/a7a5-grinex-russian-crypto-economy-ofac-sanctions-august-2025/.

2344 *Id.*; *see also* Press Release, Council of the Eur. Union, *19th Package of Sanctions Against Russia: EU Targets Russian Energy, Third-Country Banks and Crypto Providers* (Oct. 23, 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/; *Garantex, Grinex, and the A7A5 Token: A Deep Dive into Sanctions Evasion Networks*, TRM Labs (Aug. 14, 2025), https://www.trmlabs.com/resources/blog/garantex-grinex-and-the-a7a5-token-a-deep-dive-into-sanctions-evasion-networks. A7A5 is officially issued by a Kyrgyz firm Old Vector LLC and claims a 1:1 backing by Ruble deposits.

2345 Bank of Russia, *Main Directions for Digital Market Development: Proposals for Cryptocurrency Regulation* (Dec. 24, 2025), http://www.cbr.ru/eng/press/event/?id=28215. The proposal specifies a 300,000 ruble (approx. $3,800) annual cap only for non-qualified (retail) investors.

2346 Tim Alper, *Russians Will 'Never' Use Crypto to Make Payments, Top Lawmaker Says*, DL News (Dec. 16, 2025), https://www.dlnews.com/articles/regulation/russians-will-never-use-crypto-to-make-payments/.

2347 Ekaterina A. Grigoreva, Liliya F. Garifova & Elvira A. Polovkina, *The Future of Digital Technology in Russia: Blockchain as One of the Priority Directions of Development*, 10(2A) Int'l J. Emerging Techs. 42 (2019), https://www.researchtrend.net/ijet/pdf/11-17.pdf.

FZ "On Personal Data," which requires storing Russian citizen data on servers located within Russia.[2348] While not specific to blockchain systems, these rules apply to digital platforms broadly, including blockchain-based state applications, ensuring that sensitive data remains under Russian jurisdiction and is processed in accordance with national law. Non-compliance can result in significant fines or blocking of services - a pattern most recently demonstrated by the 2025 fining and blocking of Speedtest (Ookla),[2349] and threats directed at Amazon Web Services and GoDaddy for failure to localize data on Russian territory.[2350]

7.4.3. Blanket prohibitions of cryptocurrencies

While China distinguishes between decentralized cryptocurrencies—which are categorically prohibited—and state-sanctioned, permissioned blockchain systems that are actively promoted as instruments of digital infrastructure and governance, some countries have opted for comprehensive prohibitions. Jurisdictions including Algeria,[2351] Morocco,[2352] Tunisia,[2353] and Qatar,[2354] among others, have adopted statutory or regulatory measures that prohibit the use, trading, or facilitation of cryptocurrency transactions.

Motivated primarily by concerns relating to monetary sovereignty, capital controls, and financial crime, these prohibitions are broad and largely undifferentiated, significantly constraining cryptocurrency activity. Although distributed-ledger technology itself is not formally outlawed, its close association with cryptocurrencies has often discouraged experimentation by both public and private actors, and large-scale blockchain initiatives remain limited in these jurisdictions.

2348 Federal Law No. 152-FZ of July 27, 2006, on Personal Data, *SZRF* 2006, No. 31, Item 3451 (as amended) (Russ.), https://ihl-databases.icrc.org/en/national-practice/federal-law-no-152-fz-personal-data-2006.

2349 Alexander Marrow & Gleb Stolyarov, *Russia blocks Ookla's online Speedtest service due to internet security threats*, Reuters, https://www.reuters.com/sustainability/society-equity/russia-blocks-ooklas-online-speedtest-service-due-internet-security-threats-2025-07-30/.

2350 *See* CJ Moses, *Amazon Threat Intelligence identifies Russian cyber threat group targeting Western critical infrastructure*, AWS Security Blog (Dec. 15, 2025), https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-russian-cyber-threat-group-targeting-western-critical-infrastructure/; *Russian watchdog blocks websites of hosting providers*, TASS (16 April 2024), https://tass.com/society/1776239.

2351 Loi n° 17-11 du 27 décembre 2017 portant loi de finances pour 2018 [Law No. 17-11 of Dec. 27, 2017, Finance Law for 2018], art. 117, Journal Officiel de la République Algérienne Démocratique et Populaire [Official Journal of the People's Democratic Republic of Algeria] No. 76, Dec. 28, 2017, p. 13 (Alg.), https://digitalpolicyalert.org/event/28584-finance-law-for-the-year-2018-law-no-17-11-including-prohibition-of-the-purchase-sale-use-and-possession-of-virtual-currencies-under-article-117-entered-into-force.

2352 Foreign Exchange Office, *Mise au point au sujet de l'utilisation des monnaies virtuelles*, Press Release, [Clarification Regarding the Use of Virtual Currencies] (November 2017), https://www.oc.gov.ma/sites/default/files/2018-05/communique%CC%81%20monnaies%20virtuelles%20fr.pdf; Joint Statement, Ministry of Economy and Finance / Bank Al-Maghrib / Office des Changes (November 2017). Note that Morocco has since published a draft law Bill 42.25 which outlines rules to guide the issuance and trading of digital assets and would regulate companies facilitating these activities, though timelines for when it comes into effect remain unclear. Oumaima Moho Amer, *Morocco Moves to Regulate Digital Assets with New Draft Law*, Morocco World News (5 November 2025), https://www.moroccoworldnews.com/2025/11/266685/morocco-moves-to-regulate-digital-assets-with-new-draft-law/.

2353 Central Bank of Tunisia (BCT) Circular/Directive (May 2018). See *18 Countries Where Bitcoin Is Banned or Restricted,* CoinGecko (last updated August 2025), https://www.coingecko.com/learn/countries-ban-bitcoin#:~:text=Additional%20Comments:%20North%20Macedonia%20is,Ecuador

2354 QFCRA Virtual Assets Alert (26 December 2019), under QFC Law No. (7) of 2005, https://qfcra-en.thomsonreuters.com/sites/default/files/net_file_store/Virtual_Asset_Services-Email_Alert_2019.pdf.

KEY TAKEAWAYS

■ Policymakers confronting the legal uncertainty surrounding blockchain technologies face a set of strategic choices. **Four principal approaches** emerge in practice: (1) an *observational* or non-interventionist approach, which favors experimentation through soft-law tools such as guidance and regulatory sandboxes; (2) the application of *existing legal frameworks* through interpretive guidance, enforcement actions, and criminal prosecution —often described as "regulation by enforcement," whereby legal standards develop incrementally through case-based decisions; (3) the adoption of *new, technology-specific legal frameworks* designed to address regulatory gaps and adapt existing principles to blockchain applications; and (4) *restrictive regimes*, including partial or complete prohibitions on certain blockchain activities, as exemplified by China's approach to cryptocurrency. These approaches are not mutually exclusive but operate as complementary regulatory strategies that jurisdictions may deploy in parallel or sequentially.

■ The **observational approach** reflects regulatory restraint aimed at accommodating innovation and managing uncertainty. Governments following this model monitor technological developments, issue non-binding guidance, and rely on mechanisms such as regulatory sandboxes— controlled environments in which firms can test products under temporary regulatory relief and supervisory oversight. This flexibility supports innovation but carries risks of sustained legal uncertainty, reliance on non-binding instruments, and discretionary admission processes that may favor selected participants. In practice, some jurisdictions that initially adopted observational postures —including Singapore and, to a lesser extent, Canada and Australia— have subsequently transitioned toward more interventionist frameworks, suggesting that the observational approach often operates as a transitional phase rather than a stable long-term equilibrium.

■ More active oversight strategies rely on the application of existing legal frameworks without creating blockchain-specific regimes. In the United States, agencies such as FinCEN and the IRS have adopted a model of **interpretive guidance followed by enforcement**, clarifying ex ante how existing rules —particularly money transmission laws and tax regulations— apply to digital assets, and subsequently enforcing compliance. This approach depends on functional classifications that extend traditional legal categories to novel technological contexts, with significant regulatory consequences, including AML/CFT obligations and tax reporting requirements.

■ By contrast, **regulation by enforcement** represents a reactive model in which regulators define the legal obligations of crypto-asset market participants through enforcement actions rather than rulemaking. In the United States, this strategy —prominently used by the SEC and CFTC— has shaped regulatory boundaries incrementally through case-by-case decisions, as illustrated by recent securities enforcement actions such as *SEC v. Terraform Labs* and proceedings involving major platforms, including Coinbase and Binance. This approach is complemented by "regulation by prosecution," whereby the Department of Justice relies on criminal proceedings —for example, in cases involving cryptocurrency mixers such as Samourai Wallet— to address unlawful conduct. While this model allows regulators to respond flexibly to evolving technological developments, it also contributes to legal uncertainty and fragmentation, requiring market participants to infer applicable standards from enforcement outcomes and, at times, divergent judicial interpretations.

■ In response to sustained criticism of enforcement-driven approaches, U.S. digital asset policy under the second Trump administration has shifted toward a more proactive model emphasizing ex ante guidance, institutional coordination, and legislative intervention. This reorientation includes a reduced reliance on enforcement and prosecution as primary tools of policy formation, a renewed focus on regulatory clarity through agency guidance (SEC, CFTC), and the development of comprehensive federal frameworks, notably **the GENIUS Act for stablecoins** and the proposed **CLARITY Act** to clarify jurisdictional boundaries and asset classification. While this approach seeks to reduce legal uncertainty and support innovation, its implementation remains incomplete and subject to ongoing legislative and institutional debate.

■ **Regulating proactively** through new legal frameworks can foster innovation by providing greater legal clarity and predictability for blockchain applications. In the United States, multiple states have extended legal recognition to decentralized autonomous organizations (DAOs) through both "wrapper" approaches adapting existing corporate forms (e.g., LLCs) and DAO-native statutes. Many of these frameworks draw inspiration from the **Coalition of Automated Legal Applications (COALA) Model Law**, which proposes a technology-specific regime granting legal personality and limited liability based on compliance with functional and technical criteria, including on-chain governance, open-source code, and automated execution. In practice, however, no jurisdiction has fully embraced COALA's protocol-first vision of automatic, non-registered legal personhood: All enacted regimes retain a mandatory human-mediated gateway to legal recognition. While these frameworks facilitate market development and legal certainty, they remain fragmented across jurisdictions, thereby complicating cross-border and multi-jurisdictional operations. Wyoming's DUNA, for example, targets nonprofit DAOs; Utah's LLD is designed for for-profit entities; and New Hampshire law adopts a code-deferential, registry-based model. Proactive frameworks also address **conflict-of-laws challenges**: Switzerland has embedded blockchain-specific rules in its private international law, while UNIDROIT has developed soft-law principles aimed at promoting greater harmonization in the treatment of digital assets across jurisdictions.

■ Some regulatory frameworks govern blockchain technologies indirectly by targeting specific use cases rather than blockchain systems as such. The **EU Data Act,** for example, imposes design and governance requirements on smart contracts when they are used to automate data-sharing arrangements, particularly in the context of connected devices and the Internet of Things. The Data Act expressly acknowledges smart contracts as a distinct technical object, defines their core characteristics, and subjects their deployment in specific contexts to detailed technical and governance requirements. While this framework demonstrates that blockchain systems can be subject to detailed regulatory obligations, it also reveals the limits of regulating decentralized technologies: Requirements such as reversibility, access controls, and "kill switches" may conflict with core features of decentralized systems, including immutability and distributed governance. These tensions are reflected in the European Commission's proposal to repeal key provisions of the Data Act. More fundamentally, the example of the Data Act both complicates claims of blockchain alegality and reveals the practical constraints that continue to shape how far law can reach into the technical core of decentralized systems.

■ **The eIDAS 2.0 framework** reflects another strategy for integrating blockchain technologies into regulated institutional infrastructures, particularly in the domain of digital identity and trust services. By recognizing electronic ledgers and enabling blockchain-based identity solutions within the EU Digital Identity Wallet ecosystem, eIDAS grants legal effect to certain distributed-ledger applications. However, such recognition is conditional on compliance with requirements of supervision, interoperability, and accountability, notably through qualified trust service providers. As a result, the framework reinforces the role of institutional intermediaries and structurally favors permissioned or hybrid architectures, highlighting the difficulty of accommodating fully decentralized systems within existing legal frameworks.

■ Comprehensive crypto-asset regulation is exemplified by t**he European Union's Markets in Crypto-Assets (MiCA) Regulation**, which establishes a harmonized regime for crypto-assets not covered by existing financial legislation, while explicitly excluding services provided "in a fully decentralized manner without any intermediary." **Switzerland** illustrates an alternative approach, selectively adapting existing financial-market laws through targeted amendments —such as the DLT Act's introduction of ledger-based securities— rather than creating entirely new regulatory frameworks. **South Korea,** by contrast, reflects a more interventionist model, combining strict supervision, robust AML and investor-protection requirements, and constraints on token issuance, while progressively integrating crypto-asset activities into regulated financial channels.

■ A minority of states have adopted **restrictive or prohibition-based approaches to cryptocurrencies**, prioritizing monetary sovereignty, capital controls, and financial stability over the development of crypto-asset markets. **China** stands as the leading example, having banned decentralized cryptocurrency trading and mining while simultaneously promoting state-controlled, permissioned blockchain systems and the digital yuan as alternatives aligned with centralized governance. Other jurisdictions have adopted more targeted restrictions: **Russia**, for instance, prohibits the use of cryptocurrencies as a means of payment while permitting ownership, trading, and mining, thereby confining crypto-assets to an investment function rather than a monetary role. At the most restrictive end of the spectrum, some countries have implemented blanket prohibitions on cryptocurrency activity, significantly constraining market development.

■ These divergent approaches reflect fundamentally **different regulatory philosophies and risk tolerances**. The observational model prioritizes market development and regulatory learning, accepting temporary uncertainty as the price of innovation. Regulation by enforcement applies existing legal frameworks to crypto-asset activities through case-by-case decisions, offering flexibility but generating legal uncertainty and litigation costs. Comprehensive ex ante frameworks provide greater legal certainty but risk regulatory obsolescence and may impose disproportionate compliance burdens on smaller entities. Prohibition-based regimes eliminate decentralized innovation domestically while potentially displacing activity to other jurisdictions. Across these approaches, a common structural tension emerges: Most regulatory frameworks rely on identifiable intermediaries and institutional control, whereas fully decentralized systems remain difficult to accommodate within existing legal categories. As a result, the legal landscape governing blockchain remains fragmented and only partially coherent.

■ Importantly, the legal frameworks and judicial decisions discussed in this chapter demonstrate that the alegality thesis requires significant qualification. Despite persistent legal uncertainty, **blockchain systems and activities are increasingly within the reach of law**, at least to a certain extent. However, no jurisdiction has successfully addressed the core challenge of regulating genuinely decentralized, permissionless systems that lack the identifiable intermediaries upon which traditional regulation depends. This limitation is also evident in DAO-specific legislation: Statutes designed to recognize DAOs ultimately rely on human-mediated formation or registration mechanisms and designated points of contact. Even the most advanced regulatory regimes struggle to accommodate autonomous protocols operating without central operators, as illustrated by MiCA's "fully decentralized" exclusion. Until policymakers resolve **the fundamental tension between decentralized, permissionless systems and regulatory frameworks premised on identifiable intermediaries**, the most decentralized blockchain applications will continue to operate in legal uncertainty, regardless of the regulatory approach adopted.

CHAPTER 8

General Conclusion

CHAPTER 8 TABLE OF CONTENTS

CHAPTER 8. GENERAL CONCLUSION **381**

8.1. The Limits of Decentralization and the Reach of Law 383

8.1.1. Decentralization as a Relative Ideal 383

8.1.2. The Rise of Code-Governed Systems 385

8.1.3. Qualifying the Alegality Thesis 387

8.1.4. The Persistence of Regulatory Gaps 389

8.2. Policy Orientations 391

8.2.1. Exploring New Regulatory Methods 392

8.2.1.A. Hybrid Regulatory Frameworks 392

8.2.1.B. Regulation Through Governance 393

8.2.2. Defining Core Regulatory Objectives 394

8.2.2.A. Promoting Sound Governance in Decentralized Systems 395

1. Guidelines and Non-Mandatory Principles 395

2. Targeted Mandatory Requirements 396

8.2.2.B. Reducing Legal Uncertainty 397

8.2.3. International Coordination 398

8.3. Conclusion: The Blockchain Governance Challenge 401

CHAPTER 8
General Conclusion

A prevailing narrative presents blockchain technologies as transforming trust by relocating it from institutional intermediaries to technical infrastructure.[2355] In this vision, confidence no longer rests primarily on regulated entities, such as banks, but on the reliability of code and the incentive structures embedded in globally operating, censorship-resistant protocols. Yet, the practical realities of decentralization reveal persistent governance gaps and the difficulty of achieving decision-making arrangements that can plausibly be described as democratic. These tensions, in turn, complicate the task of regulators seeking to articulate a coherent and proportionate response to blockchain-based systems.

The following paragraphs draw together key observations from the preceding chapters and identify a range of policy options that may guide policymakers confronting these governance and regulatory challenges.

8.1. THE LIMITS OF DECENTRALIZATION AND THE REACH OF LAW

This section synthesizes the report's core findings by examining four interrelated dynamics: decentralization as an aspirational, rather than achieved, condition; the rise of blockchain-based, code-governed systems; the limits of the alegality thesis in light of law's continued points of intervention; and, the persistence of regulatory gaps arising from the tension between decentralized infrastructures and intermediary-centered legal models.

8.1.1. Decentralization as a Relative Ideal

Consensus mechanisms may exhibit centralization tendencies *(See section 3.3.)*. In proof-of-work (PoW) systems, mining pools concentrate hash power in the hands of a small number of dominant actors. Similar risks arise in proof-of-stake (PoS) systems, where validator power is increasingly concentrated among large intermediaries, including staking platforms and centralized exchanges such as Coinbase and Binance. While these actors do not exercise unilateral control over the protocol, their scale gives them disproportionate influence over transaction validation. These concerns are even more pronounced in networks with small validator sets operating under delegated or authority-based consensus, such as BNB Smart Chain, where a limited validator set concentrates effective control over consensus.

More importantly, even where blockchain networks exhibit *technical decentralization* at the infrastructure level, they may remain *politically centralized* in their governance *(See section 3.3.)*. Most protocols combine off-chain and on-chain governance *(See section 3.2.)*. Off-chain actors —including foundations, core developers, and major market participants— exercise substantial influence over protocol evolution and decision making. Likewise, on-chain governance can also generate forms of concentration. Power tends to accrue to a limited number of actors, including developers, validators, and large token

2355 Darcy W. E. Allen, Aaron M. Lane & Marta Poblet, *The Governance of Blockchain Dispute Resolution* 25 Harv. Negot. L. Rev. 75, 77 (2019), https://journals.law.harvard.edu/hnlr/wp-content/uploads/sites/91/75-allen-et-al.pdf.

holders. Stakeholders holding significant token positions often dominate token-based voting, while liquid staking and delegation mechanisms reinforce the advantages of early adopters and professional participants. In addition, complex governance architectures create technical and cognitive barriers that limit broader participation. As a result, the concentration of governance tokens in the hands of a small number of actors enables small groups to exercise disproportionate influence *(See section 3.2.2.C.)*.

Within this context, decentralization appears less like an achievable state than a continuum. Consequently, blockchain theorists have identified various criteria[2356] and frameworks[2357] for assessing decentralization *(See section 2.1.2.A.)*. These include indices measuring distributed governance,[2358] power distribution,[2359] resilience,[2360] and token concentration.[2361] Two examples of the latter include the *Nakamoto Coefficient*,[2362] which measures the minimum number of actors that would need to collude in order to compromise a system, and *Gini coefficients,* which quantify wealth distribution inequality.[2363] Other means for assessing decentralization involve operational indicators, including the geographic distribution of validators; the diversity of node-hosting infrastructures; and, the heterogeneity of basic software components (such as client implementations).[2364] Perhaps the most telling assessment is the *"Bahamas test*:"[2365] Could a project continue functioning if its founders disappeared, as Satoshi Nakamoto did?[2366]

Empirical studies examine decentralization through various dimensions: how participants are grouped within the network (clustering); how connections are distributed among them (degree distribution); whether the system has a dominant "core" and a more dependent "periphery;" how concentrated control is among miners

2356 For example, it may be understood as a verifiable state in which (1) the design of a DAO is collusion-resistant and grounded in long-term equilibrium, and (2) its governance processes are transparent and unrestricted in access. Henrik Axelsen et al., *When is a DAO Decentralized?*, 31 Complex Sys. Informatics and Modeling Q. 51, 56 (July 31, 2022), https://doi.org/10.7250/csimq.2022-31.04.

2357 *See, e.g.*, Ziqiao Ao et al., *Is Decentralized Finance Actually Decentralized? A Social Network Analysis of the Aave Protocol on the Ethereum Blockchain*, arXiv (June 16, 2022), https://arxiv.org/abs/2206.08401.

2358 The *Distributed Governance Index*, for instance, evaluates the strength and openness of a blockchain's internal decision-making processes. It considers factors such as the transparency of governance procedures, the existence of internal mechanisms for amending rules, whether there is open access for submitting proposals to improve the protocol, the availability of secret voting, vulnerability to majority (51%) attacks, mechanisms for correcting or reorganizing the blockchain in the event of errors or forks, systems for funding common goods, the removal of toxic or illicit data, and whether users have binding legal contracts with each other in addition to the protocol. Tom W. Bell, *Distributed Self-Government in Protocol Communities: An Introduction and Index of Examples*, 25 Indep. Rev. 293, 296-98 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4058722.

2359 The *XYZ Decentralization Index* looks at whether the code is open source and immutable, how many independent validators operate the network, how well distributed validation power is, how widely tokens are spread out among users, and whether critical infrastructure components —such as servers or clients— are diversified, rather than controlled by a few entities. Javier Sanchez Valiente, *The XYZ Decentralization Index: A Framework for Assessing Decentralization in Crypto Protocols*, dYdX Foundation (Dec. 18, 2024), https://www.dydx.foundation/blog/the-xyz-decentralization-index-a-framework-for-assessing-decentralization-in-crypto-protocols.

2360 The *Decentralization Quotient* adopts a broader perspective, measuring the network's overall resilience. It captures dimensions such as resistance to censorship and the geographic dispersion of nodes and participants. Jaeseung Lee et al., *DQ: Two Approaches to Measure the Degree of Decentralization of Blockchain*, 7 ICT Express 278, 279-80 (2021), https://doi.org/10.1016/j.icte.2021.08.008.

2361 The U.S.-based Decentralization Research Center combines various elements. A decentralized blockchain network is open source or makes the source-code available. And, it is functional, autonomous, permissionless, non-custodial, credibly neutral, economically independent, and has distributed ownership. *See generally Designing Policy for a Flourishing Blockchain Industry*, Decentralization Rsch. Ctr. (Feb. 2025), https://thedrcenter.org/wp-content/uploads/2025/02/DRC-Designing-Policy-Final.pdf.

2362 The Nakamoto Coefficient expresses the minimum number of actors that would need to collude to compromise the system's security or governance. See a dynamic list at *Nakamoto Coefficients*, Nakaflow, https://nakaflow.io/ (last visited Jan. 15, 2026), for "a measure of the smallest number of independent entities that can act collectively to shut down a blockchain" in the most popular blockchain networks.

2363 *See generally* Lidia Ceriani & Paolo Verme, *The Origins of the Gini Index: Extracts from Variabilità e Mutabilità (1912) by Corrado Gini*, 10 J. Econ. Inequality 421 (2012), https://doi.org/10.1007/s10888-011-9188-x.

2364 Stephanie Dunbar & Sam Padilla, *Evaluating Validator Decentralization: Geographic and Infrastructure Distribution in Proof-of-Stake Networks 1*, Messari (June 1, 2023), https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks; Joshua Tan et al., *Open Problems in DAOs* 16, arXiv (Oct. 29, 2023), https://arxiv.org/abs/2310.19201.

2365 Todd Henderson & Max Raskin, *A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets*, 2019 Colum. Bus. L. Rev. 443, 461, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265295.

2366 Succinctly put: if the project developers "fled to the Bahamas or ceased to show up to work —like Satoshi Nakamoto— would the project still be capable of existing?", Henderson & Raskin, *supra* note 2365.

or validators; and, how wealth and network activity are distributed across different regions and participants.[2367] These assessments reveal that decentralization is neither absolute nor uniform but rather a complex, multidimensional, and evolving property of blockchain systems. They suggest that decentralization is best understood as an aspirational and relative ideal, rather than a fully attainable end state.

Against this backdrop, these limitations should not be understood as evidence that decentralization fails as a governance paradigm. Many of the dynamics identified in Chapter 3 —concentration of influence, informational asymmetries, and limited participation— also characterize traditional forms of governance, including corporate structures and representative democracies. Token-based voting, for instance, has clear parallels in shareholder voting regimes, where large stakeholders routinely exercise disproportionate influence. Likewise, the opacity of coordination among major token holders mirrors forms of informal influence and agenda-setting that are pervasive in both public and private governance systems. Yet this comparison cuts both ways: Unlike corporate governance, blockchain systems generally lack the fiduciary duties, minority protection mechanisms, and regulatory oversight that partially constrain the exercise of concentrated power in traditional institutional settings.

Taken together, these considerations suggest that decentralization is neither a panacea nor an illusion; it is a governance modality whose advantages and limitations must be evaluated in context. The relevant question is not whether decentralized architectures achieve a perfect distribution of power —no governance system does— but whether, and under what conditions, they offer meaningful improvements over existing institutional arrangements. Decentralization is thus best understood as a relative and context-dependent objective, capable of delivering meaningful benefits even where it falls short of full or idealized distribution.

8.1.2. The Rise of Code-Governed Systems

Blockchain systems increasingly operate as code-based environments capable of coordinating —and, in some cases, autonomously managing— complex organizational functions. Lessig's expression that "code is law" emphasizes that software architecture itself functions as a powerful regulatory modality, constraining behavior in ways functionally comparable to legal rules *(See section 6.1.1.)*.[2368] Blockchain discourse revives and radicalizes this idea: Protocols and smart contracts are frequently portrayed as autonomous, self-executing sources of normativity that can rival and, in some accounts, even displace traditional legal institutions. Building on Joel Reidenberg's concept of *Lex Informatica*, some scholars describe this development as the emergence of a *lex cryptographica*: a technologically instantiated rule system in which governance is embedded in cryptographic protocols, rather than enacted through conventional legal instruments *(See section 6.1.2.)*.[2369] Within this literature, blockchain is thus presented as a paradigmatic environment in which regulatory authority is relocated from legislatures and courts to system architecture itself. Some authors use the expression "rule by code" to describe systems in which rules are embedded directly within the technological infrastructure of online networks and platforms.[2370]

2367 Carlo Campajola et al., *The Evolution of Centralisation on Cryptocurrency Platforms* 2-7, ARXIV, (June 10, 2022) https://arxiv.org/pdf/2206.05081.

2368 LAWRENCE LESSIG, CODE: VERSION 2.0, 1–8 (Basic Books 2006) https://lessig.org/product/codev2; *See generally* Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code* of *Law and Code* as *Law*, 82 MOD. L. REV. 207 (2019), https://www.jstor.org/stable/45220933.

2369 Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 POL'Y & SOC'Y 358, 363 (2022), https://academic.oup.com/policyandsociety/article/41/3/358/6529327.

2370 Primavera De Filippi, Morshed Mannan, & Wessel Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance*, 92 GEO. WASH. L. REV. 1229, 1243-44 (2024), https://www.gwlr.org/wp-content/uploads/2024/12/92-Geo.-Wash.-L.-Rev.-1229.pdf [hereinafter *Blockchain Technology and the Rule of Code: Regulation via Governance*].

Such an architecture is not without risks and uncertainties. In practice, the tension between the self-executing authority of blockchain code and the normative authority of law has been illustrated in widely discussed cases *(See section 6.2.)*. Courts have struggled with the persistent uncertainty over whether exploiting a protocol's flaws constitutes legitimate use or wrongful conduct, an ambiguity that illustrates the practical limits of the "code is law" paradigm. The legal statuses of smart contracts *(See section 6.5.)* and DAOs *(See section 6.4.)* remain unsettled, reflecting continuing confusion between their technical nature as self-executing software and their possible classification as contractual arrangements or legal entities.

More fundamentally, scholars warn that the transition from law to code threatens to disrupt the established balance of authority that forms the foundation of traditional legal orders[2371] and may generate systems that "may or may not operate according to the rule of law."[2372] At its extreme, this transfer of authority and decision-making power –from legal institutions and democratic processes to autonomous, decentralized, code-driven systems– risks degenerating into a "tyranny of code."[2373] While decentralization is often presented as a safeguard against arbitrariness *(See section 1.1.)*, blockchain systems are only imperfectly decentralized. And even highly decentralized architectures lack intrinsic mechanisms for democratic legitimation *(See section 3.3.)*. As a result, reliance on code-based governance intensifies —rather than resolves— the need for credible and democratically accountable governance arrangements.

This need is highlighted by Primavera de Filippi and her co-authors, who distinguish between "rule by code" and "rule of code."[2374] They define the "rule by code" as "a system of online governance in which there exists a sovereign (the online operator —as well as the regulators to which the operator must respond) that stands 'above the code' and, therefore, uses the code to impose restrictions and constraints over internet users who are subject to such code."[2375] Notably, the authors do not apply this notion to decentralized blockchain networks. Instead, they use it to characterize centralized systems in which one or a few operators control the execution of code, namely online platforms that are operated by companies that unilaterally determine the rules governing user interactions. In these contexts, they describe "rule by code" as being "instrumentalized by platform operators to promote their own economic or political interests" and "as a means of exercising control over the platform's users."[2376]

By contrast, the "rule *of* code" is presented as a new regulatory principle introduced by blockchain technology.[2377] Blockchain's "rule *of* code" denotes the idea that "technological arrangements can be designed in such a way as to eliminate —or, at least, reduce— the arbitrary influence of any single actor (including the state)."[2378] The authors draw an explicit parallel between the "rule of code" and "the rule of law," suggesting that the former represents a closer analogue to the rule of law that "stands in contrast to the arbitrary application of the *rule by code* by ensuring that no sovereign is

2371 Primavera De Filippi & Aaron Wright, *Regulating Decentralized, Blockchain Based Systems*, in Blockchain and the Law: The Rule of Code, 173, 174 (2018) [hereinafter *Regulating Decentralized Systems*].

2372 *Id.*, at 7.

2373 *Id.* at 55, 210, 280

2374 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370, at 1238.

2375 *Id.* at 1244.

2376 *Id.* at 1243-1244.

2377 The expression "rule of code" was introduced by Primavera De Filippi & Aaron Wright, *see* De Filippi & Wright, *Regulating Decentralized Systems*, *supra* note 2371, at 173-74.

2378 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370, at 1248.

above the code."[2379] At the same time, they acknowledge that the "rule of code" "does not provide normative conditions to guarantee the legitimacy of its rules and could, therefore, lead to situations that are contrary to the general interest."[2380] Reliance on the "rule of code" thus presupposes the existence of credible and democratically accountable mechanisms of governance for the technological infrastructure itself.[2381]

FIGURE 56.

Rule *of* code and rule *by* code

In their book, *Blockchain Governance*,[2382] De Filippi, Mannan, and Reijers distinguish various concepts:

- *Rule of law* refers to "a system for governing human behavior whereby the laws are written down and applied equally to everyone, including the sovereign who remains accountable under the law."[2383]
- *Rule by law* is where "rules are applied arbitrarily and unevenly, at the sovereign's discretion."[2384]
- *Rule by code* or *regulation by code* is when rules are embedded in the technological infrastructure of online platforms and networks.[2385]
- *Rule of code* "refers to a system for governing human behavior that is based on a series of code-based rules that apply equally to everyone, regardless of their identity or role."[2386]

The design of democratically accountable mechanisms of governance inevitably relies on experts and developers. Blockchain architectures remain the product of human design choices, while code functions as the primary instrument through which behavior is constrained or enabled. In this respect, developers exercise a form of discretionary power over the creation and evolution of these systems. While the question of whether developers can be held legally liable for software they create but do not operate remains unresolved, the broader issue of their institutional accountability is unavoidable. The shift from legal to architectural governance therefore reframes, rather than eliminates, classic questions of legitimacy, accountability, and control.

8.1.3. Qualifying the Alegality Thesis

Chapter 6 underscored the misalignment between traditional regulatory paradigms and the structural characteristics of blockchain technology. Whereas legal entities possess identifiable geographic and institutional anchors, blockchain networks operate through globally distributed nodes that transcend jurisdictional boundaries. While traditional intermediaries, such as banks, can be held accountable for compliance failures, decentralized protocols lack a single actor vested with both the authority and the technical capability to ensure compliance. Moreover, the rise of privacy-enhancing technologies has further complicated the identification of potential infringers and the attribution of responsibility.

Yet the assumption that blockchain systems exist beyond law's reach requires qualification. Although

2379 *Id.* at 1248.
2380 *Id.* at 1249.
2381 *Id.* at 1247 (discussing the need for polycentric governance mechanisms in blockchain regulation).
2382 Primavera De Filippi, Wessel Reijers & Morshed Mannan, Blockchain Governance, 69, 70 (2024).
2383 *Id.* at 69.
2384 *Id.*
2385 *Id.*, at 64.
2386 *Id.*, at 69-70.

blockchain protocols may appear to operate outside the immediate scope of traditional legal frameworks – owing to their immutable deployment, pseudonymous governance structures, and self-executing smart contract architecture– this does not entail a complete "collapse of traditional regulatory chokepoints."[2387] Law reasserts itself –not at the protocol layer, but– at the points where blockchain systems intersect with human actors, markets, and institutions.[2388] It does so through judicial proceedings, as evidenced by the growing body of U.S. case law concerning DAOs *(See section 6.4.)*; through criminal enforcement, as illustrated by the prosecution of Tornado Cash's founders *(See section 6.5.3.B.)*; and through legislative initiatives aimed at both remedying regulatory gaps and fostering the responsible development of blockchain technologies, as exemplified by the EU's Markets in Crypto-Assets (MiCA) Regulation *(See section 7.3.4.B.)*.

While blockchain technology aspires to eliminate intermediaries, it has generated new categories of actors: developers who design and maintain code; validators or miners who secure the network and operate the consensus layer; protocol foundations that finance and coordinate upgrades; token holders who participate in governance; and oracles that supply external data to smart contracts. Together, these actors shape and govern blockchain ecosystems by operating software, setting standards, enforcing protocol rules, and resolving disputes. Despite their often informal and transnational nature, they are not beyond the reach of law, as an expanding body of case law increasingly addresses their potential liability *(See section 6.3.)*.

Recent legislative initiatives further demonstrate lawmakers' continued reliance on the well-established strategy of regulating regulatory "chokepoints," as new forms of intermediaries have emerged, including exchanges, wallet providers, and crypto-asset issuers. The Markets in Crypto-Assets Regulation (MiCA) exemplifies this approach by centering regulatory obligations on crypto-asset service providers (CASPs) –that is, entities offering services functionally analogous to those performed by traditional financial intermediaries *(See section 7.3.4.B.)*.

A more structurally novel strategy consists in granting legal recognition to decentralized entities themselves, rather than regulating blockchain ecosystems primarily through intermediaries. This approach is illustrated by the emergence of DAO-specific statutory frameworks, inspired by the DAO Model Law *(See section 7.3.1.A.)*. These frameworks seek to anchor decentralized governance arrangements within existing legal systems while preserving a degree of organizational autonomy. However, although the COALA Model Law contemplates recognition of DAOs as legal entities without registration or human involvement, all regimes enacted to date retain a mandatory human-controlled entry point to legal recognition *(See section 7.3.1.E.)*. This structural choice reflects regulators' continued reliance on identifiable points of contact and accountability, even as they experiment with DAO-native entity forms.

While blockchain systems do not appear to operate in a state of alegality, jurisdictions adopt divergent regulatory strategies. For instance, some caution that states seeking

2387 Richard Fair observed that the smart contract infrastructure enables transactions to be executed autonomously through self-executing scripts without centralized oversight or ongoing developer involvement. This, he said, represents a transfer of control from human intermediaries to immutable code. He concludes that this transformation removes the chokepoints on which traditional financial regulation has long relied. Richard Fair, *Taxing Code, Not People: Behavioral Compliance For The Decentralized Future,* 32 MICH. TECH. L. REV. (forthcoming 2025), manuscript at 3. https://ssrn.com/abstract=5283918. According to Fair, an effective and sustainable enforcement strategy must, therefore, address the "transactional logic and automated execution layer," rather than focusing solely on its downstream effects. *Id*. at 10. He proposes two complementary measures: (1) imposing Pigouvian taxes on high-risk transactions directly at the smart contract level, and (2) requiring federal registration of all smart contracts in order to embed behavioral nudges, reputational incentives, and risk-tiered transparency into the foundational layer of decentralized finance. *Id*. at 1, 3-4, 24-27.

2388 De Filippi, Mannan & Reijers., *The Alegality of Blockchain Technology*, *supra* note 2369. *See also*: Andrew M. Hinkes, *The Limits of Code Deference*, 46 J. CORP. L. 869 (2021), https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Hinkes_Final_Web_0.pdf

to attract the incorporation of DAOs may offer increasingly relaxed regulatory frameworks,[2389] a dynamic that risks triggering a deregulatory "race to the bottom," potentially undermining consumer protection.[2390] The resulting landscape is best characterized as one of regulatory pluralism rather than alegality. The central challenge lies in developing legal regimes that simultaneously promote technological innovation while safeguarding consumer protection, financial stability, and market integrity.

8.1.4. The Persistence of Regulatory Gaps

The preceding developments show that blockchain is neither fully autonomous nor entirely beyond the reach of the law. The contemporary regulatory landscape is best characterized –not by the absence of legal frameworks but– by a condition of structural incompleteness. Across jurisdictions, the courts, lawmakers, and regulators have extended existing legal categories, created bespoke regimes, and experimented with new institutional tools. Yet the reach of law remains more limited and more fragile than in traditional centralized environments. Persistent regulatory gaps stem from a structural mismatch between the features of decentralized technological architectures and regulatory models historically built around identifiable actors.

A first persistent issue concerns the legal status and effects of computer code. As discussed in Chapter 6, courts are increasingly required to assess whether, and to what extent, smart contracts and protocol-level software can generate or express legally relevant obligations *(See section 6.2.)*. In most jurisdictions, code is not treated as an autonomous source of normativity but as a technical instrument whose legal significance depends on its connection to off-chain agreements or statutory frameworks. This preserves continuity with contract doctrine, yet leaves unresolved how to analyze systems in which no parallel natural-language contract exists or where execution occurs automatically without any practical possibility of human intervention. The resulting uncertainty is compounded by the fact that these questions are largely left to case-by-case judicial interpretation. Courts confronting this challenge have reached inconsistent results: In *Mango Markets* and *Platypus*, tribunals grappled with how to apply existing criminal law frameworks, reaching similar outcomes through divergent legal reasoning as to whether exploiting a protocol's own rules could constitute criminal misconduct; in *Peraire-Bueno*, a mistrial left unresolved whether manipulating transaction ordering within blockchain infrastructure constitutes fraud *(See sections 6.2.2. to 6.2.4.)*. These divergences confirm that technical compliance with protocol rules does not displace legal standards –yet existing doctrines of fraud and market manipulation, developed for conventional markets, do not translate cleanly into decentralized environments where conduct is mediated by code rather than by identifiable intermediaries.

In the *Tornado Cash* litigation *(See Section 6.5.3.)*, the U.S. Court of Appeals for the Fifth Circuit drew a clear legal distinction between immutable and mutable smart contracts. It held that immutable smart contracts cannot, under the applicable sanction framework, be legally treated as "contracts" or "services" because they operate autonomously and beyond the control of any party, including their original developers, who have irrevocably relinquished control upon deployment. This reasoning applied only to immutable contracts and left unresolved whether mutable contracts –those still subject to human modification– could fall within the scope of sanctionable property. The Fifth Circuit also declined to determine whether Tornado Cash qualified as an "entity"

2389 Lynn M. LoPucki, *Algorithmic Entities*, 95 WASH. U. L. REV. 887, 889 (2018), https://journals.library.wustl.edu/lawreview/article/3143/galley/19976/view/; Lynn M. LoPucki, *Corporate Charter Competition*, 102 MINN. L. REV. 2101, 2103-04 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2018/06/LoPucki_MLR.pdf.

2390 See, disagreeing: Matt Blaszczyk, *Decentralized Autonomous Organizations and Regulatory Competition: A Race Without a Cause,* 99 N.D. L. REV. 107 (2024), https://ssrn.com/abstract=4509636. Blaszczyk argues that the "race to the bottom" thesis fails in the DAO context because, unlike traditional corporations, DAOs lack centralized management and territorial nexus, making jurisdictional competition structurally different from the Delaware LLC incorporation phenomenon. *Id*. at 118-22.

or whether it had an "interest" in the immutable smart contracts. As a result, the legal status of mutable smart contracts and DAOs as sanctionable entities remains uncertain. The *Tornado Cash* decision supports the view that truly autonomous, decentralized code may occupy a zone of alegality existing beyond the state's direct capacity for regulation or control. The court stressed that any extension of statutory authority to decentralized technologies must come from Congress rather than the executive. Yet the case simultaneously underscores that human actors remain within the reach of the law, as Tornado Cash's founders were criminally prosecuted.

A second gap lies in the treatment of decentralized governance structures. While a growing number of jurisdictions recognize DAOs through dedicated statutes or adapted corporate forms, these regimes almost invariably presuppose a moment of human-mediated formation, registration, or representation *(See section 7.3.1.)*. In the U.S., Wyoming's Decentralized Unincorporated Nonprofit Association (DUNA), Utah's Limited Liability Decentralized Autonomous Organization (LLD), and New Hampshire's code-deferential registry-based model, each illustrate this pattern. However technologically sophisticated, each enacted framework retains a mandatory human-mediated gateway to legal recognition. Even the COALA Model Law *(See section 7.3.1.A.)* –the most ambitious attempt to design a protocol-first regime granting automatic legal personhood– has not been adopted in its full form by any jurisdiction. Fully autonomous protocols that lack identifiable founders and evolve through permissionless participation do not fit easily within these templates. The gap between legislative design and technological reality is also visible in case law: Where no formal legal structure exists, U.S. courts have started to fill the vacuum by treating DAOs as unincorporated associations or general partnerships, as in *Ooki DAO*, *Sarcuni v. bZx DAO*, and *Samuels v. Lido DAO* *(See section 6.4.2.)*. These decisions suggest that at least some governance token holders —particularly those who actively participate in governance— may be exposed to joint and several liability. This consequence may deter participation and reveal how decentralization, far from shielding participants from legal accountability, may in some contexts expand the pool of potentially liable actors precisely because governance is distributed rather than eliminated.

Additionally, even technologically sophisticated regimes struggle to cover self-executing software and continue to focus primarily on intermediaries. The European Union's Markets in Crypto-Assets Regulation (MiCA), for example, establishes a comprehensive regime for crypto-asset issuance applicable to identifiable service providers yet expressly excludes activities conducted "in a fully decentralized manner without any intermediary" *(See section 7.3.4.B.)*. The EU Data Act *(See section 7.3.3.A.)* imposes design and governance requirements on smart contracts used in data-sharing arrangements. This Act shows that detailed regulatory obligations can be imposed on blockchain systems. Yet it simultaneously exposes the limits of this approach: Requirements such as access controls, safe termination, and interruption mechanisms conflict directly with the immutability and distributed governance that are core features of decentralized systems, to the point that the European Commission has proposed repealing Article 36 of the Data Act, which sets out essential requirements for smart contracts used in data-sharing arrangements. Similarly, eIDAS 2.0 *(See section 7.3.3.B.)*, while recognizing electronic ledgers and enabling blockchain-based identity solutions within the EU Digital Identity Wallet ecosystem, conditions this recognition on compliance with supervision and accountability requirements enforced through qualified trust service providers –thereby structurally favoring permissioned or hybrid architectures and reinforcing the role of institutional intermediaries. This design choice

reflects a broader pattern: Even the most advanced regulatory frameworks remain anchored at the edges of decentralized systems, regulating the actors who interface with them rather than the self-executing software at their core. This situation generates legal uncertainty, as residual questions are left to the courts.

Finally, these structural mismatches are compounded by cross-border fragmentation. Blockchain networks operate transnationally, while regulatory frameworks remain territorially bounded and conceptually diverse. Differences in asset classification, applicable law, and jurisdictional reach generate conflicts that neither private international law adaptations nor international soft-law instruments have fully resolved. Switzerland has introduced blockchain-specific rules in its private international law *(See section 7.3.2.A.)*, and UNIDROIT has developed principles aimed at promoting greater harmonization in the treatment of digital assets across jurisdictions *(See section 7.3.2.B.)* –yet these initiatives remain partial and non-binding and have not prevented the divergent judicial approaches documented in Chapter 6.

These observations reveal several fundamental structural tensions at the heart of blockchain governance. While some claim that blockchain technology exists in a state of alegality, law inevitably reasserts itself –though incompletely and unevenly across jurisdictions. However, although law is increasingly present in the blockchain space, it remains anchored in assumptions of centralization, intermediaries, and human control. Regulatory responses struggle to accommodate the technical features of blockchain systems. Consequently, they may either stifle innovation through overly broad or restrictive requirements or create regulatory gaps by relying on frameworks ill-suited to decentralized and rapidly evolving architectures. Until regulatory frameworks develop credible ways to address responsibility, accountability, and coordination in environments where such assumptions no longer hold, genuinely decentralized and permissionless blockchain systems will continue to inhabit a space of persistent, partial, and unstable legality.

These legal tensions, moreover, mirror deeper contradictions within the technology itself: The technology promises to eliminate intermediaries and distribute power; yet, in practice, it reconcentrates control among developers, validators, and large token holders. It aspires to operate through a "rule of code" that mirrors the rule of law; yet, it lacks the democratic legitimacy and accountability mechanisms that underpin legal systems. Any effective governance framework must, therefore, address these contradictions rather than attempt to eliminate them.

8.2. POLICY ORIENTATIONS

Chapter 7 surveyed the diverse approaches adopted across jurisdictions to manage these blockchain governance tensions; yet, fundamental questions persist regarding both the aims and mechanisms of blockchain regulation. Should regulatory efforts simply transpose existing legal rules and principles onto the blockchain environment? Should they pursue objectives specifically tailored to the technology's structural features, such as ensuring the accountability of blockchain stakeholders and intermediaries? Methodological questions also arise: Through what means could regulation of blockchain systems be effectively implemented and, would such efforts require new forms of regulatory organization?

In practice, existing regulatory efforts still tend to concentrate on the most accessible points of intervention, such as cryptocurrency exchanges or custodial wallet providers. Yet examples ranging from the *Tornado Cash* ruling to MiCA's exclusion of fully decentralized systems show that a strategy focusing exclusively on such chokepoints is necessarily limited. Many scholars argue

that blockchain technology cannot be governed through the same regulatory logic that has historically guided internet regulation. Instead, they contend, it requires a dedicated, custom-made approach.[2391] In this context, the available policy options must be considered methodically by successively addressing the various steps of a viable strategy: First, identify which regulatory methods, if any, should be prioritized; and second, define the core regulatory objectives of blockchain regulation.

8.2.1. Exploring New Regulatory Methods

The structural tensions identified in the previous section cannot be resolved solely through incremental adjustments to existing regulatory models. Alternative strategies are required, whether through hybrid regulatory frameworks or through new forms of governance, such as "regulation by governance." This section examines these emerging approaches and assesses their potential to address blockchain's governance challenges.

8.2.1.A. Hybrid Regulatory Frameworks

The notion of hybrid regulation has gained increasing attention in blockchain scholarship, yet the concept itself still requires clarification and definition. Most analyses start from the premise that blockchain governance demands new regulatory taxonomies and conceptual structures.[2392] Building on this idea, several scholars argue for hybrid regulatory models –models that combine elements of different governance approaches[2393] or that integrate computer code with traditional legal rules.

This approach draws on the concept of "smart regulation" developed by Gunningham and Grabosky.[2394] They articulated a set of design principles centered on parsimony in the introduction of policy interventions and the promotion of multiple complementary instruments. Smart regulation also implies the involvement of a wide range of industry actors to encourage good practices and even voluntary compliance beyond legal minimums. Within this approach, regulators are encouraged to deploy a mix of instruments –legal rules, codes of conduct, technical standards, incentives, and transparency requirements– structured in a way that harnesses different capabilities while keeping regulatory burdens as light as possible.

In this perspective, some blockchain scholars suggest that regulatory regimes for blockchain should be based on differentiated oversight calibrated to the risk profile of specific blockchain activities.[2395] For instance, high-risk activities would be subjected to more stringent supervision, including prior authorization and continuous monitoring. Lower-risk activities would fall under lighter, primarily ex post controls. This tiered approach would allow regulators to allocate oversight resources more efficiently and avoid imposing unnecessary constraints on innovation. Comparable logic already exists in other areas of technology regulation, such as the EU AI Act.[2396] Yet, its application to blockchain raises open questions: How should risk levels be defined and measured in this context? How could such a regime be adapted to decentralized systems? And would it meaningfully address the challenges posed by fully automated protocols?

2391 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370 at 1267.

2392 Ben Charoenwong et al., *Blockchain Compliance: A Framework for Evaluating Regulatory Approaches* 14 (INSEAD, Working Paper No. 2025/46/FIN, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5368708., at 16; Shlomit Azgad-Tromer, Joey Garcia & Eran Tromer, *The Case for On Chain Privacy and Compliance*, 6 Stan. J. Blockchain L. & Pol'y 1-2 (2023). https://ssrn.com/abstract=4492919

2393 Charoenwong et al., *id.* at 36-37.

2394 Neil Gunningham, Peter N. Grabosky & Darren Sinclair, Smart Regulation: Designing Environmental Policy 37–42 (Oxford Univ. Press 1998).

2395 Charoenwong et al., *supra* note 2392 at 41.

2396 Florence G'sell, *Regulating Under Uncertainty: Governance Options for Generative AI* 213 (Stanford, 2024), https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai.

Another way to understand "hybridity" in blockchain governance is as a combination of code-based and legal oversight. Decentralized architectures offer distinctive governance affordances that are difficult to replicate in legacy systems. In particular, they enable forms of "embedded regulation," whereby rules are encoded directly into protocol design and enforced automatically through consensus mechanisms. This can enhance predictability, reduce reliance on discretionary enforcement, and lower certain coordination costs. While pure "rule by code" is neither practically feasible nor normatively desirable, a hybrid model is conceivable –one in which identifiable actors within the blockchain ecosystem remain subject to legal obligations, while certain regulatory requirements are embedded directly into the protocol itself.[2397]

In such a system, regulatory requirements can be implemented through smart contracts or protocol design, preventing non-compliant behavior ex ante rather than relying solely on after-the-fact enforcement.[2398] For example, data-protection safeguards can be built into the protocol itself.[2399] One recent paper shows that privacy-preserving compliance mechanisms can be integrated directly into a stablecoin's distributed ledger, allowing transactions to remain highly private while still satisfying compliance requirements.[2400] Rather than relying on off-chain intermediaries, this model incorporates compliance checks —such as sanctions-list screening and identity verification— into the core protocol itself. As the authors explain, this "compliance-by-design" architecture embeds regulatory controls within the ledger's technical infrastructure, enabling a more effective balance between transactional privacy and regulatory transparency.

8.2.1.B. Regulation Through Governance

Another policy option for blockchain is what some scholars describe as "regulation via governance."[2401] Rather than focusing on regulatory chokepoints, this approach seeks to exert legal pressure on off-chain structures and on the social norms that shape behavior within blockchain communities.[2402] It rests on the observation that no external authority can unilaterally modify blockchain code. Accordingly, regulatory interventions should target the off-chain layer – specifically by influencing the social norms that guide a community's design and governance choices.[2403]

This "*polycentric form of governance*" builds on the distinction between *off-chain* and *on-chain* governance *(See section 3.2.)*. *On-chain governance* combines internal architectural rules with external market dynamics shaped by mechanism design and game-theoretic incentives.[2404] *Off-chain governance* encompasses both *endogenous social norms* (the rules and procedures adopted and promoted within a blockchain community)

2397 Hanna Halaburda, *The hidden danger of re-centralization in blockchain platforms*, Brookings (April 10, 2025), https://www.brookings.edu/articles/the-hidden-danger-of-re-centralization-in-blockchain-platforms/ (last visited Jan. 15, 2026). See also: Thibault Schrepel, *Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia* (November 12, 2019). in General Principles and Digitalisation (Hart Publishing, 2020), https://ssrn.com/abstract=3485436; Thibault Schrepel and Vitalik Buterin, *Blockchain Code as Antitrust* (May 18, 2020). Berkeley Technology Law Journal, https://ssrn.com/abstract=3597399.

2398 Thibault Schrepel & Vitalik Buterin, *Blockchain Code as Antitrust*, 35 Berkeley Tech. L.J. 1, 11–12 (2021), https://btlj.org/wp-content/uploads/2023/04/Schrepel_FinalProof_04-11-23.pdf.

2399 As illustrated by Privacy Pools, a smart-contract-based privacy-enhancing mechanism; *See* Vitalik Buterin, et al., *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium* (Sept. 6, 2023), https://ssrn.com/abstract=4563364.

2400 Darrell Duffie et al., *A Note on Privacy and Compliance for Stablecoins* (Stan. Grad. Sch. of Bus., Rsch. Paper, May 5, 2025), https://ssrn.com/abstract=5242230. *See also* Andrea Rizzini et al., *A Private Smart Wallet with Probabilistic Compliance*, *in* 2025 IEEE Int'l Conf. on Decentralized Appl. & Infrastructures (DAPPS) 101, 101–10 (2025), https://doi.org/10.1109/DAPPS65174.2025.00021

2401 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370, at 1232-33.

2402 *Id*. at 1277.

2403 *Id*., at 1273-74.

2404 *Id*., at 1260-61, 1273.

and *exogenous legal pressures* that may influence or constrain those norms.[2405] Within this structure, regulators could influence the rules and practices adopted by blockchain communities by indirectly applying legal and regulatory incentives. In other words, they could identify and leverage pressure points capable of shaping both community governance and technical design.

Proponents illustrate this with the 'Parity bug incident' on the Ethereum network. A vulnerability in a library of reusable smart contracts —code that multiple wallet contracts referenced to perform key functions— allowed a user to accidentally trigger the library's self-destruct function. This rendered more than $300 million worth of Ether permanently inaccessible, as the wallet contracts could no longer execute the code needed to authorize withdrawals.[2406] Although some community members advocated for a hard fork to recover the funds, as had occurred in the case of The DAO *(See Figure 11 and section 6.2.1.A. above)*, the Ethereum community ultimately chose not to intervene. Legal considerations played a significant role in this outcome. While some community members supported the creation of a standardized procedure for fund recovery, key core developers and prominent members of the Ethereum Foundation warned that modifying the protocol to release the funds could expose them to legal risk.[2407] The refusal to alter the protocol thus reflected not only a principled commitment to immutability but also a desire to avoid legal liability —considerations that ultimately outweighed competing arguments, such as the need to compensate the victims.[2408]

However, this example does not necessarily demonstrate an effective or reliable regulatory strategy. If fiduciary duties were clearly imposed on core developers –as argued in the Tulip case *(See Section 6.3.2.A.)*– such obligations would be direct and enforceable. By contrast, in the Parity bug case, the refusal to intervene was allegedly justified by concerns about potential legal exposure; but, nothing indicates that such a choice was legally compelled. Although it is intellectually appealing to regulate blockchain systems by exerting indirect legal pressure on key decision makers, the idea remains largely theoretical —particularly given the opaque and often diffuse nature of decision making within blockchain ecosystems *(See Chapter 3)*. It is doubtful that a "global, pluralist and polycentric legal system"[2409] alone could address the structural challenges that persist in blockchain governance today, including imperfect decentralization, plutocratic control, and the absence of meaningful accountability.

8.2.2. Defining Core Regulatory Objectives

Having examined alternative regulatory methods, attention must now turn to defining what such regulation should aim to achieve. Currently, it remains challenging to articulate a definitive model for the governance or regulation of blockchain —a model capable of addressing both the technology's structural challenges and the difficulties arising from its partially alegal status. Rather than prematurely prescribing a specific regulatory method or comprehensive regime, it is, therefore, useful to begin by clarifying the core objectives that such a regime should pursue.

2405 *Id.*, at 1273-74.

2406 In fact, after an initial bug allowed hackers to steal $32 million from several multi-signature wallets, Parity launched an intensive coding and security effort to fix the vulnerability. However, the patch unintentionally introduced a second flaw that enabled a single user to become the sole owner of every multi-signature wallet. The user appears to have triggered the flaw accidentally and, upon realizing the consequences, attempted to undo the damage by deleting the relevant code. But this action permanently froze all funds held in those wallets, with no possible means of recovery. The total loss was estimated at approximately $300 million. Alex Hern, *$300 million in cryptocurrency accidentally lost forever due to bug*, The Guardian (Nov. 8, 2017) https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether

2407 For example, one Ethereum developer resigned from their role as a GitHub editor, expressing concern that an Ethereum Improvement Proposal (EIP) over a standardized format for lost fund recovery would potentially violate Japanese law. Rachel-Rose O'Leary, *Ethereum Developer Resigns as Code Editor Citing Legal Concerns*, CoinDesk (Feb. 15, 2018), https://www.coindesk.com/markets/2018/02/15/ethereum-developer-resigns-as-code-editor-citing-legal-concerns.

2408 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370, at 1276.

2409 *Id.*, at 1229,1260-61.

Two priorities emerge. First, policymakers must develop mechanisms to ensure —or at least incentivize— sound governance within blockchain systems. Second, it is essential to reduce the legal uncertainty that continues to impede the broader development and adoption of the technology.

8.2.2.A. Promoting Sound Governance in Decentralized Systems

Chapter 3 underscored the structural governance challenges inherent in decentralized systems, particularly the tendency for decision-making power to be concentrated in the hands of a few actors. In practice, the growing influence of large mining pools and concentrated governance token holdings have shifted control away from dispersed participants and toward a small group of dominant entities *(See section 1.2.)*. This dynamic of "re-centralization"[2410] stands in clear tension with the foundational goals of blockchain technology.

Against this backdrop, policymakers may seek to ensure that appropriate governance principles are embedded within blockchain systems. Importantly, doing so does not necessarily require formal regulatory intervention: Sound governance may also be promoted through non-binding guidelines and other forms of soft law, either alongside or in place of more prescriptive regulatory measures.

1. Guidelines and non-mandatory principles

Although scholarship on blockchain governance is now extensive,[2411] there is still no consensus on what "sound governance" should entail for decentralized systems. Governments, regulators, and research institutions, therefore, have a critical role to play in advancing conceptual thinking, testing governance models in practice, and assessing their impact on security, decentralization, and accountability.[2412] Well-designed governance principles must be clearly articulated, broadly disseminated, and actively promoted if they are to support meaningful implementation across the ecosystem.

In this regard, voluntary structures may be more appropriate than traditional command-and-control regulation, given the decentralized architecture of blockchain systems and the practical difficulty of enforcing binding rules across distributed networks.[2413] One promising pathway would be to develop voluntary governance standards inspired by existing disclosure regimes, such as the Global Reporting Initiative (GRI) Standards.[2414] Established in response to major environmental and corporate governance scandals, the GRI introduced the first global sustainability reporting regime, defining what companies should disclose and how such disclosures should be structured. Today, many organizations rely on GRI standards, which function as de facto requirements because investors, stock exchanges, and regulators expect them to.

Blockchain ecosystems could benefit from a similar system of voluntary standards, though significant adaptations would be necessary. Unlike traditional corporations with identifiable management and institutional investors, blockchain protocols often operate through pseudonymous participation and lack centralized entities with reputational stakes. Nevertheless, projects seeking legitimacy, institutional investment, or listing on regulated exchanges

2410 Halaburda, *supra* note 2397.

2411 See, for instance, Miles Jennings, *Machiavelli for DAOs: designing effective decentralized governance*, A16ZCRYPTO, (Sept. 21, 2023) https://a16zcrypto.com/posts/article/machiavelli-daos-designing-effective-decentralized-governance/.

2412 Halaburda, *supra* note 2397.

2413 *Id.*

2414 *See* Chris Brummer, *Disclosure, Dapps and DeFi*, 24 STAN. J.L. BUS. & FIN. 367, 370–75 (2019) (arguing that traditional regulatory mandates are ill-suited for decentralized systems and proposing disclosure-based frameworks as a viable alternative); *see also* De Filippi & Wright, *Regulating Decentralized, Blockchain Based Systems, supra* note 2371, at 172–89 (discussing the practical impossibility of enforcing "command-and-control" regulations on distributed networks).

may face market pressure to adopt governance standards. In this context, rather than imposing binding rules, policymakers and industry actors could jointly develop voluntary governance standards. These standards could, for example, encourage issuers of governance tokens to publish transparent information about voting mechanisms, token distribution, and other governance features.[2415]

2. Targeted Mandatory Requirements

Although regulation of blockchain governance may seem appealing, it requires careful consideration. Decentralized systems do not align easily with traditional regulatory tools, and direct legal intervention may generate unintended consequences: It could deter innovation and drive away projects to more permissive jurisdictions or even undermine decentralization by reintroducing regulated intermediaries.[2416] At the same time, governance crises driven by concentrated token ownership *(See Chapter 3)* show that blockchain networks cannot rely on self-correction alone. Without greater transparency in token distribution and voting mechanisms, decision-making power will continue to reconsolidate in the hands of a few actors.[2417]

Against this backdrop, policymakers could consider targeted interventions designed to reinforce decentralization and prevent the re-emergence of intermediaries and gatekeepers.[2418] They might, for example, explore measures that limit the monopolization of governance tokens or constrain the influence of any single actor. Of course**,** the enforcement of such measures would probably face practical challenges given the pseudonymous nature of blockchain participation and the difficulty of identifying who controls what across distributed networks. These measures would likely prove enforceable only against actors who surface through interaction with regulated intermediaries or who otherwise maintain identifiable off-chain presences. Within this context, mandatory governance requirements would function primarily as extensions of the chokepoint strategy rather than comprehensive solutions.

Recognizing these constraints, three categories of targeted intervention merit consideration:

First, **transparency and disclosure requirements** could mandate public disclosure of governance-token distribution as well as the ownership and control structures of major validators and mining pools.[2419] Policymakers might draw inspiration from securities and corporate-governance tools —such as shareholder-disclosure rules— to reduce the risk of excessive control by dominant stakeholders.[2420] For example, DAOs could be subject to disclosure obligations modeled on U.S. Securities and Exchange Commission reporting rules for publicly traded companies, requiring periodic filings that detail token holder identities (or pseudonymous addresses), voting patterns, and governance participation rates.[2421] Such requirements would be most effective when applied to projects with identifiable development teams, foundations, or entities seeking listing on regulated platforms.

Second, **decentralization safeguards** could impose limits on the voting power any single entity may exercise[2422]

2415 Halaburda, *supra* note 2397.

2416 *Id.*

2417 *Id.*

2418 *Id.*

2419 *Id.*

2420 *Id.*

2421 *See* Tailored Shareholder Reports for Mutual Funds and Exchange-Traded Funds; Fee Information in Investment Company Advertisements, 87 Fed. Reg. 72,758 (Nov. 25, 2022) (establishing detailed disclosure frameworks for investment companies that could serve as a model for DAO reporting).

2422 See Eric A. Posner & E. Glen Weyl, *Quadratic Voting as Efficient Corporate Governance*, 81 U. Chi. L. Rev. 251 (2014), https://ssrn.com/abstract=2264245 (proposing regulatory mechanisms to limit the voting influence of concentrated wealth in corporate governance); *see also* Vitalik Buterin et al., *A Flexible Design for Funding Public Goods*, 65 Mgmt. Sci. 5171 (2019), https://arxiv.org/abs/1809.06421 (adapting Posner and Weyl's quadratic voting model to blockchain ecosystems to prevent wealth concentration).

or restrict the influence of validators when they control a disproportionate share of network resources.[2423] Such measures might include caps on per person ownership of governance tokens, mandatory delegation restrictions, or requirements that governance decisions achieve supermajorities across multiple stakeholder groups, rather than token-weighted majorities. Enforcement would likely depend on identity verification at regulated access points, such as exchanges or tokenization platforms.

Third, **anti-collusion rules** could prohibit dominant actors from coordinating their governance influence or forming alliances that undermine meaningful decentralization. *(See Section 3.3.)* This could involve disclosure of relationships among major token holders; prohibitions on vote-buying or coordinated voting arrangements, including agreements or implicit understandings that leave no traceable record; and, requirements that governance platforms implement technical mechanisms (such as commit-reveal voting schemes) to reduce coordination opportunities. Yet such rules would face particularly acute enforcement challenges: Coordination often occurs through informal off-chain channels, such as private communications and side agreements negotiated in closed forums that leave no documentary trail and fall outside the jurisdictional reach of any single regulator.

8.2.2.B. Reducing Legal Uncertainty

Several cases, such as The DAO hack *(See Figure 11 and section 6.2.1.A.)* or the Mango Markets incident *(See section 6.2.2.)*, have underscored the legal ambiguity that surrounds computer code in blockchain systems. The issue remains unresolved. Courts and regulators have yet to settle whether exploiting a code vulnerability to drain funds constitutes theft, fraud, or merely the use of the system as designed. Nor is there a clear answer as to whether the immutable smart contracts discussed in the *Tornado Cash* litigation have a legal status or whether developers or platform operators may be held liable when the code contains exploitable weaknesses or when the protocol facilitates unlawful activity.

It is important, therefore, that legislation clarify the legal status of blockchain computer code —both to address the challenges posed by code exploits that enable the misappropriation of funds *and* to delineate the obligations and potential liabilities of developers and other protocol participants. Although regulation is often criticized for restricting innovation, the current legal uncertainty —and the litigation it fuels— also produces a chilling effect that ultimately impedes innovation. One promising approach would be for legal frameworks to draw a clear distinction between speech (the publication of code) and conduct (the deployment of self-executing smart contracts) and to specify the liability implications associated with each. Legal frameworks should also clarify whether developers owe fiduciary duties and, if so, under which circumstances these duties arise.

Moreover, clarifying responsibility within blockchain ecosystems —which rely on new categories of intermediaries— is essential.[2424] In recent years, blockchain scholarship has increasingly turned to questions of liability, accountability, and governance.[2425] The current uncertainty is proving more harmful than beneficial for industry development and innovation. In practice, the legal status of token holders remains uncertain in most jurisdictions, despite extensive litigation in the United States *(See section 6.4.2.)*. Any attempt to

2423 Halaburda, *supra* note 2397.

2424 Allen, Lane & Poblet, *supra* note 2355 at 75-77.

2425 Aneta Napieralska & Przemyslaw Kepczynski. *Redefining Accountability: Navigating Legal Challenges of Participant Liability in Decentralized Autonomous Organizations*, ARXIV (Aug. 8, 2024), https://doi.org/10.48550/arXiv.2408.04717.; Halaburda, *supra* note 2397.

address liability must, therefore, consider the potential responsibility of all relevant stakeholders, particularly those capable of influencing protocol design, updates, or network operations. One possible approach would be to impose obligations or liabilities on actors with meaningful control —such as core developers, governance-token holders, or validators. Yet, such measures must be designed with caution: Overly broad or rigid liability rules risk encouraging recentralization,[2426] deterring participation in protocol development, and ultimately slowing innovation.

These objectives —promoting sound governance while reducing legal uncertainty— are ultimately interrelated. Clear legal frameworks can facilitate better governance by defining stakeholder responsibilities and accountability mechanisms. Conversely, improved governance practices may reduce the need for heavy-handed regulation by demonstrating that blockchain systems can self-regulate effectively within appropriate legal boundaries. The realization of these objectives at scale, however, depends on international coordination, a challenge examined in the following section.

8.2.3. International Coordination

Although legislative intervention may be necessary to promote sound governance in blockchain systems and reduce the legal uncertainty that continues to impede the ecosystem, lawmakers remain confined by the territorial scope of their authority. Blockchain networks, by contrast, are transnational, borderless, and structurally detached from any single legal order. As a result, unilateral national regulation risks fragmenting the legal landscape or encouraging developers to relocate to jurisdictions with minimal oversight. This dynamic is already visible: Many projects are incorporated or deployed in jurisdictions with minimal oversight, such as the Marshall Islands, or seek out legal environments perceived as offering greater regulatory clarity and flexibility, such as Singapore.

It is, therefore, desirable that meaningful international cooperation emerge in order to promote greater harmonization in the legal treatment of blockchain-related challenges and to support the governance and accountability objectives identified in Section 8.2.2.[2427] A useful starting point may be found in existing OECD-led coordination mechanisms, such as the Base Erosion and Profit Shifting (BEPS) initiative. Mandated by the G20, BEPS has produced a suite of soft-law standards designed to prevent tax avoidance by multinational enterprises.[2428] The BEPS governance model operates through the development of common standards to which states formally commit to implement but which remain non-binding in the traditional sense. Countries voluntarily align their domestic rules with these agreed upon international norms, yet the regime exerts meaningful pressure: Jurisdictions that fail to adopt or effectively implement the standards may face negative consequences ranging from reputational damage and inclusion on tax blacklists to restricted access to information-exchange networks. Although BEPS has faced criticism regarding its effectiveness and uneven implementation across jurisdictions, this governance model demonstrates how soft-law standards can influence domestic legislation without requiring formal treaties.

2426 De Filippi, Mannan & Reijers, *Blockchain Technology and the Rule of Code: Regulation via Governance, supra* note 2370, at 1272-73.

2427 Halaburda, *supra* note 2397.

2428 The OECD was mandated by the G20 finance ministers to develop and implement the Base Erosion and Profit Shifting (BEPS) project in response to growing concerns about corporate tax avoidance and the erosion of national tax bases. The initiative aims to strengthen the international tax system by reducing the ability of multinational enterprises to shift profits artificially to low-tax jurisdictions and thereby minimize their tax liabilities. Structured around fifteen action areas, the BEPS Action Plan led to the development of key measures, including revised transfer pricing guidance, changes to international tax treaties, and enhanced mechanisms for tax transparency and information exchange. In 2016, the OECD launched the Inclusive Framework on BEPS to broaden participation beyond OECD members and to ensure the consistent implementation of the agreed standards. While all 38 OECD member countries joined automatically, non-OECD jurisdictions have progressively adhered to the Framework. Today, the Inclusive Framework brings together 145 countries and jurisdictions that have committed to implementing the BEPS minimum standards.

The work of the Financial Action Task Force (FATF), an international AML standards-setting body,[2429] offers an even more directly relevant example. Although the FATF operates without a treaty or binding enforcement powers, compliance with its soft-law standards is monitored through a peer-review process known as mutual evaluations. Non-compliant jurisdictions may face significant reputational and economic consequences. Its standards have been adopted by more than 200 jurisdictions, making it the central standard-setter in the international financial regulatory landscape. However, FATF's so-called "Travel Rule"[2430] —requiring virtual asset service providers to collect, retain, and transmit identifying information about the originator and beneficiary of a transaction— has proven difficult to implement in practice, particularly for decentralized protocols lacking identifiable intermediaries. This implementation challenge foreshadows the difficulties of applying international coordination frameworks to truly decentralized blockchain systems.

Against this backdrop, the OECD has developed several blockchain-specific initiatives. It has published a series of analytical reports examining the implications of blockchain for corporate governance, digital identity, financial markets, and public administration. These studies highlight both the transformative potential of distributed ledgers and the regulatory challenges that arise from their decentralized and cross-border nature.[2431] The OECD has also analyzed the tokenization of assets, examining why a scalable market for tokenized financial instruments has yet to emerge and setting out policy considerations for financial supervisors and policymakers.[2432]

More importantly, the OECD issued a "Recommendation on Blockchain and Other Distributed Ledger Technologies" in 2022, providing high-level guidance to governments on the responsible development and adoption of blockchain systems. The Recommendation calls on governments to develop coordinated policy approaches for blockchain adoption, to foster research and innovation, build human capacity, support enabling regulatory environments, strengthen international cooperation, and ensure interoperability, transparency, privacy, security, and environmental sustainability in DLT systems.[2433] It further stresses that innovation-supportive regulatory regimes must be reconciled with risk mitigation and public-interest safeguards. The Recommendation's impact has so far been limited. It does not establish monitoring mechanisms, impose reporting obligations, or define measurable implementation benchmarks —omissions that significantly reduce its practical traction compared to instruments such as BEPS or the FATF standards.

To date, however, the most advanced OECD instrument in this field is the Crypto-Asset Reporting Framework (CARF), designed to provide tax authorities worldwide with the information needed to monitor crypto-asset revenues on a cross-border basis and ensure tax compliance.[2434] As of

2429 The FATF is a "soft law," intergovernmental standard-setting body in which states cooperate to develop and promote policies to combat money laundering, terrorist financing, and proliferation financing. Created by the G7 in 1989 in response to rising concerns about illicit financial flows, the FATF issues non-binding recommendations that member jurisdictions commit to implement domestically. Compliance is monitored through a peer-review process known as mutual evaluations, and non-compliant jurisdictions may face significant reputational and economic consequences. *See Fin. Action Task Force*, https://www.fatf-gafi.org/en/home.html (last visited Jan. 15, 2026).

2430 Financial Action Task Force, *The FATF Recommendations*, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html (last visited Jan. 15, 2026)

2431 OECD, *Blockchain at the frontier: Impacts and issues in cross-border co-operation and global governance*, (OECD Bus. & Fin. Pol'y Papers, No. 04, 2022), https://doi.org/10.1787/80e1f9bb-en.,

2432 OECD, *Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets* (Jan. 9, 2025), https://www.oecd.org/en/publications/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_40e7f217-en.html; see also OECD, *Improving the Digital Financial Literacy of Crypto-Asset Users* (Sept. 8, 2025), https://www.oecd.org/en/publications/improving-the-digital-financial-literacy-of-crypto-asset-users_19cfecad-en/full-report.html.

2433 OECD, *Recommendation of the Council on Blockchain and Other Distributed Ledger Technologies*, (June 10, 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0470.

2434 Rabihah Butler, *The Impact of CARF on the Global Cryptocurrency Industry*, Thomson Reuters (Sept. 12, 2025), https://www.thomsonreuters.com/en-us/posts/corporates/carf-global-cryptocurrency/.

this writing, more than sixty jurisdictions have committed to implement CARF. Under the regime, crypto-asset service providers will be required to collect detailed information about their customers and their transactions and report that information annually to domestic tax authorities. Tax authorities will then automatically exchange the information with their foreign counterparts. CARF will, therefore, impose new compliance obligations on the global crypto-asset industry, much like those already imposed on banks, insurers, and investment funds under the United States' Foreign Account Tax Compliance Act (FATCA)[2435] and the OECD's Common Reporting Standard (CRS).[2436]

Taken together, the OECD's work illustrates a governance strategy grounded in soft-law standards, voluntary alignment, and multi-stakeholder cooperation, rather than binding international treaties. Yet, its most developed and operational contribution so far concerns the tax treatment of crypto-assets, notably through CARF. International cooperation has not yet produced a comprehensive regime governing blockchain systems themselves or establishing the safeguards required to ensure their integrity. Future international efforts should prioritize the development of more substantive soft-law instruments —for example, rules mandating transparency in token distribution, disclosure of governance arrangements, and other accountability mechanisms needed to support resilient and equitable blockchain ecosystems.

Despite these promising developments, soft-law coordination faces inherent limitations, particularly in the blockchain context. Unlike tax compliance or anti-money laundering —where states share strong incentives to cooperate— blockchain regulation implicates competing national interests. Some jurisdictions actively compete to attract crypto innovation through light-touch regimes, while others prioritize strict investor protection or capital controls. This divergence of interests complicates consensus-building. Furthermore, even when consensus exists, geopolitical tensions and competing national interests in maintaining technological leadership may impede effective cooperation.

Beyond political challenges, difficulties in technical implementation persist. How can soft-law governance standards be meaningfully applied to truly decentralized protocols lacking identifiable operators or central points of enforcement? As the FATF Travel Rule experience demonstrates, international standards designed for traditional financial intermediaries do not easily translate to decentralized systems. Enforcement mechanisms that rely on identifiable service providers —such as exchanges or custodial wallets— ultimately revert to the chokepoint strategy discussed earlier in this chapter, leaving fully decentralized protocols beyond the reach of international coordination.

These questions suggest that, while international coordination is necessary, it may prove insufficient without parallel development of the sound governance incentives mentioned in Section 8.2.2.A. Effective blockchain governance will likely require a multi-layered approach: international standards, to prevent regulatory arbitrage and to harmonize baseline requirements; combined with domestic measures, targeting accessible intermediaries and industry-led governance improvements driven by market pressure and voluntary standards. No single strategy alone can address the full range of challenges posed by blockchain's decentralized, borderless architecture.

2435 I.R.S., *Foreign Account Tax Compliance Act (FATCA),* https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca (last visited Jan. 15, 2026).

2436 OECD, *Consolidated text of the Common Reporting Standard (2025): Standard for Automatic Exchange of Financial Account Information in Tax Matters* (June 2, 2025), https://www.oecd.org/en/publications/consolidated-text-of-the-common-reporting-standard-2025_055664b1-en.html.

8.3. CONCLUSION: THE BLOCKCHAIN GOVERNANCE CHALLENGE

This report has demonstrated that blockchain technology presents genuine challenges to traditional legal and regulatory frameworks that cannot be addressed through incremental adjustments to existing tools. Its decentralized architecture, transnational operation, and code-based governance create a structural misalignment with legal frameworks built around identifiable actors, territorial connections, and centralized control.

The analysis has revealed several fundamental tensions that resist resolution through traditional policy approaches. Blockchain technology aspires to decentralization yet consistently tends toward the reconcentration of power among a small number of dominant actors — developers, validators, and large token holders. It seeks to operate beyond the reach of law, yet legal orders continually reassert themselves, through litigation, enforcement actions, and targeted legislation, producing an uneven and often unpredictable overlay of rules across jurisdictions. It promises disintermediation, yet regulation inevitably gravitates toward the intermediaries that remain — exchanges, custodial wallet providers, and other identifiable chokepoints— leaving fully decentralized protocols largely beyond reach. These are not transitional frictions that will eventually be smoothed away with better regulation. They reflect structural features of the technology itself, and any credible governance framework must account for them as such.

The survey of regulatory approaches conducted in Chapter 7 reinforces this diagnosis. Whether jurisdictions have favored observation and regulatory sandboxes, regulation by enforcement, comprehensive ex ante frameworks, or outright prohibition, none has successfully resolved the fundamental tension between decentralized, permissionless systems and regulatory frameworks premised on identifiable intermediaries and centralized control. As a result, the most decentralized blockchain applications continue to operate in legal uncertainty, regardless of the regulatory approach adopted. This is not primarily a failure of regulatory ambition, but a structural constraint that no jurisdiction has yet overcome.

This report does not seek to resolve these issues. Its ambition is more modest and, at this stage, more appropriate: to map the landscape with sufficient precision that future regulatory responses —whether legislative, judicial, or industry-led— can rest on solid analytical foundations. The policy options mentioned in this chapter are not prescriptions but orientations: They identify where the most consequential choices lie, without prejudging how those choices should ultimately be made. Defining sound governance for decentralized systems, clarifying the legal status of computer code, and establishing meaningful accountability mechanisms are tasks that will require sustained deliberation among technologists, legal scholars, regulators, and the broader blockchain community. What this report has sought to establish is that such deliberation is both necessary and overdue.

What is clear is that blockchain technology will not regulate itself, nor can it be governed through paradigms designed for centralized institutions. Effective governance will emerge neither from the unilateral dominance of code over law nor from the wholesale imposition of legacy regulatory frameworks onto decentralized systems. It will require adaptive, principles-based approaches, developed through international coordination and informed by a clear-eyed understanding of the technology's structural features and inherent limitations — an understanding that this report has sought to contribute.

APPENDICES

APPENDICES TABLE OF CONTENTS

Appendix 1 - Hash functions	404
Appendix 2 - Public key cryptography	405
Appendix 3 – Byzantine generals problem	407
Appendix 4 - Soulbound tokens (SBTs)	407
Appendix 5 - Various types of DAOs	408
Appendix 6 - Zero-Knowledge Proof and the Ali Baba Cave	412
Appendix 7 - Examples of blockchain-based data-sharing	413
Appendix 8 - Provenance and traceability in automobile industry; the Vinturas case	416
Appendix 9 - Automation and trade finance in global shipping industry	417
Appendix 10 - Verification and compliance in supply chain sustainability	418
Appendix 11 - The Bitcoin Knots movement	419
Appendix 12 - Quadratic voting	420
Appendix 13 - Futarchy	422
Appendix 14 - Exit scams	423
Appendix 15 - Romance scams and wallet drainers	424
Appendix 16 - Malware delivery systems	425
Appendix 17 - Crypto assets and money transmission regulation in U.S. states	426
Appendix 18 - Japan	431
Appendix 19 - Singapore	433
Appendix 20 - Switzerland	435
Appendix 21 - India	440

APPENDICES

APPENDIX 1 - HASH FUNCTIONS

by Reuben Youngblom

A hash function is a mathematical operation that accepts an input of any length and deterministically returns a random-looking, fixed-length output. To paint with broad strokes, a hash function accepts as input some string of characters. This input string is called the *preimage*. A preimage can include letters, numbers, or special characters; they can be well-formed into beautiful words and sentences or be absolute gibberish. Upon accepting this input, the hash function will **calculate an output that looks completely random and is specially designed to obscure the input**.

Hash functions are commonly used to verify the integrity of a digital file during transmission: The sender inputs the file (i.e., its underlying binary data) into a hash function and transmits both the file and the resulting hash. If any part of the file has been tampered with, the binary representation will have changed, producing a different hash output and signaling that the file has been tampered with. The unique properties of hash functions enable some critical blockchain functionality, such as proof-of-work mining.

Key properties of hash functions include:

- **Fixed length**. A hash output must have a fixed length. Regardless of how long or short the *input* is, the *output* length does not vary.[2437] A typical hash output in a blockchain is somewhere between 32 and 64 characters. This is because any correlation between the length of the input and the length of the output could enable a surprising amount of significant information to be "leaked." This could make it possible for an analyst to determine the content of the original message. It is possible for hash inputs that are extremely long to be rendered into a 64-character output. Hiding the length of the input by fixing the length of the output is a useful option when considering that hashes are crafted to hide *any* information about the input (as opposed to simply obscuring the content of a message). (Note: "The hash output" is also known as simply "the *output*" or "the hash" and, depending on the context, is occasionally called "the *hash* of a given input.")
- **Avalanche Effect.** Algorithms used for hashing take great care to ensure that even "a minor change in the hash function's input will result in a significantly different output."[2438] This is known as the "Avalanche Effect." For instance, hashing the word "elephant" and then hashing the word "elephants" will return outputs that bear no resemblance to each other despite the inputs differing by only one letter.

2437 For reference, the SHA256 hash for the letter 'a' is 'ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb' (64 characters), while the hash for Articles 1-7 of the U.S. Constitution, according to https://constitutioncenter.org/the-constitution/full-text (last visited Jan. 15, 2026) is "808c06eb701005cca960a7620ca9125b5e00ee55af043a809fc943f9ecc7a38e" (64 characters).

2438 D. Upadhyay, N. Gaikwad, M. Zaman, and S. Sampalli, *Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications,* 10 IEEE Access, pp. 112472-112486, 2022, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9923931.

- **Determinism**. Hashes are *deterministic*: For any given hashing algorithm, the same input will always, without fail, result in the same output. Given the same inputs, different algorithms can produce different outputs. This ensures consistency when verifying things such as digital signatures or the validity of bitcoin blocks.
- **Preimage Resistance**. Hashes are highly resistant to preimage attacks.[2439] *Preimage resistance* suggests that "it is computationally infeasible to find any input which hashes to [any specific] output." More broadly: The input text cannot feasibly be determined by examining the output.[2440]

All of the above properties —fixed length, avalanche effect, determinism, preimage resistance— paint a picture of hash functions as being in a class of *One-Way Functions* (OWF). OWFs are functions "for which computation in one direction is straightforward, while computation in the reverse direction is far more difficult."[2441]

The term *hashpower* refers to a machine's capacity to hash a single block one time. It is typically quantified as the number of hashes a machine can compute per second. The term *hashpower* is commonly used in the context of Proof-of-Work (PoW) systems, where work is defined by the process of hashing block data *(See section 2.2.3.)*. The total of all hashpower in the network at any given time is known as the *hash rate.*

APPENDIX 2 - PUBLIC KEY CRYPTOGRAPHY

by Reuben Youngblom

Under *public key cryptography* (PKC), a public key[2442] is widely shared, while the associated private key is kept a closely-guarded secret. If a specific message is signed using a particular private key, the corresponding public key will verify the message without any alteration. Conversely, if the message verification fails —either because the content does not match the signature or because a different private key was used— it strongly indicates one of two possibilities: (a) the message was signed by a different private key or (b) the message has been tampered with after being signed. In either case, the failure of verification undermines the assertion that a specific private key holder authored the message in question or is authorized to see the message.

Cryptography (including PKC) often relies on *choosing a number that is so large that it is functionally impossible for anyone to guess* ***what the number is*** *out of an enormous field of possible combinations*. For example, if Alice is protecting an account and chooses a password that is simply a single digit between 0-9, and Bob wishes to guess her password, there are only 10 possibilities. He might take a mere few seconds to determine which single digit Alice used to secure her information. If, however, Alice chooses a massively large number (comprised of dozens of digits), the task of figuring out **which specific string of digits** is the correct password suddenly becomes much more challenging. Rather than relying

2439 In a "preimage attack", the attacker starts from a target hash h and tries to recover some input with Hash(x)=h. See, e.g., Secure Hash Algorithm, in *Encyclopedia of Cryptography and Security* 1162, 1163 (Henk C.A. van Tilborg & Sushil Jajodia eds., 2d ed. 2011) (defining preimage resistance as the property that, given a hash value *h*, it is computationally infeasible to find any input *x* such that *H*(*x*)=*h*), https://link.springer.com/referencework/10.1007/978-1-4419-5906-5.

2440 William R. Speirs, *Hash Functions*, Purdue Univ. CS 355 lecture notes, https://www.cs.purdue.edu/homes/ssw/cs355/hash.pdf (last visited Jan. 15, 2026).

2441 M.J.B. Robshaw, One-Way Function. in *Encyclopedia of Cryptography and Security* 1343 (H.C.A. van Tilborg & S. Jajodia eds., 2d ed. 2011), Springer, Boston, MA, https://doi.org/10.1007/978-1-4419-5906-5_467.

2442 Nat'l Inst. of Standards & Tech., *Computer Security Resource Ctr*., Public Key, https://csrc.nist.gov/glossary/term/public_key (last visited Jan. 15, 2026) (defining a public key as "the public part of an asymmetric key pair that is typically used to verify signatures or encrypt data").

on the "uniqueness" of a key or a password, many cryptographic primitives rely on the "unguessability" of enormous numbers.

Then this "secret" (or "private") number is used to generate another number —one that can be shared publicly without negative consequences. This is done using a deterministic algorithm such that anyone who randomly picks a specific first (private) number will always end up with the same second (public) number. Together, these two numbers comprise a *key pair*. The secret number is known as the *private key*. The second number, deterministically derived from the private key, is known as the *public key*. In PKC, these numbers are generated such that knowing the private key (or selecting a given private key) allows one to generate the associated public key; but, knowing the public key gives a user zero information about the private key. In other words, there is no danger of anyone learning the private key given only the public key.[2443]

These key pairs can be used for many things. The PKC action that is most relevant to blockchains is *digital signatures*. The keys are mathematically linked such that "signing" a message using a private key generates a mathematical "fingerprint" within the message that, when combined with a public key, reveals the original message. In other words, signing a message (whether the message is a transaction authorization, a communication, a vote, or anything else) assures anyone reading the message that, *if* a given public key is able to produce the original message, the signing entity knows the secret private key belonging to that specific public key (and is, therefore, very likely to be the entity behind a given private key).

This mechanism also serves as a way of verifying the integrity of a message. If a specific private key signs a specific message, it *will* be the case that the associated public key will retrieve the message with no alterations whatsoever. By contrast, if a private key produces a different message than what is expected, it must be the case that either a) the message was signed with a different private key; or b) the message was tampered with.

In Bitcoin, when one party wishes to send bitcoins to another party, the sender specifies the recipient's address as the destination. This address, which is generated through cryptographic transformations of the public key, designates where the cryptocurrency is transferred on the blockchain. Once the sender initiates the transaction and broadcasts it to the network, the blockchain validates and records the transaction. This locks the transferred value under cryptographic conditions (typically a script) that require a valid digital signature generated with the corresponding private key in order to spend it. Rather than associating two public keys directly, Bitcoin records Unspent Transaction Outputs (UTXOs) that can be unlocked only by satisfying these cryptographic conditions, thereby ensuring that the cryptocurrency can be spent solely by the controller of the relevant private key.

2443 This may seem impossible, but a naive analog is relatively easily illustrated using modular arithmetic. Modular arithmetic essentially takes the *remainder* of a division option. For example, 7 divided by 3 is 2 (with a remainder of 1), so, it can be said that 7 modulo 3 (often written as 7%3) is 1. And 9 modulo 5 is 4 (9%5=4); 11 modulo 3 is 2 (11%3=2). Now, consider the equation n%7 = x. It is intuitive to think of n as the private key, and x as the public key. Why? If Alice chooses a private key of 12, so that 12%7 = x, Alice can derive her public key (x) by simply taking the remainder of 12/7, which is five. Note that, given n%7 = x, anyone else who chooses an n of 12 will always get the same x of 5. In other words, the private key deterministically derives the public key. Now, imagine that Bob is given *all* of the possible information except which specific n Alice has chosen. Bob knows that the equation is n%7 = x, and Bob even knows that x = 5 (public keys, after all, are public). Can Bob actually derive Alice's private key given this information? The answer is no. Alice happened to choose 12, but there are *many* other numbers that satisfy n%7 = 5. For example, 19%7 is also equal to 5. 26%7 is equal to 5, as is 33%7. Alice happened to choose the most intuitive answer but, in a real-world setting, Alice could choose any number: say, 16728 or 65028794, or any of the 100-digit numbers that would satisfy this equation. In the territory of numbers that are so large as to be unguessable, it becomes clear how it is possible to have a number that can reliably, deterministically, derive another number such that the derived number cannot be used to determine the original number. However, please note that this is NOT a secure key generation algorithm; it is only to provide an intuitive explanation.

APPENDIX 3 - BYZANTINE GENERALS PROBLEM

by Reuben Youngblom

The general class of problems solved by proof of work is called the Byzantine Generals Problem. The Byzantine Generals Problem, popularized by Leslie Lamport, *et al.,* in a paper by the same name,[2444] deals with a long-standing question in computer science: As computers begin to operate as networked systems of connected nodes, what can be done to handle the inevitable issue of one or more nodes accidentally or intentionally sending incorrect information to the rest of the network?

As a thought experiment, Lamport painted a picture of the Byzantine army surrounding the enemy in such a way that each division of the army was commanded by its own general and separated from the other divisions. These generals could communicate with one another via a messenger, and their task was to agree upon a common course of action. The critical goal was to reach agreement on what to do. If some of the divisions attacked while others retreated and still others did nothing, the Byzantine army would suffer defeat. If all the divisions attacked or retreated in unison, the outcome would be more acceptable. In a magical world of pure intentions and perfect fidelity to the facts, there is no problem. If every general accurately conveyed their intention and every message was faithfully and accurately delivered, then reaching consensus would be fast and easy. In the real world, however, there are often problems: Messages get lost. Disloyal generals lie about their intentions in ways that can bring harm to the rest of the army. Messages sent in good faith fall prey to disgruntled messengers who tamper with their contents en route. Given these realities, is there a way to mitigate the harms caused by malicious actors?[2445]

This problem arises in distributed systems of all kinds, including blockchain networks. In Bitcoin, for instance, each node effectively serves as an autonomous Byzantine general. The goal is not exactly to come to a consensus around a plan of attack but to come to consensus around the question of which addresses control which bitcoins. The uncertainty surrounding the intentions of other nodes remains. In Bitcoin, given that it is a completely open, permissionless system, malicious actors are free to enter the network and send self-serving or otherwise destructive transactions in an attempt to control the chain.

APPENDIX 4 - SOULBOUND TOKENS (SBTs)

by Reuben Youngblom

Beyond non-fungible tokens (NFTs), a newer token standard has emerged in recent years: Soulbound Tokens, or SBTs. The concept of Soulbound Tokens was introduced in a May 2022 paper by Vitalik Buterin, E. Glen Weyl, and Puja Ohlhaver, titled *"Decentralized Society: Finding Web3's Soul."* The proposal drew inspiration from "soulbound" items in online games — items which cannot be transferred or traded. In the blockchain context, an SBT would be a non-transferable token permanently tied to a person's digital identity (their "soul").[2446]

While use cases for SBTs are still being figured out, the early notion was to employ them to help create a robust

2444 Leslie Lamport, Robert Shostak & Marshall Pease, *The Byzantine Generals Problem,* 4 ACM Trans. Programming Languages & Sys. 382 (1982), https://lamport.azurewebsites.net/pubs/byz.pdf.

2445 While the problem is more important than the solution here, it may be reassuring to know that there is, in fact, a solution: Given *m* traitors, the loyal generals can reliably reach consensus so long as there are *3m +1* loyal generals.

2446 Coinbase, *What are Soulbound Tokens (SBT)?* https://www.coinbase.com/learn/crypto-glossary/what-are-soulbound-tokens-sbt (last visited Dec. 31, 2025).

framework for decentralized identity or reputation.[2447] The authors argued that existing blockchain ecosystems focus too heavily on transferable, financialized assets (fungible tokens, NFTs, etc.) and neglect other forms of social value and identity. SBTs were envisioned to serve a number of different functions, such as: credentialing (e.g., academic degrees, professional licenses, certificates); reputation (e.g., proof of membership, community participation, or governance history); attestations (e.g., endorsements, affiliations, or certifications); and anti-Sybil mechanisms (preventing one individual from controlling many pseudonymous wallets in governance).[2448]

As a relatively new phenomenon, there is no widely adopted, standardized implementation of SBTs. Some pilot projects and experiments exist. For example, Binance launched an "Account Bound" SBT for KYC-verified users. Smaller projects have tested SBTs for academic diplomas or conference participation. Much of the development remains experimental and limited to niche use cases. Key challenges include privacy (permanence of sensitive data on-chain), recovery (what happens if someone loses their private keys?), and interoperability (different chains and communities might design incompatible versions).

SBTs are important in the discourse around blockchain and Web3 because they highlight unresolved questions about identity, trust, and non-financial uses of blockchain. They represent an attempt to expand blockchain utility beyond speculation and financial assets, toward a "Decentralized Society."

APPENDIX 5 - VARIOUS TYPES OF DAOs

by Ashok Ayyar

Decentralized autonomous organizations (DAOs) come in several different varieties. There is no official or universally accepted typology of DAOs, and DAO structures often evolve over time. Rather than classify DAOs based on their legal form, technical architecture, or degree of decentralization, the classification below categorizes DAOs according to their primary purpose.

One commonly cited taxonomy distinguishes six major types of DAOs[2449]: protocol DAOs, investment DAOs, grant DAOs, collector DAOs, service DAOs, and social DAOs. In practice, many DAOs are hybrids, combining features of two or more of these categories and frequently relying on off-chain legal entities or foundations to operate in the real world. In addition, more recent DAO forms have emerged and are briefly discussed at the end of this Appendix. While this six-part framework provides a useful point of departure, it remains imperfect: categories overlap, some have contracted significantly since the 2022 market downturn, and each raises distinct legal issues.

1. Protocol DAOs

Protocol DAOs are generally understood to be DAOs that govern, manage, or coordinate the development of blockchain-based protocols. In a typical configuration, token holders exercise governance rights —often through on-chain voting mechanisms— while protocol developers or core teams retain responsibility for implementation.

2447 Puja Ohlhaver et al., *Decentralized Society: Finding Web3's Soul* (working paper, Social Science Research Network), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763 (last visited Dec. 31, 2025).

2448 Andrey Sergeenkov, *What Are Soulbound Tokens? The Non-Transferrable NFT Explained*, CoinDesk (Sept. 7, 2022; updated May 11, 2023), https://www.coindesk.com/learn/what-are-soulbound-tokens-the-non-transferrable-nft-explained.

2449 Ellen Naudts, T*he Future of DAOs in Finance: In Need of Legal Status*, ECB Occasional Paper Series No. 331 (Oct. 16, 2023), https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf?ca341296edabc184a32dc15e30d3020b, at 11-12. Other sources list more types. Galaxy Research, *DAOs: The Future of Organizing Communities Online* (Nov. 23, 2021), https://www.galaxy.com/insights/research/daos/.

The earliest and most influential example of a protocol DAO was MakerDAO ("Maker") *(See Figure 33)*. Founded in 2014, it was first deployed on the Ethereum blockchain in December 2017. Maker uses smart contracts to enable users to lend and borrow cryptocurrency at variable interest rates in transactions secured by crypto collateral. MakerDAO provides governance for the Dai stablecoin (DAI). Holders of MKR tokens vote on requisite collateral ratios, choosing collateral types, adjusting interest rates and the protocol's "stability fee," or even triggering an emergency shutdown.[2450] In 2024, MakerDAO rebranded as Sky Protocol under its "Endgame" restructuring plan, introducing a new stablecoin (USDS) and governance token (SKY) alongside the legacy DAI and MKR, which continue to circulate.

Uniswap is another prominent example *(See Figure 28)*. Uniswap is a leading decentralized exchange that allows users to swap tokens directly without intermediaries. Uniswap's DAO primarily manages a substantial community treasury, determines the allocation of protocol fees, and awards ecosystem grants. While the DAO formally possesses governance authority, strategic and technical influence in practice continues to be shared with, or exercised by, core development teams and affiliated entities.

The Lido DAO *(See section 6.4.2.B.)* governs Lido Finance, a decentralized finance (DeFi) protocol offering liquid staking services for Ethereum's proof-of-stake consensus mechanism. Holders of Lido's governance token vote on key decisions affecting protocol operations, validator selection, and the allocation of resources. The DAO accrues service fees from the protocol and allocates those funds to research and development, liquidity incentives, and protocol upgrades.[2451] Lido has also been the subject of governance debates concerning validator concentration and effective decentralization, illustrating broader tensions within protocol DAOs.

2. Investment DAOs

Investment DAOs resemble traditional investment funds in that they pool capital for deployment. They differ in that investment decisions are typically made collectively by token holders rather than by centralized fund managers or general partners.[2452] Investment DAOs rely on smart contracts for capital pooling, governance, and distribution of proceeds, and may operate either with or without a formal legal wrapper. Some have dubbed them the "future of venture capital," with the potential to revolutionize startup investing through transparent, crowdsourced decision making.[2453]

Investment DAOs primarily invest in crypto-native assets, such as fungible tokens, non-fungible tokens (NFTs), or virtual real estate. Increasingly, they also invest in real-world assets (RWAs), which expose them to regulatory and compliance considerations beyond the blockchain ecosystem. They often raise funds by accepting ETH or other tokens into DAO smart contracts, issuing governance tokens in return. Many have a sector-specific focus, such as DeFi, GameFi, or creative industries.[2454] MetaCartel DAO is one such example. Some investment DAOs function more like investment clubs, where members collectively deliberate and vote on individual investment decisions rather than delegating that authority.

2450 Romex K. Jha, *Challenges of Effective Decision Making in Decentralized Autonomous Organizations (DAOs)*, 17 World J. Research & Rev. 18 (2023); MakerDAO whitepaper, *The Sky Protocol: Sky's Multi-Collateral Dai (MCD) System*, https://makerdao.com/en/whitepaper/#sky-protocol-auctions (last visited Jan. 15, 2026).

2451 Chainalysis, *Introduction to Decentralized Autonomous Organizations (DAOs)* (Apr. 7, 2023), https://www.chainalysis.com/blog/introduction-to-decentralized-autonomous-organizations-daos/.

2452 Ivan Fan, *Startup Investing and Venture DAOs*, U. Chi. Bus. L. Rev. Online 1 (2023), https://businesslawreview.uchicago.edu/online-archive/startup-investing-and-venture-daos.

2453 Ahmad Takatkah, *Are Investment DAOs the Future of Venture Capital?*, KingsCrowd (Mar. 21, 2023), https://kingscrowd.com/are-investment-daos-future-venture-capital/.

2454 Bryan Wilson, *The Complete Guide to Investment DAOs*, Upside OS: The Ledger (Jan. 22, 2024), https://www.upside.gg/the-ledger/the-complete-guide-to-investment-daos.

One of the more celebrated implementations of the investment DAO is the limited liability autonomous organization (the "LAO"). The LAO is a venture capital fund structured as a formal legal entity. It is a member-directed LLC and carries out its functions using smart contracts. In other words, it is a venture fund inspired by DAOs but fully grounded in law, in operating agreements, and in the realities of the off-chain world. It uses a formal legal entity designed to limit liability.[2455] And the LAO leverages on-chain voting and the delegation of votes to third parties to decide funding investments, to use smart contracts to collect members' initial contributions, and to distribute proceeds.[2456]

3. Grant DAOs

Grant DAOs are designed to fund and foster new projects, typically within a particular blockchain ecosystem. Rather than seeking direct financial returns, grant DAOs aim to support public goods, ecosystem growth, or shared infrastructure. Grant recipients apply for funding and are selected through community voting or by committees or managers appointed by the DAO. Examples include the Uniswap Grants DAO and the Aave Grants DAO, both of which award grants to projects that contribute to their respective ecosystems.[2457] Standalone grant DAOs include Gitcoin, which funds open-source development, and MolochDAO, which supports Ethereum-based projects and community initiatives.

In each case, stakeholders decide which projects to fund. Gitcoin's governance incentivizes contributions by matching funds raised from individual donors with funds from the DAO treasury. MolochDAO is particularly notable for its governance model, which relies on "guilds" — subgroups of token holders with specific expertise in different domains.[2458] It also includes strong exit rights ("rage-quit," see Figure 32) that allow members to withdraw capital if they disagree with collective decisions.

4. Collector DAOs

Collector DAOs pool funds to purchase collectable items, such as NFTs, physical artwork, music, and even rare collector items.[2459] Collector DAOs tend to make collectibles available to the public domain in some way, "prying artistic creations from an exploitative, antiquated economic system and offering the promise of a fairer one."[2460]

ConstitutionDAO is one of the most widely known examples of collector DAOs. It formed expressly to raise capital to bid on a rare copy of the U.S. Constitution that was being auctioned by Sotheby's. The DAO raised roughly $47 million in ETH from more than 17,000 contributors in a matter of days but was ultimately outbid by hedge fund founder Ken Griffin. The loss is often attributed to the blockchain's transparency, which revealed the DAO's bidding ceiling to competing bidders,[2461] though the mechanism is less clear-cut than sometimes suggested: Sotheby's auctions are open-outcry rather than sealed-bid, and the winning bidder could in principle have continued bidding past any disclosed ceiling. Nevertheless, ConstitutionDAO showcased the potential utility of collector DAOs and single-purpose DAOs for projects or efforts of finite duration.

2455 The LAO, Organization, https://docs.thelao.io/organization.html (last visited Jan. 15, 2026).

2456 Fan, *supra* note 2452.

2457 Bud Hennekes, *The 8 Most Important Types of DAOs You Need to Know*, Alchemy (updated Feb. 15, 2024), https://www.alchemy.com/blog/types-of-daos (last visited Jan. 15, 2026).

2458 Jha, *supra* note 2450.

2459 Naudts, *supra* note 2449, at 11-12.

2460 Ben Sisario, *Meet the New Owners of the Wu-Tang Clan's One-of-a-Kind Album*, N.Y. Times (Oct. 20, 2021), https://www.nytimes.com/2021/10/20/arts/music/wu-tang-clan-once-upon-a-time-in-shaolin.html.

2461 Upside, "Constitution DAO," Upside (Oct. 11, 2023), https://www.upside.gg/the-ledger/constitution-dao; Ella Feldman, "A Group of Crypto Investors is Trying to Buy the Constitution–Again," Smithsonian Magazine (Dec. 9, 2022), https://www.smithsonianmag.com/smart-news/crypto-investors-buy-the-constitution-dao-180981264/.

A longer-term collector DAO with more indefinite longevity and objectives is PleasrDAO. Pleasr is a collective group which bought a Wu Tang Clan album and issued an NFT to memorialize the ownership on chain.[2462] PleasrDAO continues to acquire and sell culturally significant artifacts, including political and social mementos from such figures as U.S. whistleblower Edward Snowden. PleasrDAO styles its future as a blockchain-based art auction house.[2463]

5. Service DAOs

Service DAOs provide services to external clients. They often resemble cooperatives or decentralized labor collectives and are frequently organized as "guilds." Members typically apply for admission, demonstrate relevant skills, and are accepted through internal guild review processes, rather than by a formal vote of the entire membership.[2464] Projects are approved through internal governance processes, often by designated coordinators or relevant guild members, rather than by a vote of the full membership,[2465] while tasks (occasionally called "bounties") are claimed by individual contributors.[2466] For example, a DAO may post a bounty seeking a smart contract audit or website redesign for a fixed fee, and an individual contributor can claim the task and receive payment upon completion and approval. Contributors are paid through the DAO, and the DAO relies on community consensus for additional bureaucratic decisions, such as treasury expenditures (advertising, benefits, investments, etc.) or internal incentives.

RaidGuild[2467] is a frequently cited example of a service DAO providing development, design, and consulting services within the Web3 ecosystem.

The service DAO category has proven empirically fragile: many prominent examples from the 2021–2022 period have dissolved, contracted, or gone dormant, and the model has struggled to compete with traditional labor-market coordination for all but narrow Web3-native tasks.

6. Social DAOs (including Metaverse DAOs)

Social DAOs are organizations in which membership is primarily oriented toward social interaction, networking, or shared identity. Members typically gain access by acquiring DAO tokens, which function as membership credentials. FWB is a group of eclectic creators, artists, builders, and crypto influencers who convene digitally and in real life without any particular objective or goal other than fostering community and creativity. This club is also demarcated by token ownership which grants access to online spaces and events in real life.[2468]

A subcategory of social DAOs consists of metaverse DAOs, which govern *virtual* worlds or digital environments. For example, the Decentraland DAO manages and controls the smart contracts and assets of the collective metaverse, as well as a cache of its native token, MANA. Decentraland is a decentralized virtual world, currently hosted on the Ethereum blockchain, which allows users to develop their own virtual three-dimensional spaces, as NFTs. Users can

2462 Sisario, *supra* note 2460.

2463 Cam Thompson, *The Revolutionaries Will Be Televised': PleasrDAO Launching Live Auctions With Snowden, Ellsberg NFT*, CoinDesk (Jan. 10, 2023), https://www.coindesk.com/web3/2023/01/10/the-revolutionaries-will-be-televised-pleasrdao-launching-live-auctions-with-snowden-ellsberg-nft/.

2464 RaidGuild, *Join the Guild*, https://handbook.raidguild.org/docs/membership/join-the-guild (last visited Jan. 15, 2026).

2465 RaidGuild, *DAO Operations*, https://handbook.raidguild.org/docs/dao-operations/ (last visited Jan. 15, 2026).

2466 Paragraph, *How To Develop a Bounty Program* (Aug. 29, 2022), https://paragraph.com/@daomstr/s95yWrpoyskppacUQ5xd.

2467 RaidGuild, https://www.raidguild.org (last visited Jan. 15, 2026).

2468 Erin Woo & Kevin Roose, "Friends With Benefits Social Club Runs On Crypto and Vibes," N.Y. Times (Mar. 2, 2022), https://www.nytimes.com/2022/03/02/technology/friends-with-benefits-crypto-dao.html.

then charge other users for activities or services on their virtual land.[2469] Another prominent example is the ApeCoin DAO[2470], created in connection with the Bored Ape Yacht Club (BAYC), an NFT ecosystem. The DAO is supported by the Ape Foundation, which acts as its "legal steward" and implements DAO decisions.

Like service DAOs, the social DAO category reached its peak in 2021–2022 and has contracted substantially since.

7. Emerging and Hybrid DAO Forms

Beyond the categories above, newer DAO forms have gained prominence. Decentralized science (DeSci) DAOs[2471] focus on funding and coordinating scientific research, data sharing, and intellectual property management. Decentralized physical infrastructure (DePIN) DAOs[2472] coordinate the deployment and governance of real-world infrastructure, such as compute resources, storage, telecommunications, or energy networks. Impact or public-goods DAOs[2473] pursue environmental, social, or civic objectives. Finally, "network state"[2474] or city-oriented DAOs[2475] propose new forms of digitally coordinated communities, though many such initiatives remain aspirational rather than operational.

APPENDIX 6 - ZERO-KNOWLEDGE PROOF AND THE ALI BABA CAVE

by Reuben Youngblom

The goal in using "zero-knowledge proofs" (ZKPs) is not to "prove" knowledge with full mathematical certainty but to prove it with enough certainty that someone who must confirm something (the verifier) is convinced. Jean-Jacques Quisquater et al. illustrated this idea using the well-known "Ali Baba Cave" analogy.[2476] In this analogy, Peggy (the *prover*) wants to convince Victor (the *verifier*) that she knows a secret phrase that opens a magic door inside a cave, without revealing the phrase itself. The cave is somewhat of a horseshoe shape, with a "magic door" that can be opened only through use of the secret phrase. The cave can be entered through two paths, A and B. Without the secret phrase, a person who enters via path A must exit via path A, and likewise for path B.

To prove she knows the secret phrase, Peggy enters the cave by choosing either path A or path B, without Victor seeing which one she takes. Victor then randomly picks a path, either A or B, that he wants Peggy to use to return. If Peggy knows the secret phrase, she can always comply with Victor's request. If she does not know the phrase,

2469 Decentraland, "Terms of Use," https://decentraland.org/terms/ (last visited Jan. 15, 2026) (Clause 1 straightforwardly states that "[t]he Decentraland Foundation (the 'Foundation'), acting for the benefit of the Decentraland community as a whole, holds the intellectual property rights over, and makes available, (a) the DCL Client, the Desktop Client, the SDK 5.0, the Marketplace (https://market.decentraland.org), the Builder, the Blog, Events, Agora, Forum, the Land Manager, the Command Line Interface, DAO, the Developers' Hub, the Rewards tool which, with any other features, tools and/or materials made available from time to time by the Foundation, are referred to herein as the 'Tools' and (b) the website https://decentraland.org (the 'Site')"); Blockchain Social, "Decentraland Metaverse," MEDIUM (Aug. 13, 2023), https://medium.com/@blockchainsocial.eth/understanding-the-decentraland-dao-2fdcde52516c.

2470 ApeCoin DAO, *Welcome to the ApeCoin DAO Discourse* (Feb. 22, 2022) https://forum.apecoin.com/t/welcome-to-the-apecoin-dao-discourse/7.

2471 Lukas Weidener & Cord Spreckelsen, *Decentralized Science (DeSci): Definition, Shared Values, and Guiding Principles*, 7 Front. Blockchain, art. 1375763 (2024), https://www.frontiersin.org/articles/10.3389/fbloc.2024.1375763/full.

2472 COINTELEGRAPH, *Decentralized Physical Infrastructure Network (DePIN)*, Explained (Sept. 30, 2024), https://cointelegraph.com/explained/decentralized-physical-infrastructure-network-depin-explained.

2473 GENERAL MAGIC, *Decoding Impact DAOs (Part 2): Blockchain for Public Goods* (Jan. 27, 2023), https://blog.generalmagic.io/decoding-impact-daos-part-2-blockchain-for-public-goods

2474 Balaji S. Srinivasan, *The Network State: How To Start a New Country* 23–27 (2022), https://thenetworkstate.com

2475 Rebecca Davis, *Goodbye, the Beloved Country — Hello, the Network State*, DAILY MAVERICK (Sept. 26, 2022), https://www.dailymaverick.co.za/article/2022-09-26-goodbye-the-beloved-country-hello-the-network-state.

2476 Jean-Jacques Quisquater et al., *How to Explain Zero-Knowledge Protocols to Your Children*, in ADVANCES IN CRYPTOLOGY—CRYPTO '89 PROCEEDINGS (Gilles Brassard ed., 1990), https://pages.cs.wisc.edu/~mkowalcz/628.pdf.

she will be forced to exit via the same path she originally entered. If Peggy exits via the path Victor requested, this does not yet prove that she knows the secret phrase. It could simply be that Victor happened to choose the same path Peggy had entered. For this reason, the process must be repeated multiple times. With each repetition, the likelihood that Peggy succeeds by chance alone decreases. So, Peggy and Victor must repeat this cycle several times[2477] to increase Victor's confidence that Peggy knows the secret phrase.[2478]

A key feature of this process is that Victor learns nothing about the secret phrase itself. No matter how many times the experiment is repeated, Peggy never reveals the phrase, and Victor gains no information that would allow him to reconstruct it. Peggy can never prove with absolute certainty that she knows the secret phrase. Even if she does not know it, there is a 50 percent chance that she succeeds in a single round. Two successful rounds reduce that probability to 25 percent, and each additional round further reduces the odds. While the probability of success by chance can be made extremely small, it can never be reduced to zero. Even with millions of trials, there will still be a very outside chance that Peggy got lucky millions of times in a row.

APPENDIX 7 - EXAMPLES OF BLOCKCHAIN-BASED DATA-SHARING

by Juan Du

The wide adoption of blockchain-based data sharing has been slow for multiple reasons, such as the technical complexity of the infrastructure, the difficulty for non-technical users and regulators to understand the technology, and significant integration challenges with existing legacy systems in organizations.[2479] While there has been a considerable amount of research testing blockchain-based data-sharing protocols,[2480] real-world adoption lags behind. This is due to industry specific problems, such as the "last-mile" issue in data capturing[2481] and the lack of standardized, interoperable data formats. Despite the uneven adoption of blockchain across sectors, there have been successful use cases in domains under regulatory or operational pressure to digitalize data-sharing processes, such as the healthcare and insurance sectors.

1. Decentralized data directory of healthcare providers

To bridge data silos, improve data quality, and enhance efficiency in data-sharing between individual organizations, leading American healthcare companies launched the Synaptic Health Alliance in 2018 and developed a blockchain-based Decentralized Provider

2477 Siqi Liu, *Privacy Protection Revolution: Zero-Knowledge Proof*, in *Proceedings of the 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI)* 395 (Zakopane, Poland, Aug. 15-16, 2022), https://ieeexplore.ieee.org/iel7/9973806/9973442/09973872.pdf.

2478 Vitali Bestolkau & Ignas Apšega, *Zero Knowledge Proof – How It Works and the Alibaba Cave Experiment,* Byont (Sept. 11, 2022), https://www.byont.io/blog/zero-knowledge-proof-how-it-works-and-the-alibaba-cave-experiment.

2479 Mutiullah Shaikh et al., *A Systematic Literature Review for Blockchain-Based Healthcare Implementations,* 13(9) Healthcare, 1087 (2025) https://doi.org/10.3390/healthcare13091087.

2480 *See* Thanh Linh Nguyen et al., *Blockchain-Empowered Trustworthy Data Sharing: Fundamentals, Applications, and Challenges* (Mar. 12, 2023) (unpublished manuscript) 1, ArXiv, https://arxiv.org/abs/2303.06546.

2481 Juan Du, Bo Bernhard Nielsen & Catherine Welch, *From Buzzword to Biz World: Realizing Blockchain's Potential in the International Business Context*, 66(1) Cal. Mgmt. Rev. 124, 135, 140 (2023), https://doi.org/10.1177/00081256231202266

Data Directory,[2482] built on Kaleido's enterprise platform using a Quorum (Ethereum-derived) stack. The Data Directory serves as a trusted source of demographic data shared across participating healthcare organizations, enabling members to maintain up-to-date provider directories with information such as physicians' names, addresses, specialities, and phone numbers as required by state and federal regulations in the U.S.[2483]

Because providers often work with multiple insurers maintaining separate IT systems and unique insurance plans, this synchronization eliminates the need for multiple insurers to verify the same information.[2484] It helps streamline administrative processes and reduce costs for data sharing between healthcare providers and payers.[2485] Moreover, the Synaptic Health Alliance experimented with token-based incentive mechanisms to encourage data maintenance and updates by participating organizations.[2486] Data quality can be improved with updates and corrections constantly made by different parties.[2487] By reducing data errors and work redundancy when connecting patients with healthcare providers, the Directory enhances the reliability of provider information and indirectly supports more efficient access to care, while reducing data-management costs at an industry level. [2488]

Yet governance remains centralized within the consortium. Participation is permissioned, and regulatory compliance —particularly under U.S. healthcare privacy laws— continues to shape system design. The blockchain enhances coordination but does not replace institutional accountability.

2. Insurance claim settlement

Blockchain is also increasingly used in digitalizing insurance claim settlement processes.[2489] MediConCen,[2490] a Hong Kong-based company, built a blockchain-based medical platform in 2018 to automate the insurance claim workflow for insured clients, doctors, and insurers.[2491] The platform replaces physical cards, receipts, and claims with unique QR codes and digital signatures for patients. It automates insurance claim settlement with smart contracts, once specific policy terms are met, hence reducing administrative work and human errors.[2492] Users cryptographically sign transactions on the blockchain, and companies verify identities in a secure environment, to reduce fraudulent behaviors.[2493]

Multiple stakeholders choose blockchain as a solution for data sharing among and data management across

2482 Synaptic Health Alliance, *Proving Blockchain's Value in Healthcare* (last visited Jan. 15, 2026) https://4801399.fs1.hubspotusercontent-na1.net/hubfs/4801399/Kaleido%20and%20Synaptic%20Health%20Alliance%20Cobranded%20Case%20Study_digital.pdf; *See also* Benjamin Ross, *Healthcare Organizations Form Synaptic Health Alliance to Explore Blockchain's Impact on Data Quality*, Clinical Rsch. News Online (Dec. 5, 2018), https://www.clinicalresearchnewsonline.com/news/2018/12/05/healthcare-organizations-form-synaptic-health-alliance-explore-blockchain-s-impact-on-data-quality.

2483 Synaptic Health Alliance, *Why we came together* (last visited Jan. 15, 2026), https://www.synaptichealthalliance.com/about-us

2484 Synaptic Health Alliance, *supra* note 2482.

2485 Synaptic Health Alliance, *It's a True Alliance*, https://www.synaptichealthalliance.com/project (last visited Jan. 15, 2026).

2486 Synaptic Health Alliance, *supra* note 2482.

2487 Synaptic Health Alliance, *Improving Provider Data Accuracy, A Collaborative Approach Using a Permissioned Blockchain,* https://4801399.fs1.hubspotusercontent-na1.net/hubfs/4801399/Synaptic_Health_Alliance_Blockchain_White_Paper_2022.pdf (last visited Jan. 15, 2026).

2488 *Id.*

2489 Leigh Jones, *Is Blockchain the Next Big Thing for Insurance Companies?*, Reuters (Oct. 9, 2024), https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/; Nabilah Huda, *InsurTech: Automating Insurance Claims via Blockchain*, The Edge Malaysia (Aug. 12, 2019), https://theedgemalaysia.com/article/insurtech-automating-insurance-claims-blockchain.

2490 MediConCen - Automating insurance claims, https://mediconcen.com.hk (last visited Jan. 15, 2026)

2491 *MediConCen Uses Blockchain to Automate Insurance Claims*, H.K. Sci. & Tech. Parks Corp. (Nov. 22, 2018), https://www.hkstp.org/press-room/mediconcen-uses-blockchain-to-automate-insurance-claims.

2492 *Id.*

2493 Catherine Wang, *Hong Kong Startup Raises $6.85 Million Series A for Blockchain-Powered Insurance Claims*, Forbes (Feb. 9, 2024), https://www.forbes.com/sites/catherinewang/2024/02/09/hong-kong-startup-raises-685-million-series-a-for-blockchain-powered-insurance-claims/

multiple jurisdictions. Allianz,[2494] an insurance company headquartered in Munich, Germany, has deployed a blockchain-based platform to automate cross-border motor insurance claim settlements across its 24 European subsidiaries since 2021.[2495] The platform reduces back-and-forth email exchanges for cross-border motor insurance settlements involving multiple jurisdictions and languages. It provides synchronized information on insurance claims for different parties, and its built-in smart contract automates the claim settlement process for tasks, such as claim validation, reconciliation, settlement, and cost splitting.[2496]

In both cases, blockchain addresses the reconciliation problem among multiple entities operating under different jurisdictions or administrative systems. However, these systems remain institutionally governed and operate within conventional legal frameworks. Blockchain reduces friction but does not decentralize ultimate authority.

3. Intellectual property management

Apart from being used as an "insurTech" for data sharing in the insurance industry, blockchain is also being deployed as a "lawTech" tool to automate legal work, such as intellectual property (IP) management. It has been adopted in various stages of an IP asset, including registration, authentication, and protections.[2497] For instance, the European Union Intellectual Property Office (EUIPO) launched a blockchain-based IP Register in 2021 to share IP rights information with IP institutions and their clients in real time.[2498] While providing reliable records of IP information, the Register also provides an immutable track record of changes in IP statuses and allows users to download time-stamped and authenticated certificates of IP rights.[2499] IP offices from seven European countries had joined the blockchain network by 2024.[2500]

When integrated with artificial intelligence and cloud-computing technologies, blockchain also helps improve efficiency for the certification and verification of the originality of digital work, such as articles, music scores, videos, and pictures. For instance, Ant Group, a Chinese tech company, launched the Quezao Digital Copyrights Service Platform in 2020 to provide a one-stop service of IP management and licensing for individual and institutional content creators. Once users upload their digital work onto the blockchain, the Platform encrypts the data, converts it through an algorithm into a hash value, and records it on the blockchain.[2501] The blockchain assigns a unique Digital Copyright Identifier and facilitates IP protection through automated, data-driven detection of potential infringements.[2502] The blockchain record serves as probative evidence of prior creation and fixation, which users can present in court proceedings for IP disputes, although it does not on its own establish legal ownership.[2503] The evidentiary weight of the record differs significantly across jurisdictions.

2494 Allianz, https://www.allianztravelinsurance.com; (last visited Jan. 15, 2026).

2495 Allianz Technology, *Our Services*, https://tech.allianz.com/india/services.html (last visited Jan. 15, 2026).

2496 Du, Nielsen, & Welch, *supra* note 2481, at 131.

2497 Eleonora Rosati, *From Web 2 to Web 3: Harnessing blockchain technology for IP*, EUIPO https://www.euipo.europa.eu/en/news/from-web-2-to-web-3-harnessing-blockchain-technology-for-ip (last visited Jan. 15, 2026).

2498 Eur. Union Intell. Prop. Off., *EUIPO connects to TMview and DesignView through blockchain – news, EUIPO,* https://www.tmdn.org/network/-/euipo-connects-to-tmview-and-designview-through-blockchain (last visited Jan. 15, 2026).

2499 Rosati, *supra* note 2497.

2500 Eur. Union Intell. Prop. Off., *EUIPO named world's most innovative IP office for fifth time*, EUIPO, https://www.euipo.europa.eu/en/news/euipo-named-world-s-most-innovative-ip-office-for-fifth-time (last visited Jan. 15, 2026).

2501 Quezao, *Privacy Policy* https://render.alipay.com/p/c/180021120000000228/index.html?agreementId=AG01000475 (last visited Jan. 15, 2026).

2502 Quezao, *The Mechanisms and Benefits of Quezao Evidence Deposit*, https://www.mydcs.com/pages/index (last visited Jan. 15, 2026).

2503 Quezao, *Quezao Digital Copyrights Service Platform*, https://www.mydcs.com/pages/website/protect/index (last visited Jan. 15, 2026).

Here, blockchain primarily enhances evidentiary integrity and auditability. It does not itself determine ownership or resolve disputes but may strengthen the probative value of time-stamped records in judicial proceedings.

APPENDIX 8 - PROVENANCE AND TRACEABILITY IN AUTOMOBILE INDUSTRY; THE VINTURAS CASE

by Juan Du

Blockchain-based provenance and traceability initiatives in the automobile sector span several distinct layers, including industry standard-setting efforts such as the Mobility Open Blockchain Initiative (MOBI),[2504] regulatory-driven applications such as battery passports under the EU Battery Regulation (2023/1542),[2505] and responsible-sourcing platforms for cobalt, lithium, and other critical minerals. This appendix focuses on one representative layer: the use of consortium blockchain to support finished-vehicle logistics and cross-border delivery, illustrated through the Vinturas network.

To cope with changing tariffs and red tape in a rapidly shifting global trade landscape, original equipment manufacturers (OEMs) and logistics service providers (LSPs) in the automobile industry need to share real-time data for cross-border delivery of vehicles and mitigate supply chain risks. Despite the benefits of aggregate insights at an industry level, it has been difficult for OEMs and LSPs to share data due to the concern of losing control of data to third-party platforms and becoming uberized by centralized platforms. Third party platforms may monetize such data, create new business models, and threaten the competitive advantages of OEMs and LSPs.

To keep the independence of OEMs and LSPs and enable them to share data without losing data ownership, Vinturas, a Dutch software company established in 2019, built an interoperable network solution, enabled by blockchain technology that serves as a decentralized supply chain audit book for OEMs and LSPs. The blockchain provides provenance of vehicles by enabling trading partners, such as manufacturers, logistics service providers, lease companies, car rentals, fleet owners, and car dealers, to share data on milestones and documentation without losing control over their data.[2506] It serves as a single source of truth where any change to the data can be updated in real-time to a network of defined groups of supply chain participants.[2507]

The real-time data sharing between relevant parties realizes end-to-end traceability for vehicle delivery from manufacturers to customers. The availability of immutable and accurate data drives timely decision making and increases network resilience throughout the supply chain. The decentralized blockchain network prevents a single point of failure that can stall the function of the entire supply chain in the case of cyberattacks. Users can install nodes in their data center in their own country to ensure data sovereignty and compliance for cross-border data exchange.[2508]

The Vinturas model illustrates a broader pattern across consortium blockchains in the automotive sector:

2504 See https://dlt.mobi/.

2505 Vasileios Rizos and Patricia Urban, *Implementing the EU Digital Battery Passport* , CEPS (March 2024) https://circulareconomy.europa.eu/platform/sites/default/files/2024-03/1qp5rxiZ-CEPS-InDepthAnalysis-2024-05_Implementing-the-EU-digital-battery-passport.pdf (noting implementation of blockchain-secured digital IDs in EU-funded battery passport projects).

2506 *Mitsubishi Motors Europe Partners With Vinturas to Deliver Interoperability to their Supply Chain*, ANICE, https://www.anicecommunication.com/en/mitsubishi-motors-europe-partners-with-vinturas-to-deliver-interoperability-to-their-supply-chain/ (last visited Jan. 15, 2026)

2507 *How it works*, VINTURAS, https://vinturas.com/how-it-works/ (last visited Jan. 15, 2026)

2508 Du, Nielsen, & Welch, *supra* note 2481.

participants adopt distributed ledger technology not primarily to decentralize authority, but to resist platform intermediation and retain data ownership while still enabling industry-wide coordination. The architecture substitutes a governed consortium network for both the fragmented bilateral exchanges of the pre-digital era and the centralized third-party platforms that threaten to capture the value of shared data.

APPENDIX 9 - AUTOMATION AND TRADE FINANCE IN GLOBAL SHIPPING INDUSTRY

by Juan Du

The global shipping industry faces growing challenges from increasingly complex supply chains, including challenges driven by geopolitical tensions and other external shocks. In response, major industry actors have accelerated digital transformation, including the digitization of bills of lading (BLs).

A bill of lading is a legal document issued by a shipping line to a shipper which serves as a receipt for goods, a contract for carriage, and a document of title to the goods. Technological developments and the evolution of laws and regulations —notably the UNCITRAL Model Law on Electronic Transferable Records (MLETR, 2017), which establishes the international framework for the legal recognition of electronic transferable documents, and its national implementations such as the UK Electronic Trade Documents Act 2023— have accelerated the adoption of electronic bills of lading (eBLs) among shippers.[2509] Traditional manual processes in the issuance, circulation, endorsement, amendment, and replacement of BLs are streamlined using blockchain-based eBLs. [2510] The end-to-end digital process reduces errors, improves user experience, and increases the efficiency[2511] of various workflows.[2512]

In June 2025, an eBL solution supporting all major international standards for bills of lading was launched on the Global Shipping Business Network's (GSBN) blockchain-based platform. [2513] The GSBN is an independent and not-for-profit technology consortium incorporated in 2021 in Hong Kong by eight leading shipping industry companies. To date, GSBN's platform has processed over 650,000 eBLs covering more than 100 countries. GSBN serves as a blockchain-based data utility platform, harmonizing structured datasets across key trade documents for data sharing with proper consent under different trade scenarios. It streamlines the data exchange process among disparate and competing global supply chain participants, such as shipping lines and terminals, as well as banks and insurance companies.[2514] For interoperability, GSBN's blockchain-based platform addresses the legal and liability challenges of eBLs being transferred between different eBL solutions. It does this by guaranteeing the security and immutability of eBLs

2509 GSBN, *GSBN Partners with ZAN to Harness Web3 to Tokenise eBLs and Unlock New Economic Opportunities* (Nov 6, 2023), https://gsbn.trade/gsbn-partners-with-zan-to-harness-web3-to-tokenise-ebls-and-unlock-new-economic-opportunities/; *UK Electronic Trade Documents Act 2023: A Further Step Towards Paperless Trade,* CLIFFORD CHANCE (Aug 01, 2023),https://www.cliffordchance.com/briefings/2023/08/uk-electronic-trade-documents-act-2023--a-further-step-towards-p.html.

2510 GSBN, *Major Milestone Achieved with First Bulk Electronic Bill of Lading Issued Over GSBN* (Jan. 17, 2023), https://gsbn.trade/major-milestone-achieved-with-first-bulk-electronic-bill-of-lading-issued-over-gsbn/

2511 GSBN, *WiseTech Global and IQAX enhances De Well Group's freight forwarding efficiency through eBL integration with CargoWise over GSBN* (Feb 27, 2025), https://gsbn.trade/wisetech-global-and-iqax-enhances-de-well-groups-freight-forwarding-efficiency-through-ebl-integration-with-cargowise-over-gsbn/

2512 GSBN, *First PoC Linking Up Paperless Cargo Release and eBL Solutions on GSBN* (May 11, 2023), https://www.gsbn.trade/post/first-poc-linking-up-paperless-cargo-release-and-ebl-solutions-on-gsbn

2513 GSBN, *IQAX Becomes First eBL Solution Globally to Go Live with DCSA eBL API v3.0 on GSBN* (June 16, 2025), https://www.gsbn.trade/post/iqax-becomes-first-ebl-solution-globally-to-go-live-with-dcsa-ebl-api-v3-0-on-gsbn

2514 GSBN, *Industry First as GSBN Completes PoC Using Confidential Computing to Transform Global Trade Finance* (Apr 13, 2023), https://www.gsbn.trade/post/industry-first-as-gsbn-completes-poc-using-confidential-computing-to-transform-global-trade-finance

transferred across platforms, serving as a control tracking registry and maintaining a complete audit trail of the transfer status of eBLs. This guarantees that, at any given time, there is only one recognized controlling solution. Enabling eBL to be interoperable removes a major barrier in the adoption of eBLs across different platforms for shippers and financial institutions. [2515]

With the increasing adoption and acceptance of eBLs as having the same rights and obligations as paper BLs, GSBN has been exploring new ways to help bridge the USD 2.5 trillion global trade finance gap estimated by the Asian Development Bank.[2516] One such way is tokenization of eBLs to create new securitization opportunities for digital trade finance.[2517] GSBN has been working with the Hong Kong Monetary Authority (HKMA) to experiment with tokenization of eBLs for supply chain finance. [2518] However, it is still early to move trade finance projects from pilots to production due to lack of regulatory framework about tokenization and acceptance by the market. Encouragingly, the recent legislation on stablecoin adopted in Hong Kong, the U.S., and the Middle East may bring more regulatory clarity for stablecoin issuers and unlock the use case of combining eBLs and stablecoins for digital trade finance in global supply chain.[2519]

APPENDIX 10 - VERIFICATION AND COMPLIANCE IN SUPPLY CHAIN SUSTAINABILITY

by Juan Du

Global supply chain participants are facing increasing requirements to comply with regulations for sustainability, such as reporting on their sustainability impacts through their value chains[2520] and improving sustainable practices to minimize environmental risks.[2521] To meet compliance needs, suppliers must share information on the materials used in products, where they originated, and how they were reused to minimize environmental impact. However, it is hard for regulators to verify the integrity of the data and access data trails connecting multi-tiered supply chain participants.[2522] Suppliers are also reluctant to share data on compositions of materials which are mostly sensitive proprietary information.

To trace the environmental footprint of suppliers in global supply chains, Circularise, a software company founded in 2016 in the Netherlands, built blockchain-based mass balance bookkeeping and digital product passport solutions to enable suppliers to provide verifiable data to meet compliance requirements. Mass balance accounting is a method used to track, verify, and certify the proportion of virgin and recycled inputs in a shared production system, especially for products whose output

2515 GSBN, *Cross-Platform eBLs Become a Reality as OOCL and a Major Oil and Gas Company Go Live* (Mar 19, 2025), https://www.gsbn.trade/post/cross-platform-ebls-become-a-reality-as-oocl-and-a-major-oil-and-gas-company-go-live

2516 Asian Dev. Bank, *Global Trade Finance Gap Expands to $2.5 Trillion in 2022* (Sept. 2023), https://www.adb.org/news/global-trade-finance-gap-expands-25-trillion-2022.

2517 GSBN, *GSBN partners with ZAN to harness Web3 to tokenise eBLs and unlock new economic opportunities* (Nov 6, 2023), https://www.gsbn.trade/post/gsbn-partners-with-zan-to-harness-web3-to-tokenise-ebls-and-unlock-new-economic-opportunities

2518 GSBN, *GSBN joins HKMA's Project Ensemble to accelerate electronic Bill of Lading tokenisation and bridge multi-trillion-dollar trade finance gap* (Aug 28, 2024), https://gsbn.trade/gsbn-joins-hkmas-project-ensemble-to-accelerate-electronic-bill-of-lading-tokenisation-and-bridge-multi-trillion-dollar-trade-finance-gap/

2519 Interview with Betrand Chen, CEO of GSBN (Aug 26, 2025).

2520 *Directive 2022/2464, of the European Parliament and of the Council of 14 December 2022*, 2022 O.J. (L 322) 15 EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464 (last visited Jan. 15, 2026)

2521 European Commission, *Ecodesign for Sustainable Products Regulation*, https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/ecodesign-sustainable-products-regulation_en (last visited Jan. 15, 2026)

2522 Ziva Buzeti & Tian Daphne, *Packaging and Packaging Waste Regulation (PPWR): A Guide to Compliance, Timelines, and Mass Balance Solutions* (Aug 27, 2025) CIRCULARISE https://www.circularise.com/blogs/ppwr-guide-to-compliance-timelines-and-mass-balance-solutions (last visited Jan. 15, 2026)

is chemically different from their input.[2523] The method is essential for chemical recycling for products like plastic: Chemical recycling is particularly difficult because chemicals are mixed within products manufactured across complex value chains, making their separation and recovery complex. Circularise offers a critical method for scaling up the use of recycled materials and enabling the verifiability of product sustainability characteristics by certification schemes such as the International Sustainability and Carbon Certification (ISCC). Circularise's mass balance bookkeeping software utilizes blockchain and zero-knowledge proof technology (its patented "Smart Questioning" feature) to allow suppliers to cryptographically prove compliance (e.g., the percentage of recycled content) without exposing the underlying sensitive data, thus retaining full control. The blockchain-based solution provides tamper-proof and verifiable data to help prevent double counting of recycled content across participants in a production system. Blockchain ensures the accuracy and integrity of data on product material which can be verified and audited for the ISCC.

Circularise's blockchain-based digital product passport provides a secure platform to connect fragmented supply chain stakeholders, including suppliers, manufacturers, importers, distributors, and retailers,[2524] to share data during a product's life cycle to meet regulatory requirements, such as the EU Ecodesign for Sustainable Products Regulation (ESPR), adopted in 2024. According to the company, its blockchain-based platform streamlines the process for ESPR compliance, reducing administrative efforts by up to 80%, and accelerates access to the EU market. The platform is designed to align with often overlapping regulatory frameworks, enabling simultaneous compliance with multiple standards. It also helps coordinate stakeholder workflows and timelines to ensure consistent compliance and mitigate associated risks. It details the composition, location, and environmental impact of products, ranging from garments to automobiles, and stores the data on blockchain. Its immutable and time-stamped data can be trusted and accessed by regulators and consumers. The detailed product life information helps manufacturers meet compliance needs but also enables them to reuse materials, recycle products, reduce environmental impact, and improve supply chain sustainability. Circularise participates in EU-funded expert consortia such as CIRPASS-2, contributing to the development of digital product passport frameworks and ensuring the interoperability between digital product passport solutions and other EU digital systems, such as customs databases, to scale up the solution across complex global supply chains.[2525]

APPENDIX 11 - THE BITCOIN KNOTS MOVEMENT

The "Bitcoin Knots" movement has recently emerged as an effort to reassert node-level autonomy within the Bitcoin ecosystem.[2526] Originally developed by Luke Dashjr in 2011 as a variant of Bitcoin Core aggregating experimental patches and additional configuration options, Bitcoin Knots has since evolved into a client that offers operators greater flexibility. Among its distinctive features are more granular mempool and relay policy settings, extended configuration options for transaction

2523 *Id.*

2524 Mesbah Sabur, Ziva Buzeti & Tian Daphne,*Specific ESPR Requirements for Manufacturers, Importers, Distributors, and Retailers (Part 5)*, (Apr. 9, 2025) CIRCULARISE, https://www.circularise.com/blogs/get-ready-for-espr-5 (last visited Jan. 15, 2026).

2525 *Circularise advises on digital product passports at EU Parliament IMCO public hearing*, CIRCULARISE, https://www.youtube.com/watch?v=e0Bakd05yqE (last visited Jan. 15, 2026)

2526 OneSafe Editorial Team, *Bitcoin Knots: What it Means for Crypto Payments and Governance*, ONESAFE (June 21, 2025), https://www.onesafe.io/blog/bitcoin-knots-future-governance-market-stability

selection and block validation, and experimental functionalities that are either unavailable or disabled by default in Bitcoin Core. These enhancements allow node operators to fine tune their participation in the network. For example, they can filter spam-like transactions, adopt alternative fee policies, or enable broader support for non-standard transactions. A critical point about Bitcoin Knots is that it is a modification of Bitcoin Network's *policy* rules (which determine which transactions nodes will relay and store in their mempools) rather than *consensus* rules (which determine which transactions are valid and can be included in blocks). That means implementations of both Bitcoin Core and Bitcoin Knots ultimately accept the same blocks and remain on the same blockchain.[2527]

Bitcoin Knots adoption grew rapidly throughout 2025, rising from roughly 2% of publicly reachable nodes in early 2025 to approximately 17–25% by September 2025, and remaining above 20% into early 2026.[2528] This surge reflects both technical preferences and ideological resistance to Bitcoin Core's October 2025 v30.0 update, which increased the OP_RETURN data limit, made it configurable, and allowed multiple data outputs per transaction. Knots supporters view this relaxation as enabling blockchain spam,[2529] and some critics have warned that node operators, particularly those running archival nodes, could face legal exposure if arbitrary embedded data includes illegal content. In this sense, Bitcoin Knots represents not merely an alternative implementation but also —according to its proponents— an assertion of decentralization and counter-governance, emphasizing that node sovereignty, policy diversity, and accountability remain central to Bitcoin's integrity.

APPENDIX 12 - QUADRATIC VOTING

by Reuben Youngblom

Originally developed in the economics literature as a response to the limitations of one-person-one-vote systems, Quadratic Voting (QV) has attracted growing interest from blockchain communities seeking alternatives to plutocratic, token-weighted governance. This appendix first outlines the logic and limits of quadratic voting as applied to decentralized systems, then examines its adaptation to the funding of public goods through the case of Gitcoin Grants.

1. The distribution of voting power

In blockchain, quadratic voting distributes voting power based on the square root of the number of tokens (or voice credits) held, so that casting n votes on a single issue costs n^2 tokens. This reduces the concentration of influence by users who hold a large number of tokens, and it helps to mitigate the risk of plutocratic control. Some Aragon-based DAOs have experimented with applying quadratic voting to particular governance decisions, typically combining it with Sybil-resistance tools such as Gitcoin Passport, proof-of-personhood systems (e.g. Worldcoin), or social attestations. Beyond the blockchain context, the Democratic Caucus of the Colorado State Legislature —working in collaboration with the RadicalxChange Foundation and the Democracy Earth Foundation— has conducted one of the most prominent real-world pilots of quadratic voting, beginning in 2019 and repeated in subsequent legislative sessions to prioritize appropriations bills.

2527 Michael Tabone, Bitcoin Knots gain ground: Will a chain split kill BTC price?" Coin Telegraph (June 21, 2025) https://cointelegraph.com/news/bitcoin-knots-chain-split-kill-btc-price;

2528 See, e.g., Bitcoin Knots node share estimates reported in 2025–2026 network statistics (showing growth from ~2% to 17–25% in September 2025 and ~22% in early 2026): Bitref, *Bitcoin Nodes Distribution*, https://bitref.com/nodes/ (last visited Jan. 15, 2026); Jamie Redman, *Knots Revolt: Nearly 4,000 Nodes Aim to Defy Bitcoin Core's New Rules*, Bitcoin.com News (August 19, 2025), https://news.bitcoin.com/knots-revolt-nearly-4000-nodes-aim-to-defy-bitcoin-cores-new-rules/.

2529 Tabone, *supra* note 2527.

However, implementing quadratic voting fully within blockchain systems presents significant practical challenges. A central concern is the possibility that a single user could create multiple identities (dubbed a "Sybil attack") to defeat the system, since the quadratic cost structure only disincentivizes vote concentration when each voter is a distinct individual. Addressing Sybil attacks remains a critical and unresolved issue in the design of blockchain-based quadratic voting systems, and it continues to be a focus of ongoing research in the field. In practice, quadratic voting requires some form of robust identity layer —whether decentralized identifiers (DIDs), proof-of-personhood protocols, social-graph attestations, or off-chain verification— to approximate a one-person-one-identity assumption.

Quadratic voting has also been adapted to the funding of public goods. In a foundational article,[2530] Vitalik Buterin, Zoë Hitzig, and E. Glen Weyl proposed a mechanism for philanthropic or publicly funded seeding designed to support the (near) optimal provision of public goods within a decentralized, self-organizing ecosystem. This model —referred to as quadratic funding (QF)— builds upon the principles of quadratic voting and adapts them to a funding context aimed at fostering endogenous community formation around shared goals. Under this model, individuals contribute to public goods projects they value. The funding that a project receives is proportional to the square of the sum of the square roots of individual contributions.

This formula incentivizes broad-based support —rewarding projects backed by many small donors over those backed by a few large ones— and helps align funding outcomes with collective preferences. In the "standard model," this mechanism achieves a first-best outcome in the provision of public goods by correcting for the underfunding typical in voluntary contribution systems. The authors also explore variations of the model that address practical concerns, such as limiting total costs (a variant known as "capital-constrained liberal radicalism" or CLR, which was used in Gitcoin's early funding rounds), mitigating the risks of collusion, and enhancing coordination. They identify potential applications in areas such as political campaign financing, open-source software development, funding for journalism and media, and urban infrastructure projects.

2. The case of Gitcoin Grants

Built on the Ethereum blockchain, Gitcoin Grants facilitates community funding by combining individual contributions with a matching pool, distributed according to the principles of quadratic funding (QF). Gitcoin was founded in 2017 and launched its first QF-based Grants round in early 2019.

Projects seeking support create grant listings on the Gitcoin platform. Community members then contribute to the projects they find valuable. A central feature of the model is that the matching amount allocated to each project is proportional to the square of the sum of the square roots of individual contributions —a formula that rewards broad support (many small donors) rather than concentrated support (few large donors). As a result, projects with widespread support from many small donors can receive significantly more matching funds than those with only a few large contributors.

Gitcoin Grants operates in discrete funding "rounds," typically lasting several weeks, with each round often dedicated to a specific theme, such as infrastructure, education, climate solutions, or ecosystem-specific development. The matching pools for these rounds are funded by major stakeholders in the ecosystem, including the Ethereum Foundation, prominent protocols, and DAOs.

2530 Vitalik Buterin, Zoë Hitzig & E. Glen Weyl, *Liberal Radicalism: Formal Rules for a Society Neutral Among Communities*, 65 MGMT. SCI. 5171 (2019).

Since its inception, Gitcoin has progressively decentralized its governance through the Gitcoin DAO, with decision-making authority vested in holders of the GTC governance token. Although Gitcoin currently employs a one-token, one-vote system for governance, it has previously used quadratic voting to select its "Steward Council" and plans to continue experimenting with alternative voting mechanisms.

APPENDIX 13 - FUTARCHY

by Reuben Youngblom

Futarchy presents an alternative governance model originally proposed by economist Robin Hanson.[2531] In this system, citizens vote on what outcomes they want (such as economic growth, environmental health, or public happiness), while prediction markets are used to determine which policies are most likely to achieve these desired outcomes.

In practice, each policy proposal generates two separate prediction markets: One forecasts the outcome if the policy is implemented, and the other forecasts the outcome if the policy is not adopted. Market participants —acting as speculators— place bets based on their expectations of these respective outcomes. If the market associated with policy implementation consistently predicts more favorable metric values than the alternative, the policy is automatically enacted. This approach seeks to harness the informational efficiency of markets to inform policy decisions, thereby distinguishing the normative question of societal goals from the empirical question of how best to achieve them.

1. "Vote on values, but bet on beliefs"

The core principle of futarchy is "vote on values, but bet on beliefs"[2532] —meaning democratic processes to establish societal goals, but the practical means for achieving those goals are determined by market mechanisms that aggregate knowledge and forecasts from participants, who have financial incentives to be accurate.

In theory, futarchy integrates several influential concepts into a single governance model. First, it distinguishes between two fundamental questions: "What do we value?" and "What policies will achieve those values?" In conventional democratic systems, citizens typically vote based on their value judgments, selecting candidates whom they *hope* will act in accordance with their ideals. Futarchy, by contrast, aims to determine what specific proposals are actually *most likely* to lead to the world they want to see, thereby offering a more direct approach to aligning policy with collective goals.

Second, futarchy relies on economic incentives to increase the likelihood of reaching the "correct" answer. Because the "voting" is done via markets, where real financial stakes are involved, participants must risk their own money. This has two key effects: First, because those who make incorrect predictions incur financial losses, futarchy discourages participation by members who are uninformed or indifferent; second, it rewards participants who make accurate predictions, thereby encouraging individuals with superior information or strong convictions to engage. As a result, everyone is incentivized to vote carefully and honestly.

Third, futarchy aggregates information via market mechanics, drawing on the Hayekian tradition of markets as decentralized information-processing systems. Because futarchy allows anyone to vote, it captures information

2531 Robin Hanson, *Shall We Vote on Values, But Bet on Beliefs?,* 21 J. Pol. Phil. 151 (2013), https://mason.gmu.edu/~rhanson/futarchy2013.pdf.

2532 *Id*.

from a wide variety of individuals, each of whom places money on the outcome they believe is likely to prevail, based on their specific knowledge about the world.

2. Blockchain implementations

Although futarchy has significantly influenced theoretical discussions of blockchain governance,[2533] real-world implementations remained experimental for many years. Platforms such as Gnosis and Augur, which operate as prediction markets on Ethereum, possess the technical infrastructure necessary for futarchy, but they have not been employed for comprehensive governance. The most significant real-world deployment to date is MetaDAO, launched on the Solana blockchain in November 2023. Since 2024, MetaDAO has offered "Futarchy-as-a-Service" to other Solana projects, and in early 2025 the liquid-staking protocol Sanctum became the first Solana project to adopt MetaDAO for its full platform governance. Adoption nonetheless remains limited compared to traditional token-weighted governance platforms, and the long-term viability of market-based governance at scale remains an open empirical question.

APPENDIX 14 - EXIT SCAMS

An exit scam occurs when operators of a crypto exchange, platform, or project abruptly cease operations and disappear with user funds. Typically, the perpetrators first establish a business that appears legitimate then abruptly shut down the platform. The following cases illustrate some of the most significant exit scams in the history of the crypto industry, spanning multiple jurisdictions and revealing recurring patterns of fraud, flight, and protracted recovery.

- **QuadrigaCX (2018–2019)**: The Canadian-based exchange QuadrigaCX claimed its founder and CEO, Gerald Cotten, had died in India in December 2018, and that he had sole access to cold wallets containing customer funds.[2534] Over 76,000 clients were owed a combined amount of approximately $215 million in assets, and the bankruptcy trustee was able to recover or identify just $46 million, leaving clients with a collective shortfall of at least $169 million. The Ontario Securities Commission stated that, contrary to the speculation that the assets were lost or inaccessible due to the CEO's death, it found evidence demonstrating that the platform's collapse resulted from fraud committed by Cotten, who operated Quadriga like a Ponzi scheme.[2535]
- **PlusToken (2019)**: In 2019, the Chinese wallet/exchange PlusToken collapsed after collecting cryptocurrencies from millions of users worldwide, primarily in China and South Korea. The following year, a Chinese court sentenced the organizers of PlusToken to up to 11 years in prison, finding they had defrauded investors out of 14.8 billion yuan (approximately $2.25 billion) worth of cryptocurrencies through a classic Ponzi scheme with no real underlying business.[2536]
- **Thodex (2021)**: Faruk Fatih Özer, the founder of the Turkish exchange Thodex, fled the country in

2533 Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 6 J. Governance & Reg. 45 (2017) http://dx.doi.org/10.22495/jgr_v6_i1_p5; Vitalik Buterin, *An Introduction to Futarchy,* Ethereum Found. Blog (Aug. 21, 2014) https://blog.ethereum.org/2014/08/21/introduction-futarchy (early conceptualization for blockchain adoption by Vitalik)

2534 *Mystery as Quadriga Crypto-Cash Goes Missing*, BBC News (Mar. 5, 2019), https://www.bbc.com/news/technology-47454528.

2535 Ontario Securities Commission, *Quadrigacx: A Review by the Staff of the Ontario Securities Commission* (2020), https://www.osc.ca/quadrigacxreport/; Tara Deschamps, *Crypto exchange Quadriga was a fraud and founder was running Ponzi scheme, OSC report finds*, The Canadian Press (June 11, 2020), https://www.cbc.ca/news/business/osc-quadriga-gerald-cotten-1.5607990.

2536 Daniel Palmer, *Chinese Authorities Have Seized a Massive $4B in Crypto from Plus Token Scam*, CoinDesk (Nov. 27, 2020), https://www.coindesk.com/markets/2020/11/27/chinese-authorities-have-seized-a-massive-4b-in-crypto-from-plustoken-scam; *China Charges PlusToken Organizers in $2.3 Billion Crypto Scam,* Bloomberg (Nov. 27, 2020) https://www.bloomberg.com/news/articles/2020-11-28/china-charges-plustoken-organizers-in-2-3-billion-crypto-scam; *Chinese cryptocurrency scam ringleaders jailed in US$2.25 billion Ponzi scheme involving PlusToken platform*, South China Morning Post (Dec. 1, 2020), https://www.scmp.com/economy/china-economy/article/3112115/chinese-cryptocurrency-scam-ringleaders-jailed-us225-billion.

April 2021 after the platform abruptly suspended withdrawals, with Turkish prosecutors later alleging he absconded with approximately $2 billion in user assets.[2537] He was arrested in Albania and extradited back to Turkey, where a court found him, together with his brother and sister, guilty of money-laundering, fraud, and leading a criminal organization. The court sentenced each to imprisonment for 11,196 years for defrauding investors. Ozer was found dead by suicide in his prison cell in November 2025.[2538]

- **Africrypt (2021)**: The founders of the South African platform Africrypt, brothers Raees and Ameer Cajee, informed clients in April 2021 that operations had been halted because of a hack, and subsequently left South Africa. Early media reports suggested as much as $3.6 billion in Bitcoin had disappeared, but subsequent investigations placed the figure closer to $40 million to $50 million, with the exact amount of investor losses never officially reconciled.[2539] Investors filed complaints stating the brothers had "disappeared" with the money. Ameer Cajee was arrested in Zurich in 2021 in connection with a Swiss money-laundering investigation, reportedly while attempting to access hardware wallets held in safe-deposit boxes, and was later released on bail.[2540]

APPENDIX 15 - ROMANCE SCAMS AND WALLET DRAINERS

This appendix describes two prevalent categories of crypto-related fraud targeting individual users: romance scams, which rely on emotional manipulation, and wallet drainers, which exploit technical vulnerabilities in wallet approval mechanisms.

Romance scams leverage emotional manipulation to extract funds, often cryptoassets, from victims. A particularly pernicious variant of this scheme is known as "pig butchering," which combines emotional manipulation ("fattening up" victims) before deceiving them into sending money. These operations are frequently run by sophisticated criminal syndicates, including networks in Southeast Asia that forcibly traffic individuals into scam compounds.[2541] Scammers typically initiate contact via dating apps, social media, messaging platforms, or "wrong number" texts, cultivating emotional trust over weeks or months. The fraudsters then convince their targets to trust them and eventually persuade victims to invest in fraudulent schemes, including those relating to cryptoassets. Romance scams have emerged as one of the most financially damaging forms of fraud globally. The blockchain analytics firm TRM Labs estimates that at least $2.5 billion worth of crypto-related pig-butchering scams occurred globally on blockchains in 2024.[2542] The combination of psychological manipulation, technical sophistication, and emotional intimacy makes these scams especially effective and devastating.

2537 *Thodex Cryptocurrency Boss Jailed for 11,196 Years in Turkey for Fraud*, BBC News (Sept. 8, 2023), https://www.bbc.com/news/world-europe-66752785.

2538 *Defunct Turkish Crypto Founder Found Dead in Prison*, Hürriyet Daily News (Nov. 2, 2025), https://www.hurriyetdailynews.com/defunct-turkish-crypto-founder-found-dead-in-prison-215298.

2539 Chris Vallance, *Africrypt Brothers Deny Involvement in Bitcoin 'Heist'*, BBC News (June 25, 2021), https://www.bbc.com/news/technology-57582805.

2540 Jamie Crawley, *South African Police Investigate Missing Brothers' Crypto Platform, Africrypt*, CoinDesk (May 11, 2023), https://www.coindesk.com/business/2022/01/11/south-african-police-investigate-missing-brothers-crypto-platform-africrypt; *The Unraveling of Africrypt: South Africa's Bitcoin Ponzi Scheme Reaches Swiss Shores*, Satori News (Feb. 15, 2025), https://www.satorinews.com/articles/2025-02-14/the-unraveling-of-africrypt-south-africas-bitcoin-ponzi-scheme-reaches-swiss-shores-549805.

2541 Int'l Org. of Sec. Comm'ns, Policy (IOSCO), *Investor Education on Crypto-Assets* 17-19 (Oct. 2024), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD769.pdf.

2542 TRM Labs, *2025 Crypto Crime Report* 9–11 (2025), https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67f7132b33d3535ca28a54a4_TRM_2025%20Crypto%20Crime%20Report.pdf; TRM Labs, *Unmasking Pig Butchering Scams: The $4 Billion Crypto Scheme Preying on Vulnerable Investors* (Nov. 18, 2024), https://www.trmlabs.com/resources/blog/unmasking-pig-butchering-scams-the-4-billion-crypto-scheme-preying-on-vulnerable-investors.

Another rapidly growing category of crypto theft involves "wallet drainer" malware and malicious smart contracts that exploit token approvals. Victims are tricked into signing transactions that grant attackers permission to transfer assets directly from their wallets. Crypto-drainers employ several recurrent tactics: They create replicas of well-known websites, using nearly identical domain names; deploy fraudulent platforms that appear trustworthy —often surfacing as "sponsored" search results;[2543] or entice users with fake airdrops through phishing pages posing as legitimate token distribution campaigns. Once a user signs the malicious approval transaction, attackers drain all assets associated with the compromised wallet. Losses from wallet-drainer operations have surged sharply since 2022, now representing a substantial share of on-chain theft. According to Scam Sniffer, almost $300 million was drained from the wallets of 320,000 users in 2023 by wallet drainer scams, a figure that rose to approximately $494 million from over 332,000 victim addresses in 2024.[2544]

APPENDIX 16 - MALWARE DELIVERY SYSTEMS

by Sushmita Som

A distinct category of risk arises when blockchain infrastructure is used not as the target of an attack but as a component of malware delivery systems. In such campaigns, attackers embed malicious payloads or command-and-control (C2) references in smart contracts or blockchain transaction data. Because blockchains are decentralized and resistant to takedowns, this information can remain accessible even if traditional infrastructure—such as servers or domains used by the attackers—is disrupted.[2545] As a result, blockchain networks can function as a resilient coordination layer that enables malware operators to maintain or restore their command-and-control infrastructure.

Several campaigns illustrate this technique:

- **Glupteba botnet**. Glupteba infected more than one million computers, stealing user credentials and browser cookies, mining cryptocurrency on victims' devices, and deploying proxy infrastructure used for traffic anonymization and credit-card fraud. In December 2021, Google disrupted the botnet by taking down its command-and-control servers. Within hours, however, the operator broadcast a Bitcoin transaction embedding the address of a new C2 server. Infected machines monitoring the blockchain were able to retrieve the new address and reconnect to the botnet, effectively restoring the network.[2546]
- **EtherHiding.** Active since 2023, EtherHiding campaigns injected malicious JavaScript into compromised WordPress sites. The script retrieved a second-stage payload stored in smart contracts deployed on the BNB Smart Chain. Because the malicious code was hosted on the blockchain rather than on conventional web infrastructure, website operators and hosting providers could not easily remove it, making remediation significantly more difficult.[2547]

2543 Check Point Research, *Scammers Used Google Ads to Steal ~$500K Worth of Cryptocurrency* (Dec. 21, 2023), https://blog.checkpoint.com/security/scammers-used-google-ads-to-steal-500k-worth-of-cryptocurrency/.

2544 Scam Sniffer, *Scam Sniffer 2023: Crypto Phishing Scams Drain $300 Million from 320,000 Users* (Feb. 9, 2024), https://drops.scamsniffer.io/scam-sniffer-2023-crypto-phishing-scams-drain-300-million-from-320000-users/;Scam Sniffer, *Scam Sniffer 2024: Web3 Phishing Attacks – Wallet Drainers Drain $494 Million* (Jan. 3, 2025), https://drops.scamsniffer.io/scam-sniffer-2024-web3-phishing-attacks-wallet-drainers-drain-494-million/; *see also* Chainalysis, *2024 Crypto Crime Trends from Chainalysis* (Feb. 5, 2025), https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

2545 Taylor Monahan, *Blockchain Malware's Neverending Novelty*, MetaMask Security Blog (Nov. 3, 2025), https://metamask.io/news/blockchain-malwares-neverending-novelty.

2546 *Id.*; Elliptic, *Google Killed a Criminal Botnet. Did a Bitcoin Transaction Resurrect It?* (Dec. 10, 2021), https://www.elliptic.co/blog/google-killed-a-criminal-botnet-a-bitcoin-transaction-resurrected-it

2547 Monahan, *supra* note 2545.

- **Contagious Interview**. Active since 2023, this campaign—attributed to actors linked to the Democratic People's Republic of Korea (DPRK)—targets victims by impersonating cryptocurrency recruiters and has evolved over time to incorporate more sophisticated obfuscation techniques.[2548] Victims —typically developers seeking blockchain-related employment— are invited to complete coding tests that secretly execute malware. The campaign deploys multi-stage malicious software capable of stealing cryptocurrency wallets and corporate credentials across Windows, macOS, and Linux systems. Blockchain infrastructure is used to distribute or update elements of the malicious payload.
- **Cross-Chain TxDataHiding.** Identified in 2025, this technique distributes malware instructions across multiple blockchains—including TRON, Aptos, and BNB Smart Chain.[2549] By bouncing encrypted payload references across several networks, attackers make retrieval of malicious data appear indistinguishable from ordinary blockchain API traffic, complicating detection by network defenders.

In each of these cases, the blockchain component is grafted onto an otherwise conventional infection chain. The malware itself does not execute on the blockchain; rather, the blockchain functions as a resilient, censorship-resistant pointer system linking different stages of a traditional command-and-control infrastructure.

APPENDIX 17 - CRYPTO ASSETS AND MONEY TRANSMISSION REGULATION IN U.S. STATES

by Zeke Gillman

As of January 15, 2026, state regulation of crypto assets continues to evolve. U.S. states have adopted divergent and often fragmented approaches to regulating blockchain-based activities and crypto assets. Some states have emphasized investor protection and financial stability, issuing warnings about what they view as a highly speculative and potentially risky industry. Other states have taken a more permissive or innovation-oriented stance, using regulatory flexibility to attract blockchain and cryptocurrency businesses. At the state level, regulation has largely developed through the expansion, adaptation, or exemption from existing money transmission laws, which —depending on the jurisdiction— may or may not explicitly encompass digital assets within their legal scope.

Money transmission rules have thus become the central regulatory lever for U.S. states addressing crypto-asset activity. States have disagreed both on what activities should fall within the scope of such laws and on how those laws should be implemented in practice. As a result, state-level approaches vary significantly, ranging from bespoke licensing regimes to explicit statutory exemptions or reliance on interpretive guidance.

1. The CSBS and the Money Transmission Modernization Act (MTMA)

The Conference of State Bank Supervisors (CSBS) is an association representing state banking and financial

2548 Unit 42, *North Korean Threat Actors Lure Tech Job Seekers as Fake Recruiters*, Palo Alto Networks (June 17, 2025), https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/.

2549 *Id*.

regulators across the United States.[2550] In 2021, the CSBS coordinated efforts among states to develop a model framework to modernize money transmission regulation.[2551] This effort resulted in the Money Transmission Modernization Act (MTMA), a model law intended to be adopted, in whole or in part, at the discretion of individual states.[2552] By 2024–2025, a significant number of states had introduced or partially enacted MTMA-based legislation, though adoption has been uneven and often incomplete.[2553] Some states have implemented large portions of the model law, while others have adopted only selected provisions or used the MTMA as informal guidance rather than binding law.

During negotiations over the MTMA, states were unable to reach consensus on the treatment of virtual currency. As a result, the MTMA includes an optional article on virtual currency, which states may choose to adopt.[2554] That optional article addresses issues such as licensing, custody, and consumer protection obligations for certain virtual currency activities, but it does not mandate a uniform approach.[2555] Only a small number of states —most clearly Minnesota and North Dakota— have enacted the optional article on virtual currency substantially as drafted.[2556] Other states that adopted elements of the MTMA have either omitted the virtual currency article altogether or chosen to regulate crypto-asset activities through separate statutes, agency rules, or interpretive guidance.

Texas provides a prominent example of a state that has adopted portions of the MTMA while issuing separate guidance for virtual currency.[2557] Under Texas law and regulatory guidance issued by the Texas Department of Banking (TXDOB), non-stablecoin virtual currency is expressly excluded from the definition of "money" and is not treated as having "monetary value" for money transmission purposes. As a result, engaging solely in transactions involving non-stablecoin virtual currency does not, by itself, trigger a money transmitter licensing requirement. By contrast, activities involving stablecoins may fall within the scope of money transmission regulation, and the MTMA-based framework applies in those cases. Texas has also enacted House Bill 1666 (2023), which imposes obligations on certain custodial digital asset service providers, including requirements relating to the segregation of customer assets, proof-of-reserves disclosures, and annual reporting.[2558]

2. New York: the BitLicense regime

Other states have pursued regulatory objectives similar to those reflected in the MTMA's optional virtual currency article through stand-alone crypto-specific licensing frameworks. New York is the most prominent example.

In 2015, the New York Department of Financial Services (NYDFS) introduced the BitLicense, a statewide licensing

2550 Conference of State Bank Supervisors, https://www.csbs.org/ (last visited Jan. 15, 2026); Montana Division of Banking & Financial Institutions, *2021 Annual Report* (2021), https://banking.mt.gov/_docs/News-and-Consumer-Alerts/CSBS-Report-2021-annual_web.pdf.

2551 Cooley LLP , *U.S. States Adopt Model Money Transmission Act, but Harmonization Remains Elusive* (Aug. 20, 2024), https://www.cooley.com/news/insight/2024/2024-08-20-us-states-adopt-model-money-transmission-act-but-harmonization-remains-elusive; CSBS, *CSBS Releases Model for the Future of Payments Regulation* (Sept. 9, 2021), https://www.csbs.org/newsroom/csbs-releases-model-future-payments-regulation

2552 Conference of State Bank Supervisors, *CSBC Money Transmission Modernization Act* (Feb. 2023), https://www.csbs.org/sites/default/files/2023-02/CSBS%20Money%20Transmission%20Modernization%20Act.pdf.

2553 Cooley LLP, *supra* note 2551.

2554 CSBS, *supra* note 2552.

2555 *Id.* § 13.03; Tex. Dep't of Banking, *Response to Request by Senate Bus. & Com. Comm. re: Money Transmission Modernization Act* 6 (Nov. 16, 2022), https://www.dob.texas.gov/sites/default/files/files/news/Testimony/2022/11.17.22t.pdf

2556 Cooley LLP, *supra* note 2551.

2557 Tex. Dep't of Banking, Supervisory Memorandum 1037: Regulatory Treatment of Virtual Currencies Under the Money Services Modernization Act (Jan. 28, 2025), https://www.dob.texas.gov/sites/default/files/files/Laws-Regulations/New-Actions/sm1037.pdf (last visited Jan. 15, 2026); Tex. Dep't of Banking, *Texas Legislature Passes Legislation Impacting Money Services Businesses* 1 (Aug. 21, 2023), https://www.dob.texas.gov/sites/default/files/files/news/Industrynotices/in2023-03.pdf.

2558 Cooley LLP, *supra* note 2551.

requirement for businesses engaging in "virtual currency business activity." Firms operating in New York must either obtain a BitLicense or qualify under an alternative authorization, such as a charter under New York Banking Law.[2559] The BitLicense regime imposes extensive requirements, including capital adequacy standards, anti-money laundering and know-your-customer obligations, cybersecurity controls, and consumer protection measures.[2560]

The BitLicense regime has also been subject to significant regulatory scrutiny.[2561] In a January 2024 audit, the New York State Comptroller's Office concluded that "there is limited assurance that DFS is adequately performing its oversight responsibilities related to the application for and supervision of BitLicenses in the State, creating the risk that licenses could be granted to applicants whose financial stability has not been thoroughly verified or that, once licensed, businesses may not maintain financial or cybersecurity standards."[2562] NYDFS disputed aspects of the audit and indicated that changes in leadership and internal processes had addressed the identified deficiencies, though the adequacy of these reforms remains debated.[2563] On December 4, 2025, the New York State Comptroller's Office issued a follow-up report evaluating DFS's corrective actions and ongoing supervision of BitLicense holders.[2564] In January 2026, NYDFS also published its annual Regulatory Agenda outlining potential rulemaking affecting virtual currency supervision and licensing.[2565]

New York legislators have also considered additional crypto-related measures. Several pending bills sit in the New York legislature, including a regulatory sandbox program for fintech products and services,[2566] along with a moratorium on proof-of-work mining operations[2567] and the establishment of a cryptocurrency and blockchain task force.[2568] Additional crypto-related bills were introduced in the 2026 legislative session, reflecting continued legislative attention to digital asset oversight.[2569]

3. California

As the home of Silicon Valley, California plays a significant role in shaping national approaches to the regulation of emerging technologies. In 2022, Governor Gavin Newsom signed an executive order "to create a transparent and consistent business environment for companies operating in blockchain, including crypto assets and related financial technologies".[2570] Following some initial legislative uncertainty over whether virtual currencies fall

2559 N.Y. State Dep't of Fin. Servs., *Virtual Currency Businesses*, https://www.dfs.ny.gov/virtual_currency_businesses (last visited Jan. 15, 2026).

2560 Wharton Initiative on Financial Policy and Innovation, *50-State Review of Cryptocurrency Regulation*, Wharton School, Univ. of Pa. https://stevenscenter.wharton.upenn.edu/publications-50-state-review/ (last visited Jan. 15, 2026).

2561 David Hollerith, *New York's Crypto BitLicense Oversight Criticized*, Yahoo! (updated Jan 9, 2024), https://finance.yahoo.com/news/yorks-crypto-bitlicense-oversight-criticized-170722251.html.

2562 Office of the N.Y. State Comptroller, *Virtual Currency Licensing* Report No. 2024-S-18 (Jan. 2024) https://www.osc.ny.gov/files/state-agencies/audits/pdf/sga-2024-22s18.pdf.

2563 *Id.*; Hollerith, *supra* note 2561.

2564 N.Y. State Comptroller, *Virtual Currency Licensing* (Follow-Up) (2025-F-4) (Dec. 4, 2025), https://www.osc.ny.gov/files/state-agencies/audits/pdf/sga-2026-25f4.pdf.

2565 N.Y. Dep't of Fin. Servs., *Regulatory Agenda* (Jan. 13, 2026), https://www.dfs.ny.gov/system/files/documents/2026/01/2026-DFS-Regulatory-Agenda.pdf.

2566 N.Y. A.B. 3747, 244th Leg., Reg. Sess. (2021), https://www.assembly.state.ny.us/leg/?bn=a3747; N.Y. A.B. 3336, 244th Leg., Reg. Sess. (2021), https://www.assembly.state.ny.us/leg/?bn=A03336&term=2021.

2567 N.Y. A.B. 7742, 244th Leg., Reg. Sess. (2021), https://www.assembly.state.ny.us/leg/?bn=A07742&term=2021; N.Y. A.B. 7389, 244th Leg., Reg. Sess. (N.Y. 2021) https://nyassembly.gov/leg/?bn=A07389&term=2021.

2568 N.Y. S.B. 5044, 244th Leg., Reg. Sess. (2021), https://www.assembly.state.ny.us/leg/?bn=S05044&term=2021.

2569 See Press Release, Manhattan Dist. Att'y's Off. & Sen. Zellnor Myrie, *D.A. Bragg, Senator Myrie Announce New Bill to Combat Use of Cryptocurrency to Commit Crimes* (Jan. 14, 2026), https://manhattanda.org/d-a-bragg-senator-myrie-announce-new-bill-to-combat-use-of-cryptocurrency-to-commit-crimes/ (last visited Jan. 15, 2026).

2570 Cal. Exec. Order, No. N-9-22 (May 4, 2022), https://www.gov.ca.gov/wp-content/uploads/2022/05/5.4.22-Blockchain-EO-N-9-22-signed.pdf.

within existing money transmission laws, the California Legislature enacted the Digital Financial Assets Law (DFAL).[2571] The DFAL establishes a comprehensive licensing and supervisory framework for businesses engaged in digital financial asset activity with California residents. This framework covers custody, exchange, and related services. The licensing effective date is July 1, 2026.[2572] Once effective, the law will require covered entities to obtain authorization from state regulators and comply with prudential and consumer-protection requirements.

4. Wyoming

Wyoming has been the most active U.S. state in adopting blockchain-specific legislation. Since 2019, the state has enacted approximately thirty crypto- and blockchain-related laws,[2573] deliberately positioning itself as a crypto-friendly jurisdiction. These measures include exemptions from money transmission and securities laws for certain virtual currency activities,[2574] the creation of regulatory sandboxes,[2575] and statutory recognition of decentralized autonomous organizations (DAOs).[2576]

Wyoming has also authorized the chartering of Special Purpose Depository Institutions (SPDIs),[2577] which are state-regulated banks designed to serve digital asset businesses. In 2023, Wyoming enacted the Wyoming Stable Token Act, establishing the legal framework for the issuance of a state-backed stablecoin. Following a period of institutional design and implementation, the state publicly launched its stable token in January 2026, thereby operationalizing the statutory framework.[2578]

5. Louisiana

Louisiana has adopted a stand-alone regulatory framework for virtual currency activity, rather than relying exclusively on its money transmission statute.[2579] The law took effect on January 1, 2023, and licensing applications are administered through the Nationwide Multistate Licensing System (NMLS).[2580] The statute includes limited exemptions for low-volume activity, though the precise monetary thresholds and conditions are narrowly defined and subject to regulatory interpretation.[2581]

6. Illinois

Illinois has actively promoted blockchain innovation while relying largely on regulatory guidance rather than bespoke licensing laws.[2582] State guidance distinguishes between transactions involving only virtual currency

2571 Cal. Dep't of Fin. Prot. & Innovation, *Digital Financial Assets*, https://dfpi.ca.gov/regulated-industries/digital-financial-assets/ (last visited Jan. 15, 2026); Jennifer O'Brien, *California's Digital Financial Assets Law*, Dechert LLP (Nov. 29, 2023), https://www.dechert.com/knowledge/onpoint/2023/11/california-s-digital-financial-assets-law.html.

2572 *Id.*

2573 Olga Kharif, *Wyoming's Crypto-Friendly Aspirations Are Colliding With Economic Reality*, Bloomberg (Sept. 5, 2023), https://www.bloomberg.com/news/articles/2023-09-05/wyoming-s-crypto-friendly-aspirations-are-colliding-with-economic-reality.

2574 Wyo. Stat. Ann. § 40-22-104 (2021), https://law.justia.com/codes/wyoming/2021/title-40/chapter-22/section-40-22-104/.

2575 *Id.* § 40-29-103 (2021).

2576 S.F. 50, 67th Leg., Budget Sess. (Wyo. 2024), https://www.wyoleg.gov/Legislation/2024/SF0050.

2577 Melissa Pereira, *Regulatory Landscape in Wyoming and Wyoming's Leadership in Cryptocurrency*, BU Rev. Banking & Fin. L. Blog (Mar. 28, 2022), https://www.bu.edu/rbfl/2022/03/28/regulatory-landscape-in-wyoming-and-wyomings-leadership-in-cryptocurrency.

2578 S.F. 127, 67th Leg., Gen. Sess. (Wyo. 2023), https://www.wyoleg.gov/Legislation/2023/SF0127; Press Release, Office of Governor Mark Gordon, *Wyoming Ushers in New Era, Launches First-of-Its-Kind Frontier Stable Token for Public Purchase* (Jan. 7, 2026), https://governor.wyo.gov/news-releases/wyoming-ushers-in-new-era-launches-first-of-its-kind-frontier-stable-token-for-public-purchase.

2579 La. Office of Fin. Insts., *Virtual Currency Business Act* (July 31, 2023), https://ofi.la.gov/messages/virtual-currency-businesses-act-2023-legislation/ (last visited Jan. 15, 2026).

2580Cooley LLP, *Louisiana's Virtual Currency Licensing Law Taking Effect Finally* (Nov. 21, 2022), https://www.cooley.com/news/insight/2022/2022-11-21-louisianas-virtual-currency-licensing-law-taking-effect-finally.

2581 La. Rev. State. Ann. § 6:1389 (2021); Cooley LLP, *Louisiana's Virtual Currency Licensing Law Taking Effect Finally* (Nov. 21, 2022), https://www.cooley.com/news/insight/2022/2022-11-21-louisianas-virtual-currency-licensing-law-taking-effect-finally.

2582 Ill. Dep't of Fin. & Pro. Reg., *Digital Currency Regulatory Guidance*, https://idfprapps.illinois.gov/Forms/DFI/CCD/IDFPR%20-%20Digital%20Currency%20Regulatory%20Guidance.pdf (last visited Jan. 15, 2026).

—which generally do not require a money transmitter license— and transactions involving fiat currency at any point, which typically do. Illinois has also enacted a series of blockchain-friendly statutes, including the Illinois Blockchain Technology Act[2583], which recognizes the legal validity of blockchain-based records and smart contracts. In addition, the Blockchain Business Development Report called for studies and policy recommendations to support blockchain adoption within the state.[2584]

7. Florida

Florida's approach to crypto-asset regulation has been shaped significantly by litigation. In *State v. Espinoza,*[2585] the defendant sold bitcoin for cash to an undercover agent and was charged with money laundering and operating an unregistered money services business. The trial court concluded that Florida's money transmission laws did not apply to bitcoin transactions,[2586] but an appellate court later reversed that decision.[2587] In response, Florida enacted House Bill 273 (2022),[2588] which effectively abrogated the *Espinoza* ruling. Under the new law, a money transmitter license is generally required only for intermediaries, not for peer-to-peer, two-party transactions of the type at issue in *Espinoza*.[2589] Florida has also established a Financial Technology Sandbox, allowing qualifying blockchain and cryptocurrency businesses to test products under relaxed regulatory conditions.[2590]

8. Other states

Several other jurisdictions have adopted explicit statutory or regulatory frameworks addressing virtual currency activities, either through bespoke regimes or by expressly incorporating crypto assets into money transmission laws. These include Alabama,[2591] Alaska,[2592] Colorado,[2593] Connecticut,[2594] Idaho,[2595] Maine,[2596] Michigan,[2597] Minnesota,[2598] New Mexico,[2599] Oregon,[2600]

2583 Illinois General Assembly, *Blockchain Technology Act*, 205 Ill. Comp. Stat. 730, https://www.ilga.gov/Legislation/ILCS/Articles?ActID=4030&ChapterID=20 (last visited Jan. 15, 2026).

2584 Ill. Dep't of Fin. & Pro. Reg., *Blockchain Business Development Report* (Dec. 31 2020), https://www.ilga.gov/documents/reports/ReportsSubmitted/2366RSGAEmail4096RSGAAttachIDFPR%20Div%20of%20Banking_Blockchain%20Report-6.pdf .

2585 264 So. 3d 1055 (Fla. Dist. Ct. App. 2019).

2586 K&L Gates., *Trouble in Paradise: Florida Court Rules that Selling Bitcoin is Money Transmission* (Feb. 13, 2019), https://www.klgates.com/Trouble-in-Paradise-Florida-Court-Rules-that-Selling-Bitcoin-is-Money-Transmission-02-13-2019.

2587 *Id.*

2588 *See* Fla. Stat. § 559.952 (2021).

2589 *Id.*

2590 *Id.*

2591 Ala. Code § 8-7a-5 (2021), https://law.justia.com/codes/alabama/2021/title-8/chapter-7a/section-8-7a-5/ .

2592 Alaska Dep't of Commerce, Consumer Finance Div., *Money Service Businesses*, https://www.commerce.alaska.gov/web/dbs/ConsumerFinance/MoneyServiceBusinesses.aspx (last visited Jan. 15, 2026).

2593 Colo. Div. of Banking, *Regulatory Guidance: Cryptocurrency and the Colorado Money Transmitters Act* (Sept. 20, 2018), https://www.colorado.gov/pacific/dora/node/141156.

2594 Conn. Gen. Stat. § 36a-597 (2020).

2595 Idaho Dep't of Fin., *Money Transmitters*, https://www.finance.idaho.gov/securities-bureau/money-transmitters/ (last visited Jan. 15, 2026).

2596 Me. Rev. Stat. tit. 32, § 6103 (2021)

2597 Mich. Comp. Laws § 487.1011 (2021).

2598 Minn. Dep't of Commerce, *Cryptocurrency Investments Regulation*, https://mn.gov/commerce/money/investments/cryptocurrency/ (last visited Jan. 15, 2026).

2599 N.M. Reg. & Licensing Dep't, Fin. Institutions Div., *Money Services Businesses*, https://www.rld.nm.gov/financial-institutions/who-we-regulate/money-services-businesses/ (last visited Jan. 15, 2026).

2600 Or. Rev. Stat. § 717.205 (2021).

South Dakota,[2601] Vermont,[2602] Washington,[2603] and Washington D.C.[2604] However, these varied frameworks are not equivalent to New York's BitLicense regime. In many cases, regulation occurs through amendments to existing money transmission statutes or through regulatory guidance rather than through crypto-specific licensing laws. Connecticut's money transmission rules (the "Act"),[2605] for instance, were amended in 2015 to include virtual currency businesses, as was Washington's "Uniform Money Services Act."[2606] Other states have taken the opposite approach by explicitly exempting virtual currency activities from money transmission requirements, most notably Hawaii.[2607] Montana remains unique in having no state-level money transmission licensing regime at all.[2608]

APPENDIX 18 - JAPAN

by Adrian Mak

Initially cautious, Japan's approach toward digital assets has evolved toward embracing them while maintaining robust consumer protections. The Financial Services Agency (FSA) serves as the primary regulator for crypto assets activities in Japan.[2609] The Japan Financial Intelligence Center (JAFIC) also plays a crucial role in monitoring for and preventing illicit financial activities in the crypto sector.[2610]

1. Regulation of crypto assets: the Payment Services Act (PSA)

Under Japanese law, crypto assets are generally not classified as "securities" and are instead regulated primarily under the Payment Services Act (PSA), which was revised in 2017 in order to cover virtual currencies.[2611] In 2019, amendments to the PSA renamed "virtual currency" as "crypto assets" to align with international terminology.[2612] The PSA now regulates Crypto Asset Exchange Services ("CAES"), which include trading, brokerage, intermediation, management, and safekeeping of crypto assets.

This framework requires entities providing CAES to register with the Financial Services Agency (FSA).[2613] Furthermore, while the PSA already imposed asset segregation and anti-money laundering (AML) obligations, it was relatively minimal from the perspective of user protection and AML/counter-terrorist financing.[2614] Following several high-profile hacks of cryptocurrency

2601 S.D. Codified Laws § 51A-17-4 (2021).

2602 Vt. Stat. Ann. 8 § 2502 (2021).

2603 Wash. Rev. Code § 19.230.030 (2021).

2604 United States v. 155 Virtual Currency Assets, Memorandum Opinion, No. 20-cv-2228 (RC), 2021 WL 1251139 (D.D.C. Apr. 9, 2021), https://www.govinfo.gov/content/pkg/USCOURTS-dcd-1_20-cv-02228/pdf/USCOURTS-dcd-1_20-cv-02228-0.pdf

2605 Orrick, *Connecticut Amends Its Money Transmission Act*, Orrick Info Bytes (June 14, 2024), https://infobytes.orrick.com/2024-06-14/connecticut-amends-its-money-transmission-act/.

2606 Wash. Rev. Code § 19.230.030 (2021), https://law.justia.com/codes/washington/2021/title-19/chapter-19-230/section-19-230-030/ .

2607 Helen Partz, *Hawaii crypto firms no longer need MT license, regulator rules*, Coin Telegraph (July 1, 2024), https://cointelegraph.com/news/hawaii-crypto-money-transmitter-license.

2608 Mont. Dep't of Admin., *Money Transmitters*, https://banking.mt.gov/moneytransmitters (last visited Jan. 15, 2026).

2609 Tomoko Amaya, *Regulating the Crypto Assets Landscape in Japan*, Fin. Servs. Agency of Japan (Dec. 7, 2022) https://www.fsa.go.jp/en/news/2022/20221207/01.pdf .

2610 Team Sanction Scanner, *Cryptocurrency Regulations in Japan*, Sanction Scanner (Aug. 12, 2021), https://www.sanctionscanner.com/blog/cryptocurrency-regulations-in-japan-492?

2611 Payment Services Act, Act No. 59 of 2009 (Japan), https://www.japaneselawtranslation.go.jp/en/laws/view/3965.

2612 K&L Gates, *Japan's New Crypto Regulation: 2019 Amendments to Payment Services Act and Financial Instruments and Exchange Act of Japan* (Nov. 26, 2019), https://www.klgates.com/Japans-New-Crypto-Regulation-2019-Amendments-to-Payment-Services-Act-and-Financial-Instruments-and-Exchange-Act-of-Japan-11-26-2019.

2613 Masakazu Masujima, So Saito & Yuka Rikino, *Blockchain & Cryptocurrency Laws & Regulations 2025: Japan*, Global Legal Insights (Sept. 2024), https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/japan/.

2614 Takeshi Nagase, Takato Fukui, Keisuke Hatano & Huan Lee (Henry) Tan, *Blockchain & Cryptocurrency Laws & Regulations 2025: Japan*, Global Legal Insights (Sept. 2024), https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/japan/.

exchanges, Japanese authorities progressively strengthened their regulatory approach. Amendments introduced enhanced consumer protection measures, expanded the regulatory perimeter to include crypto asset derivative transactions, and clarified the regulatory treatment of custodial services.

2. Regulation of crypto derivatives and token offerings: the Financial Instruments and Exchange Act (FIEA)

The Financial Instruments and Exchange Act (FIEA) regulates crypto derivatives and certain token offerings. Following the 2019 amendments, the FIEA explicitly started covering crypto asset derivative transactions and token offerings that qualify as "Electronically Recorded Transferable Rights" and exhibit characteristics similar to traditional securities.[2615]

Initial Coin Offerings (ICOs) and Security Token Offerings (STOs) are regulated depending on their legal characteristics. Tokens granting profit-sharing or similar investor rights are classified as "Electronically Recorded Transferable Rights" under the FIEA, while other tokens may fall under the PSA as crypto assets.

3. Stablecoins

Amendments to the PSA enacted in 2022 and entering into force on June 1, 2023, formally defined stablecoins as "Electronic Payment Instruments".[2616] "Digital money-type stablecoins" are legally defined as "Electronic Payment Instruments" and must be fully backed by fiat currency and redeemable at par. By contrast, so-called "crypto asset-type stablecoins" are not a formal statutory category but rather describe tokens that resemble traditional crypto assets while incorporating price-stabilization mechanisms.[2617]

Under this framework, digital money-type stablecoins may only be issued by banks, fund transfer service providers, and trust companies. Tokenized deposits remain a legally distinct category of instrument.[2618] Intermediaries involved in trading or managing stablecoins must register as Electronic Payment Instruments Exchange Service Providers under the PSA framework.

4. Future reforms

In April 2025, the FSA released a discussion paper as part of an ongoing regulatory consultation, proposing to divide cryptocurrencies into two broad categories:[2619]

- **Type 1** (Funding / Business Crypto Assets): crypto assets used primarily to raise funds or support the business operations of an issuing project, often including tokens issued by early-stage or community-funded ventures.
- **Type 2** (Non-Fundraising / Non-Business Crypto Assets): more established or decentralized crypto assets, such as Bitcoin and Ethereum, which are not issued to raise funds for a specific business entity.

These proposed categories do not yet have binding legal effect and have not been formally incorporated into statute.

2615 Tsuguhito Omagari & Yuki Sako, *Japan's New Crypto Regulation: 2019 Amendments to Payment Services Act and Financial Instruments and Exchange Act of Japan*, K&L Gates (Nov. 26, 2019), https://www.klgates.com/Japans-New-Crypto-Regulation-2019-Amendments-to-Payment-Services-Act-and-Financial-Instruments-and-Exchange-Act-of-Japan-11-26-2019.

2616 Keiji Tonomura, Shu Sasaki, Kazuyuki Ohno & Otoki Shimizu, *Trends and Developments: Japan*, *in* Fintech 2025 (Chambers Partners 2025) https://practiceguides.chambers.com/practice-guides/fintech-2025/japan/trends-and-developments.

2617 Tokyo International Law Office, *Regulatory Landscape in Japan for Stablecoins and Related Payment Services* (Feb. 27, 2024), https://www.tkilaw.com/en/7053.

2618 *Id*.

2619 Financial Services Agency, *Discussion Paper: Examination of the Regulatory Systems Related to Cryptoassets* 8–10 (Apr. 9, 2025), https://www.fsa.go.jp/en/news/2025/20250410_2/02.pdf; Arvin Kamberi, *Japan's FSA proposes new framework for regulating crypto assets in Japan*, Digital Watch Observatory (Apr. 11, 2025), https://dig.watch/updates/japans-fsa-proposes-new-framework-for-regulating-crypto-assets-in-japan.

APPENDIX 19 - SINGAPORE

by Adrian Mak

Singapore has strategically positioned itself as a leading global hub for digital assets, adopting a nuanced, risk-based, and adaptive regulatory philosophy.[2620]

1. Key legislation and classifications

- **The Payment Services Act (PSA) 2019** serves as the cornerstone of Singapore's digital asset regulation.[2621] The PSA was significantly expanded through the Payment Services (Amendment) Act 2021, with key amendments brought into force on April 4, 2024.[2622] The PSA establishes a comprehensive licensing framework for a wide range of payment services, with a particular focus on those involving Digital Payment Tokens (DPTs) —most commonly, blockchain-based cryptocurrencies such as bitcoin and ether.[2623]
- **The Securities and Futures Act (SFA) 2001**[2624] applies to digital tokens that functionally resemble traditional capital markets products, such as shares, debentures, or units, in a collective investment scheme (CIS).[2625] This means that blockchain-based security tokens are treated under the SFA with the same regulatory rigor as conventional securities.[2626] Issuers and intermediaries must comply with prospectus, licensing, and conduct requirements, ensuring investor protection and market integrity within Singapore's digital asset ecosystem.
- **The Financial Services and Markets Act (FSMA) 2022,**[2627] implemented in phases since April 2023, applies to Singapore-based entities offering digital token services outside Singapore.[2628] This aligns Singapore's framework with international standards, such as those of the Financial Action Task Force (FATF), and mitigates risks of regulatory arbitrage.[2629] In June 2025, the Monetary Authority of Singapore (MAS) operationalised a licensing regime for Digital Token Service Providers (DTSPs) under the Financial Services and Markets Act 2022 (FSMA), requiring Singapore-incorporated entities that provide digital token services exclusively to clients outside Singapore to obtain a DTSP licence and comply with AML/CFT and prudential requirements comparable to those applicable under existing financial regulatory frameworks.[2630]
- **Single-currency-pegged stablecoins (SCS)** issued in Singapore are regulated by a bespoke regulatory

2620 Peiying Chua, Alcander Seah & Tobias Jenie, *Singapore: Digital Assets Regulation State Of Play*, IFC Review (May 20, 2024), https://www.ifcreview.com/articles/2024/may/singapore-digital-assets-regulation-state-of-play/.

2621 Payment Services Act 2019 (2020 Rev. Ed.) (Sing.), https://sso.agc.gov.sg/Act/PSA2019.

2622 Monetary Authority of Singapore, *MAS Expands Scope of Regulated Payment Services; Introduces User Protection Requirements for Digital Payment Token Service Providers* (Apr. 2, 2024), https://www.mas.gov.sg/news/media-releases/2024/mas-expands-scope-of-regulated-payment-services.

2623 Zodia Custody, *Singapore's Bold Approach to Regulating Digital Assets* , https://zodia-custody.com/singapores-bold-approach-to-regulating-digital-assets/ (last visited Jan. 15, 2026).

2624 Securities and Futures Act 2001 (Sing.), https://sso.agc.gov.sg/Act/SFA2001.

2625 Monetary Authority of Singapore, *A Guide to Digital Token Offerings* (Nov. 14, 2017), https://www.mas.gov.sg//media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf.

2626 Clifford Chance, *Security Token Offerings: Regulation Across Asia Pacific* (Nov. 2020) (briefing), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/11/security-token-offerings-regulation-across-apac-pacific.pdf.

2627 Financial Services and Markets Act 2022 (Sing.), https://www.mas.gov.sg/regulation/acts/financial-services-and-markets-act-2022.

2628 Allen & Gledhill, *Implementation of Financial Services and Markets Act 2022 in Phases with New Provisions on Technology Risk Management in Force* (May 27, 2024), https://www.allenandgledhill.com/sg/publication/articles/28137/implementation-of-financial-services-and-markets-a-ct-2022-in-phases-with-new-provisions-on-technology-risk-management-in-force.

2629 Reed Smith LLP, *Expanding the Territorial Scope of Singapore Digital Asset Regulation – MAS Consults on New Rules* (Oct. 10, 2024), https://www.reedsmith.com/en/perspectives/2024/10/expanding-the-territorial-scope-of-singapore-digital-asset-regulation.

2630 Monetary Authority of Singapore *MAS Clarifies Regulatory Regime for Digital Token Service Providers* (June 6, 2025), https://www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers.

framework adopted by the Monetary Authority of Singapore (MAS) in 2023.[2631] Issuers must meet strict requirements regarding reserve backing with high-quality, liquid assets, minimum capital, redemption at par within prescribed timeframes, and comprehensive disclosures.

- **Non-Fungible Tokens (NFTs)** are not regulated as a distinct asset class. Due to their non-fungible nature, NFTs generally do not meet the PSA definition of digital payment tokens and therefore fall outside its scope.[2632] Certain NFTs may qualify as "limited purpose digital payment tokens" in narrow circumstances, such as in-game assets that are non-transferable or not exchangeable for money.[2633]

2. Obligations of digital payment token-related services

The Payment Services Act 2019 targets service providers who offer activities related to digital payment tokens — providers such as cryptocurrency exchanges, custodial wallet providers (i.e., entities exercising control over customer assets), brokers, and custodians.[2634] Non-custodial software wallet providers, where no control is exercised over user assets, generally fall outside the scope of regulation. Digital Payment Tokens (DPTs) are defined as digital representations of value that are expressed as a unit, are not denominated in or pegged to any currency, and are intended to be used as a medium of exchange accepted by the public. They can be transferred, stored, or traded electronically and must satisfy additional characteristics prescribed by the Monetary Authority of Singapore (MAS).[2635] DPTs expressly exclude digital representations issued or guaranteed by governments or central banks.

Under the PSA, regulated entities must obtain a license from the MAS and comply with stringent requirements designed to mitigate risks such as money laundering, terrorism financing, and threats to consumer protection.[2636] Licenses are categorised based on the scope of the provider's activity (Money-changing, Standard Payment Institution, or Major Payment Institution) and its transaction/float threshold.[2637] Licensing requirements generally include Singapore incorporation (or registration of a branch), a permanent place of business, fit-and-proper management, and a minimum base capital (e.g., S$100,000 for a Standard Payment Institution), supplemented by activity-specific and risk-based capital requirements.[2638]

The Payment Services (Amendment) Act 2021 expanded regulatory oversight to cover:[2639]

- the safeguarding and custody of DPTs and related instruments where the provider exercises control over customer assets;
- the transfer of DPTs, including arranging or facilitating DPT transmissions between accounts;

2631 Monetary Authority of Singapore, *MAS Finalises Stablecoin Regulatory Framework* (Aug. 15, 2023), https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework.

2632 Ben Chester Cheong, *Application of Blockchain-enabled Technology: Regulating Non-Fungible Tokens (NFTs) in Singapore,* Law Gazette (Jan. 2022), https://lawgazette.com.sg/feature/application-of-blockchain-enabled-technology-nfts/.

2633 *Id.*

2634 Clyde & Co, *Singapore: Payment Services Act to Now Cover Token Transfer and Custody* (Apr. 4, 2024), https://www.clydeco.com/en/insights/2024/04/singapore-payment-services-act-to-now-cover-token.

2635 Payment Services Act 2019, s. 2(1) (Sing.), https://sso.agc.gov.sg/Act/PSA2019.

2636 *Id.*

2637 Monetary Authority of Singapore, *Types of Payment Services* , https://www.mas.gov.sg/regulation/payments/licensing-for-payment-service-providers/types-of-payment-services (last visited Jan. 15, 2026).

2638 Wayston Compliance Solutions, *Compliance Obligations under the New Payment Services Act* (Dec. 10, 2021) https://compliance.waystone.com/compliance-obligations-under-new-payment-services-act/.

2639 Payment Services (Amendment) Act 2021, No. 1 of 2021 (Sing.), https://sso.agc.gov.sg/Acts-Supp/1-2021/Published/20210301?DocDate=20210301 (amending the Payment Services Act 2019 and subsequently brought into force on Apr. 4, 2024).

- the facilitation of DPT exchanges, even where the service provider does not take possession of the funds or tokens; and
- inducing or attempting to induce persons, by way of business, to buy or sell DPTs, encompassing brokerage and certain advisory activities.

These amendments granted the Monetary Authority of Singapore enhanced powers[2640] to introduce regulations for DPT service providers concerning user protection (such as the safeguarding of customer assets), and to impose measures on DPT service providers in the interest of the public, financial stability, or monetary policy.

Overall, the amended PSA imposes robust safeguards aimed at protecting consumers and maintaining financial stability —including mandatory segregation and trust arrangements for customer assets, user-protection measures, and enhanced AML/CFT controls.[2641] Comprehensive AML/CFT obligations apply, including customer due diligence (CDD), transaction monitoring, sanctions screening, suspicious transaction reporting, recordkeeping, independent audits, and compliance with the Financial Action Task Force (FATF) Travel Rule for qualifying cross-border DPT transfers.[2642]

APPENDIX 20 - SWITZERLAND

by Claude Humbel

Switzerland has long adopted an innovation-friendly and pragmatic approach to blockchain technology and its applications, particularly in the area of the tokenization of financial instruments.[2643] Swiss authorities —including the Swiss Financial Market Supervisory Authority (FINMA), the Swiss Federal Council, and several cantons and municipalities (notably the Canton of Zug[2644] and the City of Lugano with its "Plan ₿"[2645])— have actively acknowledged the economic potential of distributed ledger technology (DLT) while seeking to ensure legal certainty and financial stability.

Swiss law does not define terms such as "blockchain," "cryptocurrency," or "virtual currency," but there are legal definitions and categorizations of several aspects of the blockchain technology. FINMA's 2018 Guidelines on Initial Coin Offerings (ICOs)[2646] introduced a widely used categorization of tokens into three non-exclusive groups:[2647] payment tokens, utility tokens, and asset tokens. While this taxonomy is not itself statutory, it has become a cornerstone of Switzerland's regulatory treatment of crypto assets.[2648]

2640 Rajah & Tann Asia, *New Regulated Activities under Payment Services Act and New User Protection Requirements for Digital Payment Token Service Providers from 4 April 2024* (Apr. 2024), https://www.rajahtannasia.com/wp-content/uploads/2024/05/2024-04-_New-Regulated-Activities2.pdf; Duane Morris LLP, *Singapore Amends Payment Services Act* (Jan. 27, 2021), https://www.duanemorris.com/alerts/singapore_amends_payment_services_act_0121.html.

2641 Allen & Gledhill, *MAS Expands Scope of Regulated Payment Services, Amends Ongoing Compliance Requirements, and Introduces User Protection and Financial Stability-Related Requirements for DPT Service Providers Under Payment Services Act 2019* (Apr. 18, 2024), https://www.allenandgledhill.com/sg/publication/articles/27857/mas-expands-scope-of-regulated-payment-services-amends-ongoing-compliance-requirements-and-introduces-user-protection-requirements-for-dpt-service-providers-under-payment-services-act-2019.

2642 Wayston Compliance Solutions *AML/CFT Requirements for Payment Service Firms*, https://compliance.waystone.com/aml-cft-requirements-for-payment-service-firms/ (last visited Jan. 15, 2026).

2643 Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock, Switzerland, in *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2025* 458, 458 et seq. (Global Legal Group 2024), https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/switzerland/.

2644 Steuerverwaltung des Kantons Zug, *Steuern bezahlen mit Kryptowährungen* (*Paying Taxes With Cryptocurrencies*), https://zg.ch/de/steuern-finanzen/steuern/steuerbezug/steuern-bezahlen-mit-kryptowaehrungen (last visited Jan. 15, 2026); Canton of Zug, *The Cantonal Government Supports Blockchain Research in the Canton of Zug* (July 6, 2022), https://zg.ch/dam/jcr:b498ba31-36f8-4f25-a7c1476da8a2263c/20220706_The%20cantonal%20government%20supports%20blockchain%20research%20in%20the%20Canton%20of%20Zug.pdf.

2645City of Lugano & Tether, *Lugano's Plan ₿*, https://planb.lugano.ch/ (last visited Jan. 15, 2026).

2646 Elliptic, *Switzerland Country Guide* (Nov. 6, 2022), https://www.elliptic.co/country-guides/switzerland; David Gardos, *Swiss Regulators Set Precedent with Groundbreaking ICO Guidelines* (Feb. 27, 2018), https://cassels.com/insights/swiss-regulators-set-precedent-with-groundbreaking-ico-guidelines/; Swiss Financial Market Supervisory Authority (FINMA), *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs)* (Feb. 16, 2018), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf.

2647 FINMA, *supra* note 2646.

2648 Patrick Schärli, § 9 *Finanzmarktrechtliche Kategorisierung von Kryptowerten,* in *Kryptowerte* no. 9.04 et seq. (Corinne Zellweger Gutknecht, Dominik Tschudi & Kevin MacCabe eds., Helbing Lichtenhahn 2024), https://www.helbing.ch/de/detail/ISBN-9783719047443/Kryptowerte.

FINMA explicitly recognizes that tokens may combine features of multiple categories, giving rise to hybrid tokens.

1. Offering and sale of crypto assets

The offering and sale of crypto assets is not necessarily subject to Swiss financial market regulations.[2649] However, tokens may fall under securities regulations if they qualify as securities under Swiss law (i.e., standardized, mass-tradable instruments, such as certificated or uncertificated securities, derivatives, or intermediated securities).[2650] There is no statutory guidance or case law defining when tokens qualify as securities, but the FINMA ICO Guidelines provide some degree of legal certainty.

Thus, while token classification requires a case-by-case analysis, in general, FINMA distinguishes between different types of tokens and assesses whether they are securities based on their characteristics and functions:

- **Payment tokens,** such as Bitcoin or Ether, are not treated as securities. The rationale is that payment tokens do not grant holders any rights against an issuer or third party; they primarily serve as a medium of exchange and a potential store of value. Similarly, under the Financial Services Act (FinSA), payment tokens are generally not considered financial instruments.[2651]
- **Utility tokens** are not classified as securities if their sole purpose is to provide digital access to a service or application and if this utility is already usable when the tokens are issued. However, utility tokens that have an investment or capital market connection may additionally represent characteristics of an asset token (see below), thereby coming into securities law scrutiny.[2652]
- **Asset tokens** may be regarded as securities. This includes tokens representing uncertificated securities or derivatives that are standardized and suitable for mass trading. For instance, tokens that create future purchase claims in pre-financing scenarios could be treated as securities.[2653]
- **Stablecoins** may qualify as securities, depending on their structure. If a stablecoin is linked to underlying assets (such as commodities or securities) and grants holders contractual claims (redemption rights), it can be classified as a derivative or security under Swiss law.[2654] If a stablecoin merely evidences an ownership right of the token holder, it generally does not qualify as a security. The key factor distinguishing stablecoins is that the underlying asset link primarily aims at price stabilization, rather than serving as an investment vehicle.[2655]

Activities involving tokens that qualify as securities under Swiss law may trigger regulatory obligations under three key frameworks: the Financial Institutions Act (FinIA),[2656] the Financial Markets Infrastructures Act (FinMIA), and the Financial Services Act (FinSA).

Persons and legal entities that create or trade tokenized securities in a professional capacity on behalf of clients may be classified as securities firms and must

2649Swiss Federal Council, *Federal Council Moves Forward With Stablecoins and Crypto: Consultation Launched* (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY; Erläuternder Bericht zur Änderung des Finanzinstitutsgesetzes (FINIG) (Oct. 22, 2025), https://cms.news.admin.ch/dam/en/der-schweizerische-bundesrat/bqoaKNhbpGcb/finig-erlaeuternder-bericht-de.pdf.

2650 Federal Act on Financial Services (FinSA) *art. 3(b)* (Switz.), https://www.fedlex.admin.ch/eli/cc/1999/404/en (last visited Jan. 15, 2026)

2651 Federal Act on Financial Services (FinSA) *art. 3(a)* (Switz.), https://www.fedlex.admin.ch/eli/cc/1999/404/en; FINMA, *supra* note 2646.

2652 FINMA, *supra* note 2646, at no. 3.2.2.

2653 FINMA, *supra* note 2646, at no. 3.2.3.

2654 Swiss Financial Market Supervisory Authority (FINMA), *Supplement to the Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs): "Stable Coins"*, at 2.2 (Sept. 11, 2019), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf.

2655 *Id.* at 2.2.2.

2656 Federal Act on Financial Institutions (FinIA) SR 954.1, https://www.fedlex.admin.ch/eli/cc/2018/801/en (last visited Jan. 15, 2026).

obtain a FinIA license. If such tokens also qualify as financial instruments, additional obligations under FinSA may apply (particularly if the entity qualifies as a financial service provider).[2657] For instance, issuing asset tokens linked to a company's or project's performance may constitute a regulated activity and trigger the prospectus requirements under the FinSA.[2658] However, if these activities are conducted on a purely cross-border basis (without personnel or a branch in Switzerland), a FinIA license is, in general, not required. However, FinSA can still apply if financial services are provided to clients in Switzerland.[2659]

Operating a trading platform for tokens in Switzerland may also trigger licensing obligations under FinMIA. Only licensed banks, securities firms, or recognized foreign trading venues may operate what Swiss law defines as "organized trading facilities" (OTFs).[2660] These include platforms enabling multilateral or bilateral trading of securities or other financial instruments, following rules that may be discretionary.[2661] Even if the tokens traded are not classified as securities, a platform may still fall within the definition of an OTF if the tokens are considered other financial instruments under the FinSA.[2662]

2. Anti-money laundering regulations

The issuance and trading of payment tokens in Switzerland may fall under anti-money laundering (AML) regulations, depending on whether the activity qualifies as financial intermediation under the Anti-Money Laundering Act (AMLA).[2663]

Swiss law distinguishes between two types of financial intermediaries. The first are entities in the banking sector (such as banks, insurance institutions, and securities firms) which are subject to a comprehensive prudential regulation.[2664] The second group includes non-banking intermediaries, such as individuals or companies that professionally accept or manage third-party assets, assist in investments, or help transfer such assets.[2665] Anyone engaging in such activity must join a Swiss self-regulatory organization (SRO)[2666] and comply with standard AML duties, including verifying customer and business identity and identifying beneficial owners.[2667]

When it comes to tokens, AML obligations depend on the context. According to FINMA, issuing payment tokens or stablecoins qualifies as financial intermediation, since it involves creating a means of payment.[2668] The

2657 Haeberli et al., *supra* note 2643.

2658 Federal Act on Financial Services (FinSA) arts. 35–57 (Switz.).

2659 Haeberli et al., *supra* note 2643, at 464.

2660 Claude Humbel, *Organisierte Handelssysteme in der Schweiz – Quo vadis? Handlungsspielräume de lege lata und Gestaltungsoptionen de lege ferenda im Lichte aktueller Entwicklungen*, GesKR – *Schweizerische Zeitschrift für Gesellschafts- und Kapitalmarktrecht sowie Umstrukturierungen* 2021/1, 25, 25 et seq., https://www.zora.uzh.ch/bitstreams/166e7d08-16d6-4a34-bed9-e9150a888bc4/download

2661 Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) art. 42 (Switz.).

2662 Haeberli et al., *supra* note 2643, at 464.

2663 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA) of Oct. 10, 1997, SR 955.0 (Switz.), https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de.

2664 Art. 2 para. 2 of the Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0 (Switz.), defines additional categories of financial intermediaries to which AMLA applies; the proposed "payment instrument institutions" and "crypto institutions" would fall in this category; on the proposed law currently under public consultation, see Swiss Federal Council, *Federal Council Moves Forward with Stablecoins and Crypto: Consultation Launched*, Press Release, Bern (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY, and Eidgenössisches Finanzdepartement, *Erläuternder Bericht: Neue Regulierung – Schweiz als Standort für Stablecoins und Kryptos* (Oct. 2025), https://cms.news.admin.ch/dam/en/der-schweizerische-bundesrat/bqoaKNhbpGcb/finig-erlaeuternder-bericht-de.pdf.

2665 Art. 2 para. 3 of the Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0 (Switz.), https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de.

2666Art. 14 para. 1 AMLA, SR 955.0 (Switz.).

2667Art. 3 et seqq.

2668 Swiss Financial Market Supervisory Authority (FINMA), Guidance 06/2024: Stablecoins – Risks and Challenges for Issuers of Stablecoins and Banks Providing Guarantees, at no. 3 (July 26, 2024), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20240726-finma-aufsichtsmitteilung-06-2024.pdf?hash=03D675C1247EAFAE0C391&sc_lang=en&utm_source.

simple sale of payment tokens or using them to buy goods or services does not, on its own, trigger AMLA requirements.[2669] However, under the (revised) Swiss Anti-Money Laundering Ordinance,[2670] services that facilitate the transfer of virtual currencies may be subject to AMLA if offered within the scope of a permanent business relationship (*dauernde Geschäftsbeziehung*).[2671]

3. Stablecoins

FINMA addressed stablecoins in a 2019 supplement to its ICO Guidelines (FINMA Supplement)[2672] and later issued Guidance in July 2024, setting out regulatory expectations and risk considerations for stablecoin issuers and related financial institutions.[2673] When it comes to stablecoins, FINMA does not issue a blanket rule on whether financial market licenses are necessary.[2674] Instead, the classification and licensing requirements for stablecoins depend heavily on their specific characteristics. FINMA applies three key principles in its assessment:

- **"substance over form,"** meaning the economic reality matters more than the label;
- **"same risks, same rules,"** ensuring similar risks are regulated consistently; and
- **a "case-by-case analysis"** that carefully examines the unique features of each stablecoin.[2675]

Depending on the specific features of the stablecoin, a banking license under the Banking Act or a license under the Collective Investment Schemes Act (CISA)[2676] may be required.

In order to distinguish between a collective investment scheme and a deposit under banking law, it is essential to determine whether the underlying assets are managed for the account and at the risk of:

- the stablecoin holder (which is indicative of a collective investment scheme) or
- the issuer (which is indicative of a deposit under banking law).[2677]

The latter implies that, since (currently) there are no dedicated regulations for stablecoins in Switzerland, each stablecoin must be evaluated individually. Important factors include whether the stablecoin is backed by a single asset or a basket of assets; what type of assets is backing it; and, whether the stablecoin gives holders a contractual right to redeem it against those underlying assets or simply represents an ownership claim.[2678] For example, if a stablecoin is pegged to fiat currency on a

2669 FINMA ICO Guidelines, *supra* note 2646, at 3.6 et seq.

2670 Ordinance on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance, AMLO) of November 11, 2015 SR 955.01, https://www.fedlex.admin.ch/eli/cc/2015/791/en?utm_source.

2671 *Id.* Art. 4 para. 1 lit. b; FINMA ICO Guidelines, *supra* note 2646, at 3.7.

2672 FINMA, Supplement, *supra* note2654.

2673 FINMA Guidance 2024, *supra* note 2668.

2674 See Bundesgesetz über die Banken und Sparkassen (Bankengesetz, BankG) [Federal Act on Banks and Savings Institutions (Banking Act)] of Nov. 8, 1934, SR 952.0, art. 1b (Switz.); Swiss Federal Council, *Federal Council Moves Forward with Stablecoins and Crypto: Consultation Launched*, Press Release (Bern, Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY; Eidgenössisches Finanzdepartement, *Erläuternder Bericht:* Neue Regulierung – Schweiz als Standort für Stablecoins und Kryptos (Oct. 22, 2025), https://www.sif.admin.ch/dam/de/sd-web/dUviLBIEgTjT/finig-erlaeuternder-bericht-de.pdf.

2675 On these principles, see FINMA Supplement, *supra* note 2654, at 2.1.

2676 Federal Act on Collective Investment Schemes (Collective Investment Schemes Act, CISA) of June 23, 2006 (SR 951.31).

2677 In its proposal currently in a public consultation procedure, the Swiss Federal Council proposes the introduction of a license for "payment instrument institutions" that is tailor-made for stablecoin issuers and that would replace the current fintech license under article 1b of the Federal Act on Banks and Savings Institutions (Bundesgesetz über die Banken und Sparkassen, Bankengesetz, BankG) of 8 November 1934 (SR 952.0). See Bundesgesetz über die Banken und Sparkassen [Bankengesetz, BankG] [Federal Act on Banks and Savings Institutions] of Nov. 8, 1934, SR 952.0 (Switz.); Federal Council, Federal Council Moves Forward with Stablecoins and Crypto: Consultation Launched (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY; Eidgenössisches Finanzdepartement, Neuer Regulierungsrahmen: Schweiz als Standort für Stablecoins und Kryptos – Erläuternder Bericht 1 ff. (Oct. 21, 2025), https://cms.news.admin.ch/dam/en/der-schweizerische-bundesrat/bqoaKNhbpGcb/finig-erlaeuternder-bericht-de.pdf; FINMA Supplement, *supra* note 2654, at 2.2.1.

2678 FINMA Supplement, *supra* note 2654, at 2.2.

fixed ratio (e.g., 1 token equals 1 Swiss franc) or backed by precious metals held by banks that provide holders with a redemption claim, then issuing such a stablecoin may require a banking license.[2679] If a stablecoin is linked to currencies, securities, or commodities in a way that provides holders with a redemption claim and the underlying assets are managed on behalf of token holders, FINMA may treat the stablecoin as a collective investment scheme under the CISA.[2680] This means the token holders bear the risks of the underlying asset management (such as fluctuations in asset value, interest rate changes, or counterparty risks).

The Swiss approach —particularly in relation to reserve backing, redemption rights, and AML obligations— has been viewed by some market participants as relatively restrictive and as having limited large-scale stablecoin issuance in Switzerland. In response to these concerns, the Swiss Federal Council launched a public consultation on October 22, 2025,[2681] proposing targeted reforms to financial market legislation. Among those proposed reforms were new licensing categories for payment instrument institutions and crypto-institutions, and a refined regulatory framework for certain stablecoin models aimed at balancing innovation with financial integrity.

4. Central bank digital currency

Payment tokens are not legal tender under Swiss law.[2682] However, some legal practitioners argue that, if payment tokens become widely used, accepted by the public, and able to fulfill the typical functions of money, they might qualify as "money," in a broader sense.[2683]

The Swiss National Bank (SNB) has acknowledged the potential of digital tokens but has not issued a retail or wholesale state-backed digital currency.[2684] However, it has been actively involved in experimental projects exploring the use of wholesale Central Bank Digital Currency (CBDC) for interbank settlement. Since 2019, the SNB has collaborated with the Bank for International Settlements (BIS) Innovation Hub, notably through Project Helvetia,[2685] which tested the settlement of tokenized assets using wholesale CBDC and demonstrated technical feasibility in a distributed ledger technology-based environment.[2686] Additional cross-border initiatives include Project Jura,[2687] conducted jointly with the Banque de France and the BIS Innovation Hub, which explored wholesale CBDCs for cross-border payments, and Project Mariana, launched in 2022 with central banks from Switzerland, the euro area, and Singapore, focusing on foreign-exchange settlement using automated market makers and wholesale CBDCs.

2679 FINMA Supplement, *supra* note 2654, at 2.2.1.

2680 FINMA Supplement, *supra* note 2654, at 2.2.3 (discussing stablecoins linked to real estate).

2681 See Swiss Federal Council, *Federal Council Moves Forward with Stablecoins and Crypto: Consultation Launched*, Press Release, Bern (Oct. 22, 2025), https://www.news.admin.ch/en/newnsb/x4TMWQ1SWofNoFx7XyHhY.

2682 Federal Act on Currency and Payment Instruments (Bundesgesetz über die Währung und die Zahlungsmittel [WZG]) of Dec. 22, 1999 SR 941.10, https://www.fedlex.admin.ch/eli/cc/2000/186/en.

2683 Lukas Müller, Milena Reutlinger & Philippe J.A. Kaiser, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, 20 EuZ - Zeitschrift für Europarecht 80, 80 (2018) https://www.alexandria.unisg.ch/entities/publication/6caaba44-d662-40c6-b357-a395159032ea.

2684 Thomas Jordan, *Towards the Future Monetary System* (speech, Swiss National Bank event "Towards the Future Monetary System," Zurich, Apr. 8, 2024), https://www.snb.ch/en/publications/communication/speeches/2024/ref_20240408_tjn.

2685 See Swiss National Bank, *Project Helvetia*, https://www.snb.ch/en/the-snb/mandates-goals/payment-transactions/projekt_helvetia.

2686 See Swiss National Bank, *Multilateral Cooperation*, https://www.snb.ch/en/the-snb/mandates-goals/international-cooperations/multilateral .

2687 See Bank for International Settlements & Swiss National Bank, *Project Jura* (Dec. 2021), https://www.snb.ch/dam/jcr:66a4914a-7f31-461b-91da-15a0c16b3341/project_jura_report.en.pdf.

APPENDIX 21 - INDIA

by Sushmita Som

With an estimated 107 million crypto users and market valuation of approximately USD 6.4 billion, India has the largest retail base of cryptocurrency users in any jurisdiction.[2688] Still, it is notable less for its approach to crypto-asset regulation than for the scale of its state-led blockchain deployment. India has pursued what appears to be a deliberate two-track approach: containing speculative crypto activity through fiscal disincentives and anti-money laundering enforcement, while developing one of the largest national blockchain deployment programs for public administration currently in operation.

1. Crypto-asset regulation in India: from prohibition to taxation

India's regulatory posture is characterized by fiscal disincentive which followed after a phase of attempts to ban cryptocurrency. In April 2018, the central bank Reserve Bank of India (RBI) issued a circular barring all RBI-regulated entities, including banks, payment system providers, and non-banking financial companies, from providing any financial services in relation to cryptocurrency.[2689] The effect was immediate: virtual digital asset ("VDA") service providers lost access to the banking system, rendering fiat deposits, withdrawals, and fiat-to-crypto conversion effectively impossible. The prohibition was challenged by industry stakeholders and, in 2020, the Supreme Court of India set it aside in *Internet and Mobile Association of India v Reserve Bank of India*[2690] on the grounds that it was disproportionate and violated citizens' fundamental rights. The judgment did not, however, prevent the government from legislating a ban.

The government came close to doing so. In 2019, an Inter-Ministerial Committee proposed the Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, which would have prohibited the mining, holding, selling, and use of cryptocurrency in India.[2691] This was followed in 2021 by the Cryptocurrency and Regulation of Official Digital Currency Bill, listed for introduction in the lower house of Parliament, which sought to prohibit all private cryptocurrencies while creating a framework for a state-issued digital currency.[2692] Neither bill was ever formally introduced before Parliament, and both lapsed without enactment.

Following the Supreme Court judgment, the RBI reportedly pursued an informal approach, with reports emerging from 2022 of the RBI instructing banks to exercise caution when facilitating VDA transactions, a practice referred to in the industry as a "shadow ban."[2693] Coinbase cited this dynamic in a 2022 earnings call before withdrawing from the Indian market.[2694] Other exchanges adapted by pivoting to peer-to-peer transaction models

2688 ICR Research Team, *Crypto Adoption & Blockchain Outlook in India*, India Crypto Res. (May 26, 2025), https://indiacryptoresearch.co.in/learn/blogs/crypto-adoption-blockchain-outlook-in-india. India has ranked first in the Chainalysis Global Crypto Adoption Index for two consecutive years, leading across both on-chain value and retail transaction value on centralised platforms when weighted by GDP per capita on a purchasing power parity (PPP) adjusted basis. Chainalysis, *The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption*, Chainalysis Blog (Sept. 2, 2025), https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/.

2689 Reserve Bank of India, RBI/2017-18/154, DBR.No.BP.BC.104 /08.13.102/2017-18, *Prohibition on Dealing in Virtual Currencies (VCs)* (Apr. 6, 2018), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2632.

2690 *Internet and Mobile Association of India v Reserve Bank of India (2020 SCC Online SC 275).*

2691 Inter-Ministerial Committee on Virtual Currencies, Ministry of Finance (India), *Report of the Committee to Propose Specific Actions to Be Taken in Relation to Virtual Currencies* (July 22, 2019), https://prsindia.org/files/bills_acts/bills_parliament/1970/Report%20of%20the%20Inter-Ministerial%20Committee%20on%20Virtual%20Currencies.pdf.

2692 Lok Sabha Bulletin, Part II, No. 3547, at entry 12 (Jan. 29, 2021) (listing the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 for introduction), https://prsindia.org/files/parliament/session_track/2021/session_alert/Parliament_Session%20Alert_Winter%20Session%202021.pdf.

2693 Probir Roy Chowdhury & Nikhil George, *Blockchain 2025 — India: Trends and Developments,* Chambers Global Practice Guides (June 12, 2025), https://practiceguides.chambers.com/practice-guides/blockchain-2025/india.

2694 Amitoj Singh, *The Curious Case of Coinbase's India Communications Strategy*, CoinDesk (May 27, 2022), https://www.coindesk.com/policy/2022/05/27/the-curious-case-of-coinbases-india-communications-strategy

that reduced bank visibility into VDA-related flows.[2695]

The current framework emerged from this context. In 2022, the government began taxing VDA income, a step widely interpreted as signaling that an outright ban was no longer the policy direction. Under the Finance Act 2022, India introduced a flat 30% tax on VDA profits, with no deductions permitted for trading expenses or transaction fees and no ability to offset or carry forward losses, significantly higher than the 10–15% rate applicable to gains on equities and other capital assets. An 18% goods and services tax applies to crypto-related services.[2696]

In March 2023, India's anti money laundering legislation, the Prevention of Money Laundering Act (PMLA), was amended to encompass VDA service providers, imposing Know Your Customer (KYC) and anti-money laundering (AML) obligations on crypto exchanges and custodians and bringing them within the supervisory remit of the Financial Intelligence Unit - India (FIU-IND).[2697] Notably, the FIU-IND is an agency under the central government rather than its securities regulator SEBI. FIU-IND has adopted an activity-based enforcement approach, focused on functions such as on/off-ramping, custody, and token transfers, rather than on the structural form of a platform.[2698] In December 2023, FIU-IND issued show-cause notices to nine major offshore exchanges, including Binance, KuCoin, Kraken, and Bitfinex, for operating without PMLA registration, resulting in the blocking of their URLs for Indian users.[2699]

The government has consistently stated that crypto assets will not be recognized as legal tender and that monetary sovereignty takes precedence over sector development.[2700] The Ministry of Finance's discussion paper on comprehensive VDA regulation, originally expected in late 2024,[2701] has not been released as of early 2026. The Securities and Exchange Board of India (SEBI)'s reported proposal for a multi-regulator oversight framework remains unimplemented.[2702] In January 2025, the Delhi High Court directed the RBI, SEBI, and the Ministry of Finance to respond to a user petition on VDA regulation; the RBI informed the Court it would not

---

2695 PRS Legislative Research, *Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019*, PRS LEGIS. RSCH., https://prsindia.org/billtrack/draft-banning-of-cryptocurrency-regulation-of-official-digital-currency-bill-2019 (last visited Jan. 15, 2026).

2696 Finance Act, 2022, No. 6 of 2022, § 115BBH (India) (inserting § 115BBH into the Income Tax Act, 1961 imposing a 30% tax on income from transfer of virtual digital assets, permitting only cost of acquisition as a deduction, and disallowing set-off or carry-forward of VDA losses); *id.* § 194S (imposing 1% TDS on transfers of VDAs above prescribed thresholds, effective July 1, 2022). Gazette of India, Extraordinary, Part II, Section 1, No. 6 of 2022), https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf. *But see* Lakshmikumaran & Sridharan Attorneys, *Supreme Court of India Lifts the Ban on Cryptocurrency*, LEXOLOGY (Mar. 10, 2020), https://www.lexology.com/library/detail.aspx?g=8fba60f0-1a38-4bd3-af58-8578bb070018 ("Despite the opinion that a tax-rate as high as 30% on crypto-investments is likely to disincentivise young investors and crypto-enthusiasts in the Indian market, India fares on a reasonable scale compared to countries like Australia, USA and Canada where, tax on crypto-currencies fall within a range of 37%-50%.")

2697 Ministry of Finance, Dep't of Revenue (India), Notification Nos. S.O. 1072(E) and S.O. 1074(E), Gazette of India, Extraordinary, Part II, Section 3(ii) (Mar. 7, 2023) (extending the Prevention of Money Laundering Act, 2002 to virtual digital asset service providers and amending the PML (Maintenance of Records) Rules, 2005 to impose KYC and AML obligations).

2698 Financial Intelligence Unit — India (FIU-IND), *AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets* (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf.

2699 Press Release, Financial Intelligence Unit — India, *FIU IND Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs)* (Dec. 28, 2023), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372. In June 2024, a formal order was issued against Binance imposing fines of approximately USD 2.25 million, Financial Intelligence Unit — India, Order in Original No. 10/DIR/FIU-IND/2024, *In the Matter of Binance* (June 19, 2024), https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf; Bybit was fined approximately USD 1.07 million for similar violations, Financial Intelligence Unit — India, Order No. 15/DIR/FIU-IND/2024, *In the Matter of Bybit Fintech Limited* (Jan. 31, 2025), https://fiuindia.gov.in/pdfs/judgements/Bybit_Order_15_2024.pdf.

2700 Nirmala Sitharaman, Union Minister of Finance (India), *Remarks at India Today Conclave 2024*, *reported in* Ankita Upadhyay, *Crypto Assets Cannot Be Legal Currencies, Says Finance Minister Nirmala Sitharaman*, INDIA TODAY (Mar. 15, 2024), https://www.indiatoday.in/business/story/india-today-conclave-2024-nirmala-sitharaman-finance-minister-7-trillion-economy-aim-consumer-spending-household-savings-2515088-2024-03-15.

2701 Minister of State for Finance Pankaj Chaudhary, Statement in Lok Sabha, Winter Session 2024 (Dec. 16, 2024) (responding to parliamentary questions on VDA regulation, confirming «there is no timeline anticipated for introduction of comprehensive regulatory guidelines for VDA industry in India»); *see also* Cyril Amarchand Mangaldas, *FIG Paper No. 41 — VDA Series 4: Global Crypto Developments: Lessons for India's Regulatory Regime in 2025* (Jan. 2025), https://corporate.cyrilamarchandblogs.com/2025/01/fig-paper-no-40-vda-series-4-global-crypto-developments-lessons-for-indias-regulatory-regime-in-2025/.

2702 Nikunj Ohri, *Exclusive: India's SEBI open to oversight of crypto trade, in contrast to RBI*, REUTERS (May 16, 2024) https://www.reuters.com/world/india/indias-sebi-open-oversight-crypto-trade-contrast-reserve-bank-2024-05-16/ (reporting on confidential documents submitted to a government advisory panel).

regulate VDA platforms.[2703] As of the date of this report, India has no comprehensive legislation governing VDAs and SEBI-regulated collective investment vehicles, including mutual funds and alternative investment funds, are prohibited from any VDA exposure.

2. The National Blockchain Framework for public infrastructure

The National Blockchain Framework (NBF), initiated in 2021 by the Ministry of Electronics and Information Technology (MeitY) and officially launched on September 4, 2024 with a budget of approximately USD 7 million, provides a unified permissioned blockchain infrastructure for government services, deployed across National Informatics Centre (NIC) data centres in a few Indian cities.[2704] The MeitY-developed Vishvasya Blockchain Stack provides Blockchain-as-a-Service (BaaS) through a geographically distributed infrastructure, which supports several operational chains:[2705]

- The Document Chain enables verifiable, tamper-resistant authentication of government-issued certificates including academic records, birth and death certificates, land titles, and ration cards; as of October 2025, over 340 million documents had been verified through the platform.
- The Logistics Chain supports end-to-end supply chain traceability, with Karnataka's *Aushada* platform as a representative deployment: a blockchain-secured system tracking the movement of medicines from manufacturer to hospital to reduce counterfeit drug exposure.
- The Judiciary Chain produces verifiable, time-stamped records for bail orders, summons, and electronic notices, with over 39,000 documents from the Interoperable Criminal Justice System validated on-chain.
- The Property Chain is directed at title integrity in India's land registration system, with state-level pilots in Telangana, Goa, and Maharashtra. By recording sale and mortgage transactions on a permissioned ledger, the Property Chain aims to produce title records that are immutable and cryptographically verifiable, reducing reliance on paper-based registration systems.

The RBI's central bank digital currency, the e-rupee (e₹), occupies a separate position within this framework. Pilot programs for both wholesale (e₹-W) and retail (e₹-R) segments have been operational since late 2022.[2706] By end-2024, the retail pilot had reached over 5 million users and 420,000 merchants, with State Bank of India, ICICI, and HDFC - the three largest commercial banks in India by market capitalization - among the participating institutions.[2707] Use cases under the pilot have included purpose-bound credit for tenant farmers without formal land titles,[2708] agricultural carbon credit generation,

2703 *Rana Handa v. Bitbns Internet Pvt. Ltd.* and *Aditya Malhotra & Ors. v. Union of India & Ors.* (Delhi H.C.), Order dated Jan. 9, 2025 (Justice Sachin Datta, J.) (issuing notice to RBI, SEBI, Ministry of Finance, and MeitY on petition seeking a regulatory framework for VDA exchanges, and fixing Apr. 4, 2025 for further hearing), *reported in* ANI (Jan. 9, 2025), https://www.aninews.in/news/national/general-news/plea-moved-in-delhi-hc-over-financial-crisis-at-bitbns-crypto-exchange-court-seeks-stand-of-respondents20250109164238/.

2704 Ministry of Electronics & Information Technology, Govt. of India, Press Release, *National Blockchain Framework: Strengthening Governance through Blockchain Technology* (Oct. 24, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2182023.

2705 *Id*.; *See also* Pradipta Mukherjee, *2024 Sees India Embracing Blockchain for Various Use Cases* (Dec. 30, 2024), https://coingeek.com/2024-sees-india-embracing-blockchain-for-various-use-cases/.

2706 Reserve Bank of India, *Concept Note on Central Bank Digital Currency* (Oct. 7, 2022), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF.

2707 Reserve Bank of India, *Report on Currency and Finance 2023–24*, at ch. IV (July 29, 2024), https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF

2708 *See* Shaktikanta Das, Governor, Reserve Bank of India, Address at the Conference on *Digital Public Infrastructure and Emerging Technologies*, Reserve Bank of India, Bengaluru (Aug. 26, 2024) (describing the State Bank of India pilot launched on August 16, 2024 in Odisha and Andhra Pradesh providing programmable CBDC credit to tenant farmers lacking land titles, noting that «programming the end use for purchase of agricultural inputs can give the required comfort to banks»), *reported in* Global Government Fintech (Sept. 3, 2024), https://www.globalgovernmentfintech.com/india-cbdc-trial-more-than-five-million-users-no-rush-for-launch/.

and direct welfare transfers under the state of Odisha's Subhadra Yojana scheme for women.[2709]

Broadly, India's trajectory illustrates both the governance potential of permissioned blockchain for large emerging economies and the difficulties inherent in maintaining a regulatory distinction between blockchain as infrastructure and blockchain as a medium for financial activity.

2709 Reserve Bank of India, *Annual Report 2024–25*, at ch. IV (2025) (noting use cases including «direct benefit transfers to farmers against carbon credits generation»), https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx.

SELECTED BIBLIOGRAPHY

SELECTED BIBLIOGRAPHY

Books

Bonomi, Andrea, Matthias Lehmann, and Shaheeza Lalani (eds), *Blockchain and Private International Law* (Leiden: Brill/Nijhoff, 2023)

De Filippi, Primavera, Wessel Reijers, and Morshed Mannan, *Blockchain Governance* (Cambridge, MA: MIT Press, 2024)

De Filippi, Primavera, and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, MA: Harvard University Press, 2018)

Dixon, Chris, *Read Write Own: Building the Next Era of the Internet* (New York: Random House, 2024)

G'sell, Florence, and Florian Martin-Bariteau, *The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law* (Strasbourg: Council of Europe, 2022)

Goldsmith, Jack, and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006)

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Lessig, Lawrence, *Code: Version 2.0* (New York: Basic Books, 2006)

Werbach, Kevin, *The Blockchain and the New Architecture of Trust* (Cambridge, MA: MIT Press, 2018)

Werbach, Kevin, Eva Micheler, and Bianca Kremer (eds), *Foundations of Decentralized Organizations: Blockchain and the Future of Corporate Law* (Oxford: Oxford University Press, forthcoming 2026)

Wu, Tim, *The Attention Merchants: The Epic Struggle to Get Inside Our Heads* (New York: Knopf, 2016)

Wu, Tim, *The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity* (New York: Knopf, 2025)

Reports and Institutional Publications

Cambridge Centre for Alternative Finance, *Cambridge Digital Mining Industry Report* (Cambridge, 2025)

De Filippi, Primavera, Sofia Cossar, Morshed Mannan, Kelsie Nabben, Tara Merk, and Jamilya Kamalova, *Report on Blockchain Governance Dynamics* (BlockchainGov / Project Liberty Institute, 2024)

De Filippi, Primavera, Morshed Mannan, Sofia Cossar, Tara Merk, and Jamilya Kamalova, *Blockchain Technology and Polycentric Governance* (European University Institute, 2024)

De Filippi, Primavera, Sofia Cossar, Morshed Mannan, Kelsie Nabben, Tara Merk, and Jamilya Kamalova, *The Blockchain Governance Toolkit: A Cookbook for a Resilient and Robust Ecosystem* (Project Liberty Institute & BlockchainGov, 2024)

Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008)

Princeton University, DeCenter, *Decentralizing Power Through Blockchains: Key Research Questions Across Disciplines* (2024)

Chapters in Edited Volumes

Cannarsa, Michel, "Contract Interpretation," in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Larry A. DiMatteo, Michel Cannarsa, and Cristina Poncibò eds, Cambridge: Cambridge University Press, 2020), 111–12

Guillaume, Florence, "Decentralized Autonomous Organizations (DAOs) Before State Courts: How Can Private International Law Keep Up with Global Digital Entities," in *Decentralized Autonomous Organisation (DAO) Regulation* (Madalena Perestrelo de Oliveira and António Garcia Rolo eds, 2024), 135

Mannan, Morshed, "Technocratic Despotism in the Network State," in *Decoding Digital Authoritarianism* (Global Affairs Canada, 2023)

Mannan, Morshed, Primavera De Filippi, and Wessel Reijers, "The Emergence of Blockchain Constitutionalism," in *The Oxford Handbook of Digital Constitutionalism* (Giovanni De Gregorio, Oreste Pollicino, and Peggy Valcke eds, Oxford: Oxford University Press, 2024)

Post, David G, "Anarchy, State, and the Internet," in *Crypto Anarchy, Cyberstates, and Pirate Utopias* (Peter Ludlow ed, Cambridge, MA: MIT Press, 2001), 207–08

Schrepel, Thibault, "Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia," in *General Principles and Digitalisation* (Giovanni De Gregorio and others eds, Oxford: Hart Publishing, 2020)

Walch, Angela, "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains," in *Regulating Blockchain: Techno-Social and Legal Challenges* (Philipp Hacker et al eds, Oxford: Oxford University Press, 2019), 58–67

Journal Articles and Academic Papers

Abramowicz, Michael, "The Very Brief History of Decentralized Blockchain Governance," *Vanderbilt Journal of Entertainment & Technology Law* 22 (2020): 273–76

Allen, Darcy W. E., Aaron M. Lane, and Marta Poblet, "The Governance of Blockchain Dispute Resolution," *Harvard Negotiation Law Review* 25 (2019): 75–104

Alston, Eric, Wilson Law, Ilia Murtazashvili, and Martin B. H. Weiss, "Blockchain Networks as Constitutional and Competitive Polycentric Orders," *Journal of Institutional Economics* 18 (2022): 707–23

Aouidef, Yann, Federico Ast, and Bruno Deffains, "Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects," *Frontiers in Blockchain* 4 (2021)

Axelsen, Henrik et al., "When Is a DAO Decentralized?" *Complex Systems Informatics and Modeling Quarterly* 31 (2022): 51–56

Buterin, Vitalik et al., "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium," *Blockchain: Research and Applications* 5 (2024)

Chan, Timothy, "The Nature of Property in Crypto-Assets," *Legal Studies* 43 (2023): 480–99

De Filippi, Primavera, and Samer Hassan, "Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code," *First Monday* 21 (2016)

De Filippi, Primavera, and Benjamin Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure," *Internet Policy Review* 5 (2016)

De Filippi, Primavera, Chris Wray, and Giovanni Sileno, "Smart Contracts," *Internet Policy Review* 10 (2021): 1–3

De Filippi, Primavera, Morshed Mannan, and Wessel Reijers, "The Alegality of Blockchain Technology," *Policy & Society* 41 (2022): 358–69

De Filippi, Primavera, Morshed Mannan, and Wessel Reijers, "Blockchain Technology and the Rule of Code: Regulation via Governance," *George Washington Law Review* 92 (2024): 1229–1300

De Filippi, Primavera et al., "Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance," *Technology in Society* 62 (2020): 101284

Finck, Michèle, "Blockchains: Regulating the Unknown," *German Law Journal* 19 (2018): 665–92

Fritsch, Robin, Marino Müller, and Roger Wattenhofer, "Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?" *Blockchain: Research and Applications* 5 (2024)

Genc, Huseyin Oguz, and Eray Acikgoz, "Constructing an Evaluation Framework for Full Decentralization," *Stanford Journal of Blockchain Law & Policy* 8 (2025): 177–80

Hassan, Samer, and Primavera De Filippi, "Decentralized Autonomous Organization," *Internet Policy Review* 10 (2021): 1–2

Jain, Shrey et al., "AI and Democracy's Digital Identity Crisis," *Stanford Journal of Blockchain Law & Policy* 7 (2024): 56–75

Johnson, David R., and David G. Post, "Law and Borders—The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367–1402

Kaal, Wulf A., "Blockchain-Based Corporate Governance," *Stanford Journal of Blockchain Law & Policy* 4 (2021): 3–27

Langvardt, Kyle, "Crypto's First Amendment Hustle," *Yale Journal of Law & Technology* 26 (2024): 130–78

Lehmann, Matthias, "Digital Assets in the Conflict of Laws: A Comparative Search for the 'Ideal Rule'," *Singapore Journal of Legal Studies* (2024): 197–220

Nabben, Kelsie, and Primavera De Filippi, "Accountability Protocols? On-Chain Dynamics in Blockchain Governance," *Internet Policy Review* 13 (2024)

Reijers, Wessel et al., "Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies," *Topoi* 40 (2021): 821

Reyes, Carla L., "Creating Cryptolaw for the Uniform Commercial Code," *Washington and Lee Law Review* 78 (2021): 1521–41

Reyes, Carla L., "Emerging Technology's Language Wars: Cryptocurrency," *William & Mary Law Review* 64 (2023): 1193–98

Rizal, Syamsul, and Dong-Seong Kim, "Enhancing Blockchain Consensus Mechanisms," *Blockchain: Research and Applications* 6 (2025)

Schmitz, Amy J., "Resolving NFT and Blockchain Disputes," *Stanford Journal of Blockchain Law & Policy* 6 (2023): 156–210

Strnad, Jeff, "Delegation and Participation in Decentralized Governance: An Epistemic View" ArXiv abs/2505.04136 (2025)

Strnad, Jeff, "Economic DAO Governance: A Contestable Control Approach" ArXiv abs/2403.16980 (2024)

Weidener, Lukas et al., "Delegated Voting in Decentralized Autonomous Organizations," *Frontiers in Blockchain* 8 (2025)

Werbach, Kevin, Primavera de Filippi, Joshua Tan & Gina Pieters, "Blockchain Governance in the Wild," 3 *Cryptoeconomic Systems* no. 1 (2024)

Wright, Aaron, "The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges," *Stanford Journal of Blockchain Law & Policy* 4 (2021): 1–34

Yeung, Karen, "Algorithmic Regulation: A Critical Interrogation," *Regulation & Governance* 12 (2018): 505–509

Yeung, Karen, "Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code of Law and Code as Law," *Modern Law Review* 82 (2019): 207–40

Zafar, Ammar, "Reconciling Blockchain Technology and Data Protection Laws," *Journal of Cybersecurity* 11 (2025)

LIST OF FIGURES

LIST OF FIGURES

Figure	Title
Figure 1	The Bitcoin white paper
Figure 2	Diagram of a blockchain
Figure 3	Attributes of blockchains
Figure 4	Example of hash algorithm functionality
Figure 5	Simplified architecture of a Bitcoin block
Figure 6	Chain of blocks
Figure 7	Bitcoin's monetary policy
Figure 8	Linear relationship among blocks
Figure 9	Orphaned blocks
Figure 10	A chain fork
Figure 11	The DAO fork (2016)
Figure 12	Market share (%) of 10 leading cryptocurrencies
Figure 13	Coins versus tokens
Figure 14	USD Coin (USDC)
Figure 15	NFTs as digital identifiers
Figure 16	Automating royalty payment with NFTs
Figure 17	Privacy, Pseudonymity, and Anonymity
Figure 18	The Bank Robbery
Figure 19	CoinJoin: a standalone privacy protocol
Figure 20	Practical value of Zero-Knowledge Proof for privacy
Figure 21	Double-spending attacks
Figure 22	Layer 1 and Layer 2 solutions
Figure 23	Protocol change terminology
Figure 24	The SegWit Saga
Figure 25	The problem of plutarchy
Figure 26	Compound's proxy-voting implementation
Figure 27	The Terra collapse (2022)
Figure 28	Uniswap

Figure	Title
Figure 29	Curve
Figure 30	The Steem governance takeover
Figure 31	Solend
Figure 32	Rage-quit mechanisms
Figure 33	MakerDAO's on-chain governance system
Figure 34	The Kleros Court
Figure 35	The Tether (USDT) controversy
Figure 36	SpiceDAO
Figure 37	Yuga Labs v. Ripps (2025)
Figure 38	Silk Road (2013)
Figure 39	Blender (2022)
Figure 40	Ransomware-as-a-service
Figure 41	BitConnect (2018)
Figure 42	Poly Network (2021)
Figure 43	The Mango Markets price manipulation (2022)
Figure 44	Munchables (2024)
Figure 45	Mt. Gox (2014)
Figure 46	United States v Gratkowski
Figure 47	The Platypus exploit (2023)
Figure 48	The Tulip Trading Limited claim
Figure 49	The Uniswap class action
Figure 50	From bZx DAO to Ooki DAO
Figure 51	The typology of smart contracts by the U.K. Law Commission
Figure 52	Williams v Binance (2024)
Figure 53	SEC v Schueler (aka Heart) (2025)
Figure 54	FinCEN enforcement actions
Figure 55	Applying the Howey Test to Crypto
Figure 56	Rule of code and rule by code

MAY 2026

Stanford
University