

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 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 that blockchain is increasingly used 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. Pseudonymity may prove insufficient to prevent large-scale deanonymization. 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 *Tulip Trading* appellate decision 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.