Scilight

Journal of Emerging Technologies with Industrial Applications
https://www.sciltp.com/journals/jetia

Review

Check for updates

Blockchain for Next-Generation Digital Platforms: A Systematic Review of Decentralized Trust, Interoperability, and Governance

Yang Lu

Faculty of Business & Accounting, Kuala Lumpur University of Science and Technology, Kajang 43000, Malaysia; ziiyuu@gmail.com

How To Cite: Lu, Y. Blockchain for Next-Generation Digital Platforms: A Systematic Review of Decentralized Trust, Interoperability, and Governance. *Journal of Emerging Technologies with Industrial Applications* **2026**, *1*(1), 6. https://doi.org/10.53941/jetia.2026.100006

Received: 12 May 2026
Revised: 23 July 2026
Accepted: 14 September 2026
Published: 21 September 2026

Abstract: Blockchain technology is expanding beyond cryptocurrency into broader digital platform infrastructure. Existing scholarship remains highly fragmented: trust, interoperability, and governance occupy separate disciplinary traditions, with little integrative analysis across dimensions. This paper systematically reviews blockchain research in these three areas, identifies core findings, theoretical disagreements, and knowledge gaps, and proposes an integrative analytical framework for blockchain applications in next-generation digital platforms. Following PRISMA guidelines, we searched six academic databases and included 137 peer-reviewed studies after screening. In the trust dimension, blockchain relocates the basis of trust from credible institutions to verifiable protocols, yet it does not eliminate the need for trust itself. Algorithmic trust and institutional trust are complementary rather than substitutable. In the interoperability dimension, cross-chain solutions have diversified considerably, but governance arrangements lag substantially behind technical progress, and standardization trajectories differ systematically between Europe and the United States. In the governance dimension, on-chain governance practices such as DAOs expose structural contradictions between participation failure and power concentration. Effective governance requires co-designing on-chain mechanisms with off-chain norms. All three dimensions are mutually dependent in practice. Blockchain platform success depends on their coordinated configuration rather than the optimization of any single dimension. This paper proposes five priority research directions: multi-level trust modeling, interoperability governance, comparative institutional analysis, hybrid platform architecture, and cross-study measurement framework development. Governance arrangements must also address mounting regulatory compliance requirements, including securities regulation, data protection, and anti-money laundering obligations, which vary substantially across jurisdictions. The emergence of re-intermediation—where influential validators, platform operators, and consortium coordinators assume coordination roles—poses fundamental questions about the substantive decentralization of blockchain governance.

Keywords: Blockchain; digital platforms; decentralized trust; cross-chain interoperability; blockchain governance; systematic literature review

1. Introduction

Digital platforms have become core infrastructure for the modern economy. The rapid expansion of e-commerce, ride-sharing, social media, and financial technology has allowed platform organizations to reshape competitive dynamics across multiple industries within little more than a decade. As platform operators accumulate network effects, they also gain unilateral control over data, rules, and user access. This concentration has fueled ongoing debates about trust, fairness, and monopolistic power [1,2]. Blockchain technology offers a technical response to these tensions. Through cryptography and distributed consensus, blockchain redistributes the verification and rule-enforcement functions previously centralized in platform operators to a decentralized protocol layer [3]. This property has positioned blockchain as a candidate infrastructure for next-generation digital platforms, providing a foundation for trusted collaboration among multiple parties without relying on a single trusted intermediary [4,5].

Academic output on blockchain has grown exponentially over the past decade. Much of this research proceeds in isolation. Studies focused on technical security rarely engage with governance questions; research on governance mechanisms seldom examines interoperability constraints; and trust scholarship tends to pursue either an institutional or a technical perspective without synthesis [6,7]. This fragmentation impedes the accumulation of findings and sustains a persistent gap in cross-disciplinary understanding. The present paper argues that fragmentation itself is a research problem deserving attention. Trust, interoperability, and governance are not independent technical or managerial issues. They constitute three mutually dependent dimensions of blockchain platform viability. A platform with robust trust mechanisms but no interoperability faces severe scaling constraints. A platform that is technically open but lacks governance faces ongoing security and compliance risks. A platform with mature governance but no credible technical foundation cannot fulfill its governance commitments [8–10]. Against this background, three core research questions are addressed. First, what are the key findings in blockchain research on trust, interoperability, and governance? Second, how do these three dimensions relate to one another? Third, where do significant knowledge gaps remain?

This paper follows a systematic literature review methodology in accordance with PRISMA guidelines. Systematic searches were conducted across WOS and five additional databases, focusing on the intersection of blockchain and digital platforms with trust, interoperability, and governance as primary thematic terms. The search covers 2015 to 2026. After title-abstract screening and full-text assessment, 137 peer-reviewed studies meeting quality standards were included. The paper proceeds as follows. Section 2 describes the literature search and selection methodology. Section 3 presents descriptive bibliometric characteristics of the corpus. Sections 4 through 6 systematically review decentralized trust, interoperability, and governance mechanisms, respectively. Section 7 identifies future research directions. Section 8 provides conclusions.

2. Methodology and Study Selection

This review adopts a structured research design integrating three analytical components: systematic literature identification, descriptive bibliometric analysis, and qualitative thematic synthesis. The aim is to construct an analytically rigorous corpus for examining decentralized trust, interoperability, and governance mechanisms in next-generation digital platforms.

2.1. Literature Search

Systematic searches were conducted across six databases: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink, supplemented by citation tracking, yielding 1878 initial records. The Ethereum mainnet launch in July 2015 anchors the start of the search period. The temporal scope spans January 2015 to April 2026.

As shown in Table 1, the search string comprises three mandatory modules. Module A targets blockchain technology types. Module B restricts the scope to digital platform contexts. Module C covers the three research themes. All three modules are combined with AND logic to ensure direct relevance to the core topics of this paper (Table 2).

Table 1. Search String Module Structure.

Module	Function	Representative Search Terms (OR-Expanded)
Module A	Blockchain technology (mandatory)	blockchain, distributed ledger technology (DLT), smart contract, decentralized application (dApp), decentralized autonomous organization (DAO), decentralized finance (DeFi), Web3
Module B	Digital platform context (mandatory filter)	digital platform, platform ecosystem, platform governance, multi-sided platform, decentralized platform, platform infrastructure, digital infrastructure
Module C	Three research themes (at least one required)	trust, decentralized trust, interoperability, cross-chain, blockchain bridge, oracle, governance, on-chain governance, off-chain governance, DAO governance, self-sovereign identity (SSI), decentralized identifier (DID), verifiable credential, blockchain standard, regulatory framework

Table 2. Search Strategy Overview by Database.

Database/Source	Search Fields	Date Range	Document Types	Initial Hits
Scopus	TITLE-ABS-KEY	2015–2026	Journal articles, reviews, conference papers	412
Web of Science	TS= (topic field)	2015–2026	Journal articles, reviews, conference papers	389
IEEE Xplore	Abstract	2015–2026	Journals, conferences, early online	298
ACM Digital Library	Abstract	2015–2026	Research papers, review papers	267
ScienceDirect	Title, Abstract, Keywords	2015–2026	Research papers, review papers	241
SpringerLink	Full text and metadata	2015–2026	Journal articles, conference papers	240
Citation tracking	Forward + backward citation tracking	-	Peer-reviewed publications	31
Total				1878

2.2. Screening

The six databases yielded 1847 records. Citation tracking supplemented these with 31 additional studies, giving 1878 initial records. After deduplication, 610 duplicate records were removed, leaving 1268 for title and abstract screening. Following systematic assessment against inclusion criteria, 891 topically irrelevant records were excluded, yielding 377 full-text candidates. Full-text review applied journal quality, topical relevance, and methodological criteria, excluding 240 studies. The final corpus comprises 137 studies (Figure 1).

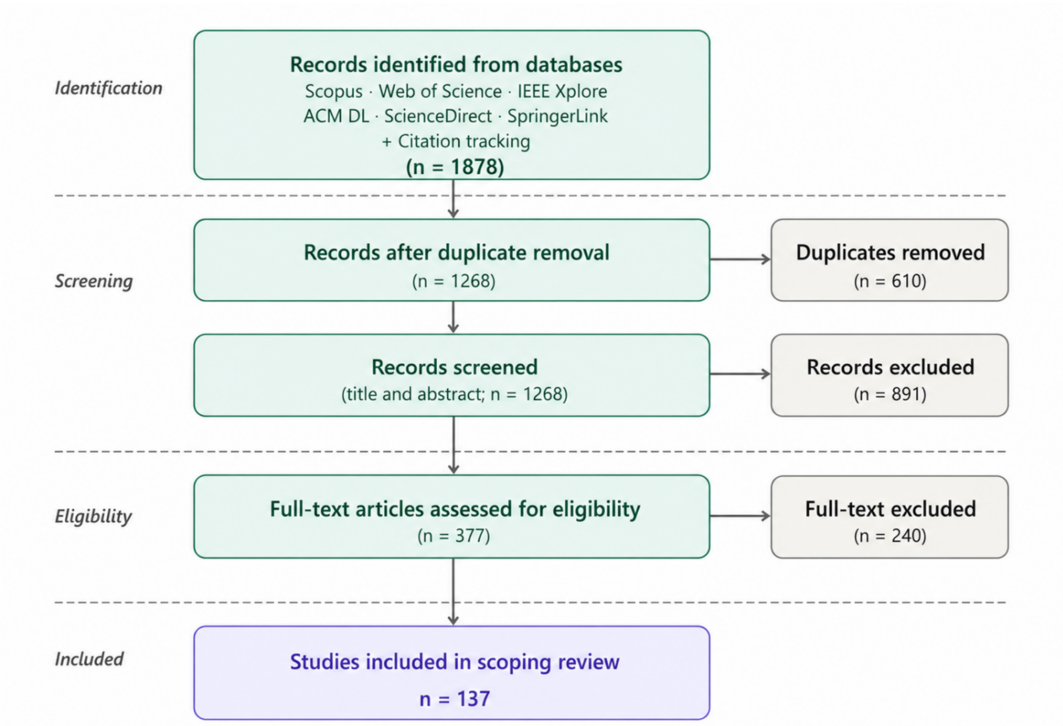

Figure 1. Review protocol and paper selection flow.

3. Descriptive Analysis

3.1. Publication Trends

Figure 2 presents the annual distribution of included studies from 2015 to April 2026 (n = 137). Overall publication volume shows an upward trajectory, growing from 2 studies in 2015 to 20 in 2024, at an average annual rate of approximately 17%. Brief declines occurred in 2020 and 2022. The 2020 dip reflects delays in academic publication cycles during the COVID-19 pandemic. The 2022 dip coincides with a cyclical downturn in the crypto-asset market and a contraction in sector confidence. A strong rebound followed in 2023 and 2024, with 11 studies appearing in 2025 as of the data cutoff. This reflects sustained scholarly attention to blockchain platform governance and institutional design. The overall trajectory indicates that academic output at the intersection of blockchain and digital platforms has entered a mature growth phase.

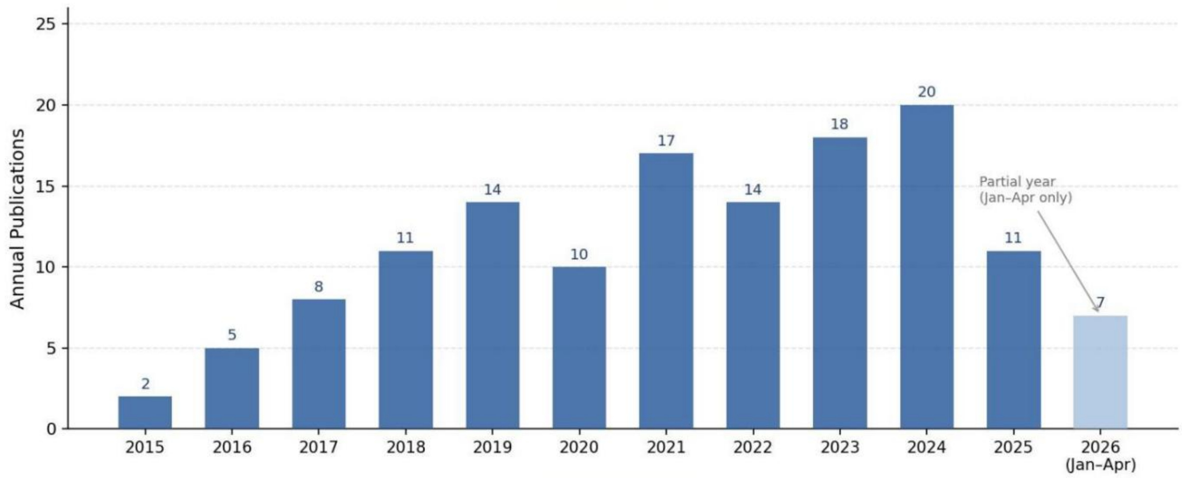

Figure 2. Annual publication trend.

3.2. Thematic Concentration

The three core research themes of this review, governance (45 studies, 33%), trust (28 studies, 20%), and interoperability (19 studies, 14%), together account for 67% of the corpus. Identity and SSI (13 studies, 9%) and smart contracts (12 studies, 9%) provide technical support for the core themes and form a secondary tier. Blockchain foundations and applications (20 studies, 15%) serve primarily as background reference material. This distribution closely aligns with the analytical framework of this paper. It indicates that existing scholarship has built substantial knowledge across the three core dimensions while revealing density differences among themes, providing a bibliographic foundation for the integrated analysis in subsequent sections (Figure 3).

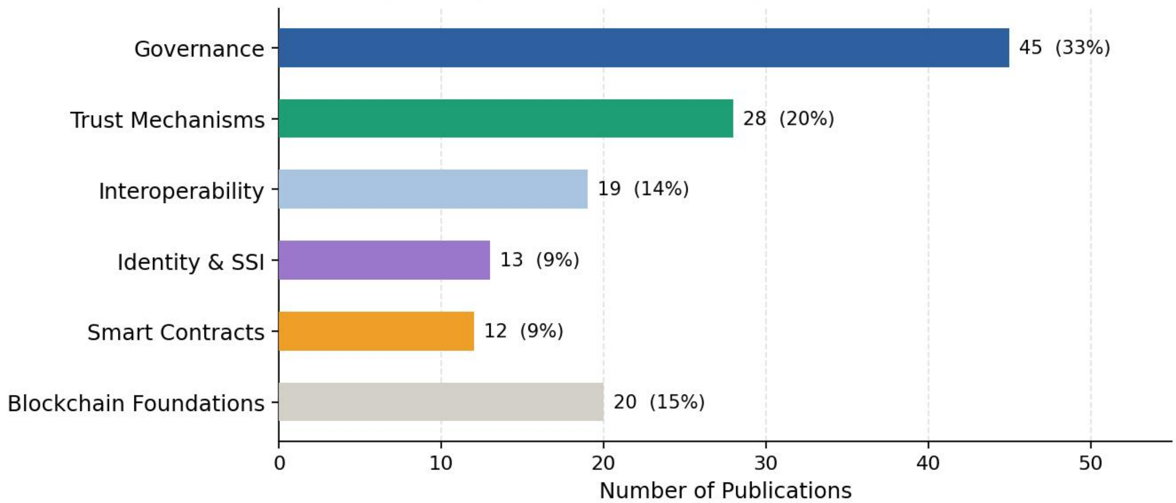

Figure 3. Thematic concentration.

3.3. Publication Outlets

Figure 4 lists the nine most productive outlets. Frontiers in Blockchain leads with six publications, indicating its role as a primary venue for blockchain and platform governance research. IEEE Access, Technological Forecasting and Social Change, and Internet Policy Review each contribute five publications, representing technical engineering, innovation management, and digital policy perspectives, respectively. This further confirms the interdisciplinary character of the field. Blockchains contributes four publications, and other outlets each contribute three. High-output venues span technical (IEEE Access), managerial (Technological Forecasting), and legal-political (Internet Policy Review) disciplines, directly corresponding to the trust-interoperability-governance framework of this review.

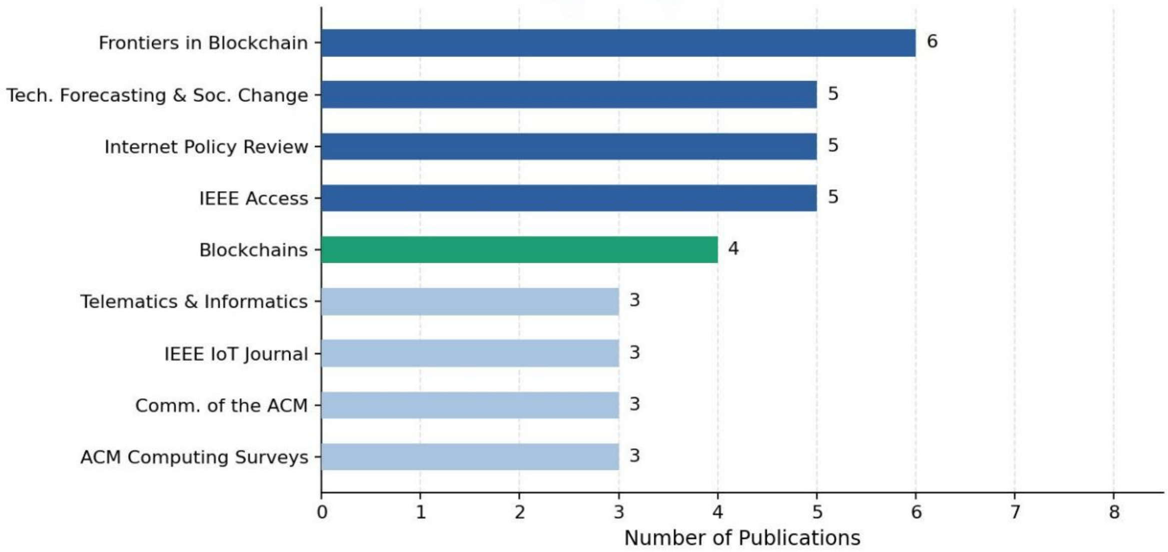

Figure 4. Publication outlet analysis.

3.4. Thematic Evolution

Between 2015 and 2018, the two groups were relatively balanced, reflecting the dominance of technical description and application exploration in that period. From 2019 onward, the core-theme share increased steadily, exceeding two-thirds of total publications in most years after 2021 and peaking in 2024. This trend indicates a systematic shift in blockchain research priorities. Scholarship is moving from questions about what blockchain can do toward questions about how its trust mechanisms, interoperability architecture, and governance logic operate. This shift provides direct bibliographic justification for organizing this review around the three-dimensional integrative framework. Figure 5 uses stacked bar charts to present the annual composition of publications on the three core themes relative to other topics from 2015 to 2026.

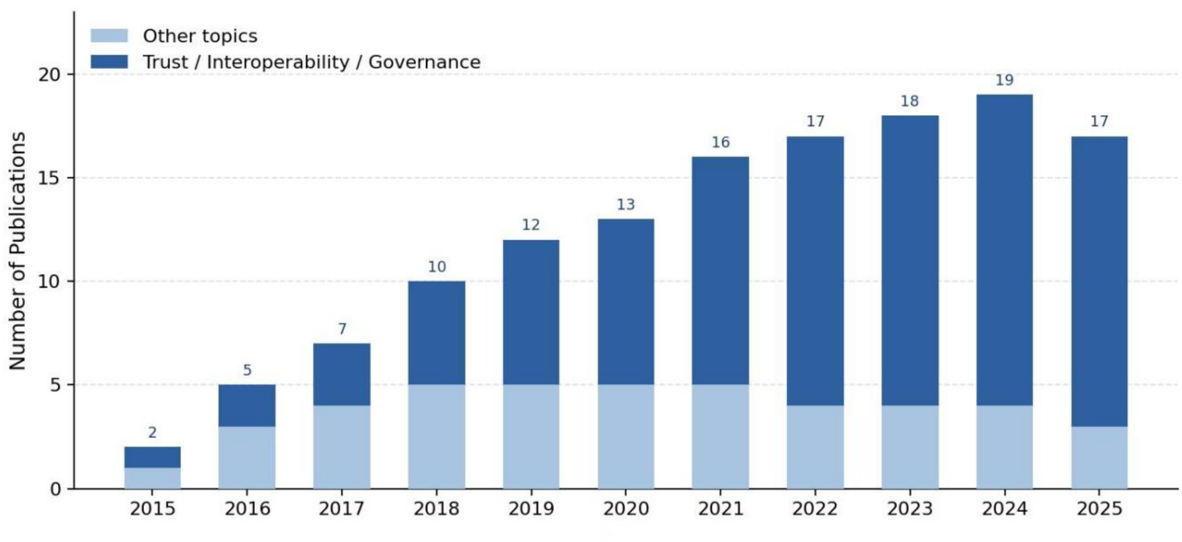

Figure 5. Thematic evolution.

4. Decentralized Trust

Trust is the foundational prerequisite for digital platform operation. Traditional platform architectures rely on institutional intermediaries such as banks, notaries, and platform operators to provide trust guarantees to transacting parties through legal constraints and reputational mechanisms. This third-party-centered trust system contains well-documented systemic vulnerabilities. The presence of intermediaries introduces friction costs, information asymmetries, and single-point failure risks [11,12]. Blockchain offers an alternative path around these vulnerabilities. As a distributed ledger architecture that transfers value without trusted intermediaries, blockchain relocates trust from credible institutions to verifiable mathematical protocols, substituting cryptographic certainty for institutional authority [3,13,14]. This path has inherent limits, however. Trust is fundamentally a social concept and cannot be fully replaced by algorithms [15]. This chapter examines four dimensions: the conceptual reconstruction of trust, the trust-execution infrastructure of smart contracts, the identity-layer transformation of self-sovereign identity, and the practical limits of decentralized trust. Together, they illuminate how blockchain redefines the generation, transmission, and maintenance of trust in digital platforms (Table 3).

Table 3. Multi-Level Trust Framework for Blockchain-Based Digital Platforms.

Trust Layer	Core Focus	Key Mechanism	Primary Challenge	Representative Studies
Protocol Layer	Consensus security and ledger integrity	Cryptographic hashing PoW/PoS consensus Immutable record structure	51% attacks Code correctness verification Hardware-level trust assumptions	[16–18]
Interface Layer	User experience and operational transparency	Audit trail accessibility Readable transaction records On-chain data visualization	Cognitive barriers for non-technical users UX complexity of wallets and keys	[19,20]
Organizational Layer	Developer and operator accountability	Governance frameworks Code auditing and disclosure Smart contract lifecycle management	Accountability gaps in pseudonymous settings Incentive misalignment among stakeholders	[21–23]
Institutional Layer	Legal recognition and regulatory legitimacy	Regulatory compliance frameworks Smart legal contracts Cross-jurisdictional standards	Jurisdictional fragmentation Lex Cryptographia vs. traditional law Enforcement blind spots	[8,24,25]

4.1. From Institutional Trust to Algorithmic Trust

Understanding how blockchain affects trust requires first clarifying the structure of trust in digital environments. Existing research distinguishes two nested dimensions of trust in digital platforms. The first concerns trust in the platform system itself, relating to users' judgments about technical reliability and operational fairness. The second concerns mutual trust among participants within the platform, sustained through platform mechanisms [20,25]. Traditional centralized platforms serve as key trust intermediaries at both levels. This intermediary role is also a source of the power asymmetry that poses latent threats to ecosystem health [23].

The paradigm of algorithmic trust initiated by blockchain does not seek to eliminate the need for trust. It relocates the anchor of trust from personified institutions to depersonified protocols. Trust is redistributed into consensus rules, cryptographic commitments, and immutable ledger structures [8]. Protocol rules are objectively neutral, code execution outcomes are deterministically predictable, and historical records are fully auditable. Shin [19] describes blockchain as an emerging technology of digital trust, emphasizing that its transparency and immutability provide a new basis for multi-party interaction without requiring any party to hold a privileged position. From a long-term archival perspective, this objective transparency has the potential to address persistent challenges in the trustworthiness of digital records [26,27].

In practice, establishing algorithmic trust is considerably more complex than theoretical accounts suggest. Blockchain's trust function depends on participants' collective acceptance of the entire technical architecture, including consensus mechanism design, the degree of node network decentralization, and the correctness of smart contract code [27,28]. Trust in a technical system is therefore no simpler than trust in an institution. It merely shifts the cognitive threshold from social judgment to technical understanding, and this threshold is often higher for ordinary users. Decentralized trust frameworks also face institutional compatibility challenges at the deployment stage. Algorithmic trust tends to complement rather than substitute for institutional trust [22]. At a deeper technical level, blockchain infrastructure rests on trust assumptions at the level of node hardware and operating systems. Algorithmic trust therefore presupposes a form of institutional trust at its foundation [17,29]. Trust reconstruction thus involves a downward relocation rather than an elimination.

4.2. Smart Contracts

If blockchain ledgers address trust at the data layer, smart contracts extend this trust logic to the contract execution layer. Smart contracts encode agreement terms in immutable on-chain code and execute automatically when predefined conditions are met, thereby bypassing the friction of enforcement through judicial systems [30,31]. This mechanism enables cross-organizational business process collaboration to proceed securely without requiring mutual trust [32], making smart contracts the most direct technical expression of blockchain's trustless promise [33].

At the application level, smart contracts have penetrated core domains including financial settlement, supply chain traceability, identity management, and digital rights protection. Their programmability represents a key transition from simple value storage to programmable trust infrastructure [29,34]. Academic research on smart contracts has grown exponentially, with the Ethereum ecosystem as the primary source of this research wave [35,36]. From an Internet of Things perspective, smart contracts provide foundational protocols for machine-to-machine autonomous trust execution, with the potential to support large-scale decentralized applications without human intervention [37].

When code fails, however, trust breaks down irreversibly. Systematic security vulnerabilities in smart contracts are well documented. Race conditions, integer overflows, and re-entrancy attacks are the most common vulnerability types. The immutability of on-chain execution amplifies their consequences far beyond those of conventional software failures [38]. Large-scale automated analysis of deployed Ethereum contracts has identified exploitable security flaws in a substantial proportion of contracts [39]. This reality stands in deep structural tension with the trusted-execution positioning that smart contracts are intended to embody [40,41]. Even the conceptual boundaries of smart contracts remain contested in the scholarly literature, and this ambiguity further compounds the uncertainty around trust construction [42].

Responses to these challenges operate at two levels. At the technical level, unified contract interface specifications and security audit standards are being developed to reduce systemic risk [43,44]. At the theoretical level, scholars are deepening their understanding of the relationship between smart contracts and substantive justice. Code-based rigid execution can establish procedural trust, but it may sacrifice substantive fairness when contract terms fail to capture the complexity of real-world situations. The tension between algorithmic certainty and legal flexibility thus becomes visible [45,46]. Smart contracts are not complete substitutes for trust but rather effective trust-supporting tools under specific conditions.

4.3. Self-Sovereign Identity

Identity authentication is the most fundamental and most vulnerable element of the trust infrastructure in digital platforms. Traditional platforms rely on centralized identity providers for user authentication and store identity data on the platform side. This creates a delegated trust structure in which users must trust that the platform will handle their identity information appropriately [34]. This structure has become increasingly untenable as data breaches accumulate and it tightly binds identity trust in platform ecosystems to the commercial interests of platform operators.

The core breakthrough of the self-sovereign identity (SSI) paradigm is the return of identity control from platforms to individuals. Users establish autonomous identities on the blockchain through decentralized identifiers (DIDs), independent of any centralized registry. They then prove specific identity attributes to third parties through verifiable credentials (VCs) without disclosing underlying data. This mechanism shifts the foundation of trust from trust in the platform to trust in cryptographic mechanisms, structurally decoupling identity trust from platform power [47]. Different technical approaches involve significant trade-offs among privacy protection strength, interoperability, and user experience. Public-chain solutions and consortium-chain solutions each carry distinct trust assumptions and applicable boundaries [48,49].

SSI applications are accelerating from technical prototypes to practical deployment. In platform access management, SSI-based access control frameworks enable fine-grained permission management while protecting user privacy [50]. In e-government contexts, blockchain-mediated identity frameworks offer a decentralized path for cross-institutional identity verification, though they also face deep institutional compatibility challenges with national sovereign authentication systems [51]. At the infrastructure level, decentralized PKI architectures offer viable alternatives or complements to existing internet trust anchors [52]. SSI effectiveness depends heavily on the legal and socio-cultural context in which it is embedded. Technical implementation alone cannot generate social-level identity trust [53].

4.4. The Limits of Decentralized Trust

The term trustless is blockchain's most evocative conceptual label, indicating that participants can complete secure interactions without mutual trust [18]. Under closer scrutiny, however, this description is misleading. Blockchain does not eliminate trust; it relocates the object of trust. Users must place substantial trust in the correctness of protocol code, the degree of decentralization in the validator network, and the enduring validity of underlying cryptographic assumptions [21,54]. Trust in a technical system carries no lower epistemic standing than trust in traditional institutions. It merely shifts the cognitive threshold from social judgment to technical understanding [55].

Blockchain is equally insufficient as a self-contained legal system. The determinism of code execution cannot replace the core functions of legal institutions in addressing incomplete contracts, redressing unintended outcomes, and protecting vulnerable parties. When smart contract execution diverges from the genuine intent of parties, blockchain provides no built-in error-correction mechanism, and existing legal frameworks contain significant jurisdictional gaps over automated on-chain execution [24,56]. Blockchain must therefore operate in conjunction with legal institutions rather than replace them. Blockchain's real value lies in reducing the coordination costs of establishing trust and limiting opportunities for opportunistic behavior through objective transparency. It does not fundamentally eliminate the necessity of trust [8].

Even in the most highly decentralized platforms, the social dimension of trust is pervasive. Misinformation diffusion and content credibility challenges do not dissolve through technical decentralization. Addressing these problems still depends on social-layer trust tools such as community norms and reputation mechanisms [57,58]. The effectiveness of decentralized trust therefore depends on the coordinated design of three layers: the technical layer, the economic incentive layer, and the socio-cultural layer. Over-reliance on any single layer produces structural vulnerability in the trust system [59]. The central challenge for blockchain trust research is understanding how these three layers form robust configurations across different platform contexts and institutional settings.

5. Blockchain Interoperability

Interoperability is the critical bottleneck determining whether blockchain can evolve from isolated technical experiments into unified digital infrastructure. The current blockchain ecosystem is characterized by extreme fragmentation. Hundreds of heterogeneous chains operate in parallel, each enclosed within its own consensus rules, data structures, and smart contract execution environments, with little capacity for cross-chain asset transfer, data sharing, or contract invocation [60,61]. This situation suppresses blockchain's network effects and creates fundamental technical obstacles to cross-platform digital service integration [62]. Resolving interoperability challenges is therefore a necessary path for blockchain's transition from single-chain ecosystems to multi-chain collaboration and eventually to unified digital platform infrastructure. This chapter examines the technical spectrum of cross-chain communication solutions, the role of oracles as a bridge between on-chain logic and off-chain data, and the function and limitations of international standardization in constructing an institutional framework for interoperability.

Beyond cross-chain communication protocols, data-level interoperability is a foundational prerequisite for constructing a genuinely interconnected digital ecosystem. The absence of unified blockchain data standards, semantic interoperability frameworks, and integration mechanisms between blockchain platforms and legacy information systems remains a significant barrier to real-world deployment [9,60]. Semantic interoperability—the capacity of heterogeneous blockchain networks to interpret shared data with consistent meaning—requires standardized data models, domain-specific ontologies, and metadata schemas. Without a shared semantic layer, even technically successful cross-chain message passing may fail to achieve meaningful information exchange. Equally important is the integration between blockchain platforms and traditional enterprise systems—including ERP, CRM, and supply chain management platforms—where middleware and API-gateway architectures serve as critical bridging infrastructure [63]. These considerations are increasingly recognized as central to the transition from isolated blockchain pilots to production-grade, interoperable digital platform infrastructure (Table 4).

Table 4. Comparative Analysis of Cross-Chain Interoperability Solutions.

Approach	Core Mechanism	Security	Decentralization	Latency	Throughput	Key Limitation
Notary Schemes	Trusted committee witnesses and relays cross-chain messages	**Medium**	**Low**	**High**	**High**	Reintroduces centralized trust; single point of compromise risk
Relay/SPV	Lightweight on-destination verification of source-chain block headers	**High**	**High**	**Medium**	**Medium**	High communication complexity; cost of storing block headers

Table 4. *Cont.*

Approach	Core Mechanism	Security	Decentralization	Latency	Throughput	Key Limitation
Hash Time-Locked Contracts (HTLC)	Cryptographic time-lock enables conditional atomic asset transfer across chains	**High**	**High**	**Low**	**Low**	Capital lock-up cost; inefficient in multi-hop routing; liquidity constraints
Dedicated Interop Layer	Protocol-level hub-and-spoke infrastructure relocates interoperability below the application layer	**Medium**	**Medium**	**Medium**	**High**	Systemic risk concentrated at hub node; cascade failure exposure
ZKP-Based Bridges	Succinct cryptographic state proofs enable trustless cross-chain state synchronization	**Very High**	**High**	**Medium**	**Medium**	High computational overhead; circuit design complexity limits scalability

Rating scale for Security and Decentralization columns: Very High, High, Medium, Low | Latency: Low = Fast (favorable), High = Slow (unfavorable)

5.1. Origins and Consequences of Interoperability Failure

Understanding the interoperability problem requires examining the causes of fragmentation. At the technical level, individual blockchain protocols were designed to be highly autonomous from the outset. Incompatibilities in consensus algorithms (PoW, PoS, PBFT, etc.), address formats, transaction models, and virtual machine specifications create multiple heterogeneous barriers to cross-chain communication [64,65]. At the economic level, intense competition among early blockchain projects sometimes made the absence of interoperability a deliberate strategic choice, intended to deepen technical lock-in and strengthen network effect advantages. At the standardization level, the blockchain field lacks broadly accepted foundational interoperability standards comparable to the TCP/IP protocol family, and this communication barrier persists [66,67].

The economic consequences of fragmentation are growing more pronounced as the multi-chain ecosystem matures [68]. Inefficient cross-chain asset flows produce extensive liquidity fragmentation. Hundreds of billions of dollars in on-chain assets within the DeFi ecosystem are confined to individual chains and unable to participate in financial activities on other chains. In enterprise blockchain applications, supply chain, logistics, and trade finance scenarios typically require spanning multiple consortium chains. The absence of interoperability restricts the digital coverage of these use cases [63,69,70]. Interoperability is therefore not merely a technical engineering challenge. It is an important economic boundary condition constraining the commercial value of blockchain technology.

5.2. The Technical Spectrum of Cross-Chain Communication

Both academia and industry have proposed multiple technical approaches to cross-chain interoperability, forming a continuous spectrum from highly centralized to fully decentralized. Notary schemes introduce a trusted third-party node or committee to witness and relay cross-chain messages. They are the lowest-barrier and most historically established solution, but their cost is the reintroduction of centralized trust assumptions, creating tension with blockchain's fundamental decentralization ethos [71]. Relay/SPV schemes verify the source chain block header on the destination chain in lightweight fashion, achieving cross-chain state proofs without trusted intermediaries. They are more purely decentralized, and their security and communication complexity have been analyzed from a distributed computing theory perspective [72,73].

Hash Time-Locked Contracts (HTLCs) use cryptographic commitment schemes to synchronize conditional asset transfers across different chains. They offer strong security guarantees in bilateral atomic swap scenarios but face constraints from lock costs and routing efficiency in multi-hop and large-scale liquidity settings [74]. Dedicated interoperability layer solutions construct independent cross-chain coordination infrastructure, relocating interoperability capabilities from the application layer to the protocol layer and enabling scaled multi-chain collaboration through hub-and-spoke structures [9]. These solutions, however, concentrate systemic security risk at the hub node. Cross-chain bridge layers have become the most concentrated site of value loss in blockchain systems, and security design is a central dimension in comparing interoperability solutions [75,76].

The rapid maturation of zero-knowledge proofs (ZKPs) opens a new technical path for cross-chain interoperability. By generating succinct cryptographic state proofs, ZKP-based cross-chain bridges achieve efficient cross-chain state synchronization without relying on trusted relays, offering a better trade-off between security and decentralization than existing solutions. This direction is regarded as a strong candidate for next-generation cross-chain technology, but the computational overhead and circuit design complexity present substantial obstacles to large-scale deployment [77]. The optimal solution for any given cross-chain scenario ultimately depends on the specific trade-offs among security, degree of decentralization, latency, and throughput [78]. No single universally superior solution exists [71,74].

5.3. Bridging on-Chain Logic and off-Chain Reality

Cross-chain interoperability addresses communication between blockchain networks, but a different interoperability challenge arises at the boundary between blockchain and the external world. Smart contract execution logic is sealed within the blockchain and cannot directly perceive changes in external world states. Asset prices, IoT sensor data, logistics events, and election results are all inaccessible to on-chain contracts directly [79]. Oracles serve as the bridging mechanism connecting on-chain logic with off-chain data and are therefore indispensable infrastructure for smart contracts to realize their full potential [80].

The fundamental tension of the oracle problem lies in its structural conflict with the trust commitments of smart contracts. Smart contract trustlessness guarantees rest on the sealed and isolated nature of on-chain execution environments and the deterministic verifiability of code logic [81]. Once external data is introduced, the entire trust chain develops a gap at the data input stage. Attackers need not break any cryptographic mechanism. Manipulating the data sources that an oracle references is sufficient to control contract execution outcomes. Price oracle manipulation attacks have become one of the leading attack types causing asset losses in the DeFi ecosystem. Their root cause is the excessive reliance of early DeFi protocols on single data sources [80]. Decentralized oracle networks partially mitigate this risk through multi-source data aggregation and economic incentive mechanisms. Whether off-chain data faithfully reflects the real-world state it claims to represent remains an epistemological problem that cryptography cannot fully resolve [36].

Oracle trustworthiness design is therefore a critical element of interoperability solutions in real applications. In Industrial IoT data markets, combining trusted execution environments (TEEs) with blockchain provides hardware-level integrity guarantees for data collection and transmission, establishing stronger trust foundations before data enters the blockchain [82]. In health data interoperability settings, simultaneously satisfying oracle trustworthiness, privacy protection, and compliance standards remains a primary technical obstacle to large-scale blockchain adoption in healthcare [83,84]. The oracle problem thus reveals that blockchain interoperability is fundamentally a trust design challenge spanning technical, economic, and institutional layers rather than a purely communications protocol issue.

5.4. Institutional Foundations of Interoperability

Technical pluralism reflects the innovative vitality of the interoperability space, but it simultaneously constitutes an institutional obstacle to achieving interoperability. This fragmentation pattern has been documented by early systematic reviews [85]. Standardization converts isolated islands into interoperable collaborative networks by establishing a common technical language and interface specifications. It is a necessary stage in any technology ecosystem's transition from fragmentation to maturity. Standards reduce transaction costs and shape technology trajectories in innovation ecosystems, but they may also suppress disruptive change by creating technical lock-in [86]. This tension is especially acute in the blockchain domain. Premature standard-setting risks consolidating suboptimal technical paths, while the absence of standards continues to obstruct large-scale interoperability deployment [87].

Current international blockchain standardization proceeds on multiple tracks with insufficient coordination. ISO TC307, ITU-T FG DLT, the IEEE Blockchain Initiative, and the W3C DID Working Group each operate in parallel. Overlaps and conflicts exist in core areas including terminology, reference architecture, and security requirements. The absence of cross-organizational coordination mechanisms makes standard fragmentation an obstacle to interoperability standardization itself [88,89]. Standardization challenges at the smart contract layer are particularly complex. Missing specifications for contract interfaces, security auditing, and contract lifecycle management prevent smart contracts on different platforms from achieving portability and reusability [43]. Agile, experiment-driven standardization is therefore regarded as a pragmatic strategy for advancing interoperability in rapidly evolving technical environments.

At the regulatory-driven standardization level, the European Union and the United States have taken markedly different approaches. The EU uses the EBSI platform to prioritize decentralized identity, verifiable credentials, and cross-border blockchain interoperability as regulatory agenda items. Legislative instruments including MiCA and eIDAS 2.0 provide institutional anchors for the standardization process, continuing the governance logic of government-led blockchain infrastructure for cross-institutional information sharing. The United States relies more heavily on industry self-regulation and market competition to drive technical standard formation, offering greater innovation diversity but also higher regulatory uncertainty. The divergence between these two approaches reflects not merely different technical governance styles but deeper value disagreements about digital sovereignty, innovation policy, and regulatory philosophy. Blockchain interoperability standardization is therefore not only a technical coordination problem but also a digital governance challenge with substantial geopolitical dimensions [90,91].

5.5. Data Standards, Semantic Interoperability, and Legacy System Integration

The interoperability challenge extends beyond cross-chain protocol design into the realms of data standardization, semantic consistency, and enterprise system integration. At the data layer, heterogeneous blockchain networks employ incompatible data structures, transaction formats, and state representations, creating obstacles to seamless information exchange even when communication channels exist [60]. Standardized data schemas—including common asset representations, event log formats, and metadata conventions—are prerequisites for scalable cross-platform collaboration. The development of common blockchain data standards has accordingly been identified as a priority for interoperable digital infrastructure.

Semantic interoperability introduces a further layer of complexity. Different blockchain applications may assign divergent meanings to superficially similar data fields, leading to interpretation failures in cross-chain transactions. Ontology-based approaches, which define shared vocabularies and relationship schemas for domain-specific blockchain applications, offer a promising path toward semantic alignment [47]. In supply chain contexts, for example, standardized product identification and provenance ontologies enable interoperability across consortium chains operated by different industry participants [63]. However, achieving semantic consensus across competing blockchain ecosystems requires not only technical specifications but also coordinated governance arrangements—a challenge that bridges the interoperability and governance dimensions of this review.

Integration with legacy information systems constitutes the third pillar of data interoperability. Most enterprise blockchain deployments must coexist with established ERP, CRM, and database systems rather than replacing them outright. Middleware architectures, oracle-based data bridges, and API gateway layers serve as critical infrastructure for connecting blockchain networks to traditional systems [37,79]. These integration mechanisms must address data synchronization, conflict resolution, and consistency guarantees across hybrid architectures. The absence of robust legacy integration remains a key factor limiting blockchain's transition from experimental pilots to production-scale digital platform infrastructure, particularly in regulated industries such as finance, healthcare, and public administration.

6. Blockchain Governance

Governance is blockchain research's broadest and most persistently contested core topic [92]. In the widest sense, blockchain governance encompasses two intertwined but distinct problem dimensions. The first asks who has the authority to determine the rules of the blockchain protocol itself, including their formulation, amendment, and upgrading. This is governance of the blockchain. The second asks how blockchain's technical properties can be used to improve organizational, platform, and social decision-making structures. This is governance through blockchain [6,93]. On-chain rule design shapes who can participate in governance and with what weight, while off-chain political processes ultimately determine the direction of on-chain rule evolution [94]. This chapter examines the theoretical framework of on-chain and off-chain governance, the rise and practical limitations of DAOs, blockchain governance's structural reshaping of digital platform ecosystems, and the evolving logic of regulatory and institutional governance.

A central tension in blockchain governance is the emergence of re-intermediation: while blockchain technology is often promoted as a decentralized alternative to traditional intermediaries, its practical deployment frequently gives rise to new forms of governance centralization. Influential validators, platform operators, foundation members, and consortium coordinators increasingly assume coordination and decision-making functions that resemble those of the intermediaries blockchain was intended to replace [10,95]. Understanding these re-intermediation dynamics is essential for assessing the substantive degree of decentralization in blockchain-based digital platforms.

6.1. On-Chain and Off-Chain Governance

The basic structural tension of blockchain governance lies in the relationship between on-chain and off-chain governance forms. On-chain governance achieves automated protocol rule changes through mechanisms such as token voting in smart contracts. It is characterized by high execution determinism and transparency. Off-chain governance, by contrast, drives rule evolution through social-political processes including developer community deliberation, miner and validator collective action under consensus mechanism constraints, and foundation strategic decisions. It retains flexibility and space for human judgment [96]. The two forms are not mutually exclusive. In practice they form a division of labor. Community-level consensus formation occurs off-chain and eventually solidifies into on-chain protocol changes through hard forks or soft forks [97].

Blockchain governance finds its theoretical roots in social contract traditions. Participants accept protocol rules in exchange for network services, a relationship structurally analogous to Lockean voluntary contracting. What distinguishes blockchain governance is the relatively low cost of exit for participants, who can choose not to participate or even create new protocol versions through forking. This gives blockchain governance a highly competitive dynamic equilibrium character [98,99]. Rules embedded in unbypassable code give governance very high execution certainty, but this also eliminates interpretive flexibility when responding to unforeseen situations [30]. Blockchain governance thus faces a fundamental tension. The conflict between execution certainty and rule adaptability is a core constraint that any governance architecture must confront [100].

The practical implication of this framework is that no optimal governance design exists for blockchain. Only optimal trade-offs for specific objective functions exist. Three challenges constitute the basic criteria for evaluating any blockchain governance design: who has the authority to define rules, how a decentralized participant distribution can be maintained, and what remedies are available when code execution contradicts intended outcomes [101]. Existing literature on governance failure scenarios remains relatively thin. How systems should safely degrade when governance mechanisms cannot respond effectively to technical crises or external shocks is a research direction that urgently requires development [6].

6.2. Decentralized Autonomous Organizations

Decentralized autonomous organizations (DAOs) represent the most radical experiment in blockchain governance theory at the level of organizational practice. Their core proposition is to encode organizational operating rules in smart contracts and enable collective governance by token holders through on-chain voting, realizing self-operation without managers. From an institutional economics perspective, DAOs can be understood as a hybrid coordination mechanism between markets and hierarchies, substituting token incentives and code rules for price signals and administrative authority [102,103]. This vision is rhetorically compelling, promising equal participation, transparent decision-making, and an anti-monopoly organizational future.

Empirical research has raised serious challenges to the decentralization promise of DAO governance. Large-scale DAO data analysis shows that DAO success depends heavily on early liquidity, token distribution fairness, and governance participation rates. Most operational DAOs have not achieved genuine decentralization. Small numbers of early large token holders effectively control overwhelming voting weight [104]. Empirical analysis of multiple real-world DAOs confirms that DAOs perform well in increasing decision transparency but face persistent structural challenges from a democratic dilemma in decision efficiency and participation rates [105]. Extreme inequality in token wealth distribution maps directly onto extreme concentration of governance power, creating a form of technocratically packaged oligarchic governance [10,95].

This governance centralization extends beyond token distribution to encompass structural forms of re-intermediation. Core development teams, foundation councils, and influential validators often wield disproportionate agenda-setting power, effectively functioning as the "new intermediaries" within nominally decentralized systems [10,95]. The concentration of protocol upgrade authority and treasury management in the hands of small core teams further illustrates the gap between decentralization rhetoric and governance reality. Comparative studies of DAO governance across jurisdictions therefore highlight the need for institutional frameworks that can accommodate both organizational autonomy and the accountability expectations of traditional corporate governance [6,100].

Research on DAO governance is moving from descriptive accounts toward mechanism improvement. Design-level explorations include quadratic voting to reduce the weight of capital, reputation systems to incorporate non-tokenized participation contributions, and multi-committee structures to disperse single decision-making authority [105]. Predictive governance frameworks based on parallel intelligence attempt to use AI simulation to evaluate proposal impacts before execution, compensating for inherent limitations of purely on-chain voting mechanisms in foresight and adaptability [106]. Fine-grained analysis of DAO decision processes reveals that high voter turnout does not necessarily translate into high-quality decisions. The nonlinear relationship between participation rates and decision quality is an important constraint on DAO governance mechanism optimization [107]. The deep interactions among decentralization degree, consensus mechanism choice, and ownership concentration imply that different governance mechanism combinations inevitably face fundamental trade-offs between efficiency and decentralization [108]. Algorithmized on-chain rules represent only one layer of

DAO governance. Non-algorithmic governance mechanisms such as community norms, reputational culture, and platform constitutions often exert more profound influences on ecosystem behavior [109].

6.3. Structural Reshaping of Digital Platform Ecosystems

The impact of blockchain governance mechanisms on digital platform economies is concentrated in the reconfiguration of power structures. In traditional digital platforms such as Uber, Amazon, and Facebook, governance authority is highly concentrated in platform operators. Users, developers, and content creators have little substantive influence over platform rules and are locked into platform ecosystems with limited genuine exit options. By encoding core platform rules in immutable smart contracts and opening rule modification rights to multiple stakeholders through token governance, blockchain structurally challenges this unilateral power arrangement [10,95].

This power reconfiguration has profound implications for platform organizational boundaries [110]. Blockchain redefines, through trusted code, the range of transactions that can be coordinated through markets without internalization. Activities that once required organizational internalization to avoid opportunistic risks can now be safely outsourced to the market through smart contracts [34]. In multi-sided platform settings, blockchain effectively promotes multi-sided market participation by reducing trust friction at the platform core, though smart contract rigidity and user experience complexity remain primary obstacles to large-scale adoption [111]. Blockchain platforms show their greatest advantages under three conditions: collaborative ecosystems involving multiple parties, market environments lacking credible intermediaries, and industry settings with strong regulatory demands for audit transparency [5].

At a more macro-narrative level, blockchain is regarded as a strategic tool for small and medium enterprises and individual creators to counter large platform monopolies. The logic is that decentralized governance gives participants genuine influence over platform rules, a fundamental institutional difference that no centralized platform can provide [2]. In the sharing economy, blockchain has the potential to redistribute value from platform operators to actual service providers and consumers by eliminating the platform layer's trust intermediary role [112]. Analysis of layered governance frameworks for decentralized platform ecosystems shows that effective governance requires designing appropriate mechanisms at the infrastructure layer, protocol layer, and application layer separately [113]. In emerging interdisciplinary settings, the synergy of artificial intelligence and blockchain provides new momentum for Web3 platform business model innovation but also introduces institutional contradictions between AI opacity and blockchain transparency. Resolving this contradiction will be a central challenge for next-generation decentralized platform architecture design [114]. Emerging domains such as decentralized finance and voluntary carbon markets provide real-world cases of blockchain governance addressing public resource challenges, demonstrating both the innovative potential and institutional design tensions of DAO governance models in sustainability contexts [115].

6.4. Regulatory Frameworks and Institutional Governance

Deep institutional tensions exist between blockchain's decentralized properties and existing regulatory frameworks. Traditional regulation assumes the existence of identifiable responsible parties, but blockchain's anonymity, cross-border character, and automatic code execution fundamentally challenge this premise at the technical level. When automated contract execution causes losses, when anonymous participants create market manipulation, or when cross-border flows circumvent any single jurisdiction, existing regulatory tools face enforcement blind spots [24,116]. De Filippi and Wright [33] describe this phenomenon as the rise of Lex Cryptographia. A new legal order grounded in cryptography is quietly forming within the blockchain ecosystem. It substitutes automated code execution for traditional legal intervention but contains deep institutional gaps in legal redress and normative legitimacy.

From an institutional economics perspective, blockchain is fundamentally a new form of institutional technology. By restructuring transaction cost structures in social coordination, it competes with and complements the three traditional institutional forms of market, firm, and government [3]. At the corporate governance level, blockchain's technical properties offer viable paths to real-time shareholder voting, automated dividend distribution, and transparent information disclosure. At the same time, they create unresolved compliance tensions between blockchain's automated execution logic and corporate law requirements [117,118]. These challenges collectively indicate that blockchain's institutionalization is not a one-way process of technology replacing law. It is instead a complex adaptive process requiring the co-evolution of technical norms, legal institutions, and market mechanisms [119].

At the practical regulatory level, regions worldwide are advancing blockchain institutionalization at very different paces and along different paths. The EU, through MiCA regulations, the eIDAS 2.0 framework, and the EBSI infrastructure, has formed a systematic governance path characterized by regulatory leadership and unified standards. This approach has demonstrated considerable policy efficiency in advancing public service interoperability and digital identity standardization. The United States, hindered by slow legislative progress and competition among multiple regulatory bodies, has produced a regulatory environment marked by high policy uncertainty but vigorous technical innovation. Ethereum's historic transition from proof of work to proof of stake provides a paradigmatic case of how fundamental protocol-level governance changes can be completed under the surface of technical upgrades, and of how such changes deeply reshape power structures within network ecosystems [120].

The regulatory landscape for blockchain-based digital platforms has intensified significantly. In the United States, the Securities and Exchange Commission (SEC) has progressively clarified its stance on digital assets, applying the Howey Test framework to determine whether token offerings constitute securities, thereby imposing substantial compliance obligations on blockchain platforms and token issuers. The SEC's enforcement actions against major cryptocurrency exchanges and DeFi protocols have underscored the regulatory uncertainty facing blockchain platforms operating in U.S. jurisdictions [3,24]. In Asia, Singapore's Monetary Authority (MAS) has adopted a more calibrated approach through its Payment Services Act and the regulatory sandbox framework, providing clearer guidance for digital payment token services while maintaining consumer protection standards. Similarly, Thailand's Securities and Exchange Commission has established a licensing regime for digital asset exchanges and token issuance, creating a structured compliance pathway for blockchain platforms. These divergent regulatory approaches reflect fundamentally different policy philosophies: the U.S. emphasis on investor protection through enforcement, Singapore's pragmatic sandbox model, and the EU's comprehensive regulatory harmonization via MiCA. For blockchain platforms operating across jurisdictions, navigating this fragmented regulatory environment requires substantial compliance infrastructure and legal expertise, creating barriers to entry that may inadvertently reinforce the platform concentration blockchain was intended to disrupt.

The core consensus in blockchain governance research is shifting toward questions of which governance architectures are most effective in which contexts [121]. On-chain governance certainty and off-chain governance flexibility each have irreplaceable value at their respective boundaries. The efficiency advantages of algorithmic governance must be supplemented by the error-correction capacity of institutional governance, and decentralized participation structures require compatibility with incentive-aligned mechanism design [91]. No single governance model can simultaneously achieve optimality on all dimensions. Blockchain governance mechanisms will therefore evolve through continuous adaptive adjustment [6,10,100].

Compliance challenges are particularly acute for blockchain platforms serving regulated industries. Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, data protection regulations such as the GDPR, and sanctions screening obligations create tension with blockchain's pseudonymous and immutable design principles [24]. The "right to be forgotten" under GDPR, for instance, is structurally incompatible with immutable ledger records, requiring innovative technical solutions such as off-chain data storage with on-chain hashes or zero-knowledge proof-based identity verification. Institutional oversight mechanisms—including audit committees, compliance officers, and regulatory reporting frameworks—are being adapted to blockchain contexts, but the effectiveness of these mechanisms in decentralized environments remains an open empirical question. Future governance research must examine how blockchain platforms can achieve regulatory compliance without sacrificing the decentralization properties that constitute their core value proposition.

7. Future Research Directions

Blockchain research has entered a mature phase. Early literature focused heavily on demonstrating technical feasibility and identifying application scenarios [61,122,123]. The central questions have now shifted to whether decentralized infrastructure can support trustworthy, interoperable, and well-governed digital platforms at scale under real-world conditions. Existing literature has built solid theoretical foundations across the trust, interoperability, and governance dimensions but has also clearly exposed several systemic knowledge gaps. This review proposes five priority research directions based on these gaps.

7.1. Multi-Level Trust Modeling

Trust is a multi-level phenomenon, but existing research tends to treat individual levels in isolation. User-perceived trust, system security, and institutional legitimacy are addressed separately, with limited systematic theorization of their dynamic interactions [7,21]. This fragmented state limits the cumulativeness of research findings. Trust variables at different levels lack a common reference framework for cross-study comparison.

Building integrative multi-level trust models is the core path to closing this gap. Such models should simultaneously cover four dimensions: protocol-level guarantees such as consensus security, interface-level trust including user experience and transparency, organizational-level accountability regarding developer and operator responsibility structures, and institutional-level legitimacy measured by the degree of legal framework endorsement. Existing research has touched on each of these dimensions separately, but the theoretical work of integrating them into a unified framework remains unfinished [16,20,22,24].

Large-scale platform adoption depends fundamentally on whether all four trust dimensions simultaneously reach critical thresholds. Optimizing any single dimension cannot substitute for the coordinated configuration of the whole [8,58]. Future research should prioritize constructing and empirically testing multi-level trust frameworks, with particular attention to mutually reinforcing or mutually attenuating effects across dimensions.

7.2. Interoperability Governance

Cross-chain technology is evolving rapidly. Innovations including bridge protocols, modular blockchain architectures, shared sequencers, and cross-chain messaging layers continue to emerge [9,74]. Technical progress has clearly outpaced governance arrangements. Questions of who sets interoperability standards and how liability should be determined when cross-chain incidents occur currently have no clear answers [65,66].

The governance deficit in interoperability is not merely a management problem. It is an economic and security problem. Cross-chain bridge layers have become the most concentrated site of value loss in the blockchain ecosystem, and existing cross-chain incident response mechanisms are highly fragmented. International standardization efforts have begun but coverage overlaps and the absence of cross-organizational coordination remain primary obstacles [47,66,75].

Future research needs to answer three categories of questions. First, how should interoperability governance authority be allocated among protocol developers, application platforms, and regulators? Second, how should risk-bearing structures for cross-chain failures be designed? Third, how will deepening interoperability reshape competitive interdependencies and bargaining power among platforms? Oracle governance belongs equally to the core agenda of this research direction. Mechanisms for ensuring data source authenticity and allocating accountability remain insufficiently studied [15].

7.3. Comparative Institutional Analysis

Blockchain governance never operates in an institutional vacuum. It is deeply embedded in the distinct legal traditions, regulatory systems, and digital sovereignty preferences of different countries. The systematic divergence between the EU and the United States on blockchain standardization paths provides a natural quasi-experimental setting for comparative institutional analysis. Existing comparative research, however, remains at the level of macro-policy description, with limited exploration of how institutional design differences affect the strategic choices of micro-level actors.

Institutional arrangements worth comparing span multiple dimensions: the legal classification of token governance, the cross-border portability of decentralized identity, the judicial enforceability of smart contracts, and the modes of recognition of DAO legal status [3,33]. Variations in how different jurisdictions approach these issues will profoundly affect the geographic distribution of blockchain platforms, the scope for regulatory arbitrage, and the formation path of global standards [10].

The value of comparative institutional research lies not only in documenting differences but in identifying institutional complementarities, specifically which institutional combinations effectively support healthy blockchain ecosystem development and which produce inhibitory effects. This research direction can help the field move beyond technology-centered explanatory frameworks and toward a more systematic understanding of institutional conditions [19,63].

7.4. Hybrid Platform Architecture Research

Real-world blockchain platforms rarely match the ideal of complete decentralization. More common are hybrid architectures in which public chains provide foundational infrastructure, private or consortium layers manage data permissions, middleware suppliers provide interface services, and regulatory interfaces satisfy compliance requirements [5,42]. These hybrid models are not transitional exceptions. They are very likely the dominant long-term organizational form.

Existing research has accumulated more analysis of pure public chains and pure consortium chains. The organizational logic and strategic implications of hybrid architectures receive insufficient systematic attention. The core tension facing hybrid platforms is how to maintain sufficient interoperability openness while preserving governance controllability and regulatory compliance, avoiding the lock-in patterns of centralized platforms [14,99]. This tension has been illustrated in numerous cases of enterprise blockchain deployment and the migration of DeFi protocols toward compliance, but theoretical work lags significantly behind.

Future research should examine how enterprises and communities can jointly design hybrid governance architectures that seek dynamic equilibrium between controllability and openness. Research should also investigate how AI-blockchain integration creates new value within hybrid architectures while introducing new governance complexity, and how hybrid platform organizational boundaries adjust dynamically in response to technological evolution and institutional pressures [2,33]. These questions constitute the frontier of blockchain platform strategy research.

7.5. Cross-Study Measurement Frameworks

A long-standing constraint on blockchain research is the absence of reliable cross-study comparison tools. Core constructs such as degree of decentralization, governance quality, trust distribution, interoperability maturity, and identity portability are operationalized in fundamentally different ways across studies. This makes it difficult to accumulate research findings effectively [63,104].

The consequences of this measurement gap are systemic. Assessments of DAO governance quality use different indicators across studies, leading to contradictory and irreconcilable conclusions about DAO effectiveness [89,105]. Blockchain trust measurement oscillates between technical security metrics and user perception scales, lacking a unified multi-dimensional measurement system [20,81]. Interoperability maturity equally lacks a tiered assessment framework comparable to CMM models, making systematic cross-platform comparison difficult [17].

Advancing this direction requires coordinated efforts. Building publicly reusable blockchain platform datasets, developing shared classification standards covering trust, governance, and interoperability, and creating benchmarking tools applicable across contexts are all necessary steps [10,104]. Maturing measurement frameworks is the key prerequisite for moving blockchain research from observation-driven inquiry to theory-testing inquiry and for enhancing the policy relevance of empirical work in this field.

8. Conclusions

Blockchain's fundamental contribution to digital platforms lies not in decentralization itself but in the reconstruction of coordination mechanisms. Verification, rule enforcement, and data control are redistributed from corporate internalization to protocols, validator networks, and community governance [3]. The central argument of this review is that trust, interoperability, and governance are not three independent topics. They constitute mutually supporting systems. Trust without interoperability creates silos. Interoperability without governance compounds fragility. Governance without technical grounding remains rhetorical [8].

In the trust dimension, blockchain shifts trust from identifiable institutions to technical systems, reducing opportunistic risk without eliminating the need for trust. Algorithmic trust and institutional trust are complementary rather than substitutable [21,24]. In the interoperability dimension, technical solutions are now substantial, but cross-chain liability attribution, standard authority, and risk-sharing mechanisms remain in an institutional vacuum. The ultimate shape of interoperability will be determined by regulatory negotiation rather than engineering logic alone [27,88]. In the governance dimension, on-chain mechanisms provide certainty while lacking adaptability. Power concentration and participation failure in DAO practice indicate that effective governance must co-design on-chain rules with off-chain norms [96,105].

The governance dimension must also reconcile blockchain's decentralized architecture with evolving regulatory requirements. The fragmented regulatory landscape—characterized by the SEC's enforcement-led approach in the United States, Singapore's regulatory sandbox model, and the EU's comprehensive MiCA framework—creates compliance complexity for cross-jurisdictional platforms. Re-intermediation dynamics further complicate governance: influential validators, foundation councils, and core development teams often function as de facto intermediaries, narrowing the gap between blockchain's decentralization aspirations and governance practice.

For practitioners, evaluating blockchain adoption should take the ecosystem as the unit of analysis. The alignment of architecture with the coordination problem being solved carries more decision-making significance than the degree of decentralization itself [5,113]. For policymakers, standardization and regulatory design are endogenous variables in the formation of platform competitive landscapes rather than external considerations. Absence from standard-setting processes during the formative period effectively cedes that space to specific technological or commercial interests [86]. For researchers, advancing multi-level integrative frameworks and shared measurement tools is the primary task for increasing the density of knowledge accumulation in this field [124,125].

This review relied primarily on academic databases. Industry white papers and standards documents were not included, creating a currency gap in technically fast-moving areas such as interoperability. Interdisciplinary literature integration also introduces heterogeneity in construct operationalization, which affects the rigor of cross-study comparisons to some degree.

The defining standard for next-generation digital platforms will not be whether they are decentralized but whether they can translate decentralization into trustworthy, interoperable, and governable coordination mechanisms. Blockchain is an institutional and architectural infrastructure that continues to evolve. Its development trajectory will be shaped by coordinated progress in protocol engineering, identity standards, security specifications, governance design, and regulatory coordination [6,33].

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

No new data were generated or analyzed in this study.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

During the preparation of this work, the author used ChatGPT solely to improve the language and readability of the manuscript, as the author are non-native English speakers. The author reviewed and edited the content as needed and take full responsibility for the content of the published article.

References

1. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horizons* **2019**, *62*, 295–306. https://doi.org/10.1016/j.bushor.2019.01.009.
2. Gala, K. Digital Davids, global Goliaths, and the Web3 sling. *Bus. Horizons* **2024**, *67*, 5–17. https://doi.org/10.1016/j.bushor.2023.06.002.
3. Davidson, S.; De Filippi, P.; Potts, J. Economics of blockchain. *Public Choice* **2018**, *176*, 111–134. https://doi.org/10.1007/s11127-018-0505-1.
4. Glaser, F. Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. In Proceedings of the Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 4–7 January 2017. https://doi.org/10.24251/hicss.2017.186.
5. Pereira, J.; Tavalaei, M.M.; Ozalp, H. Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technol. Forecast. Soc. Chang.* **2019**, *146*, 94–102. https://doi.org/10.1016/j.techfore.2019.04.030.
6. Liu, Y.; Lu, Q.; Zhu, L.; et al. A systematic literature review on blockchain governance. *J. Syst. Softw.* **2023**, *197*, 111576. https://doi.org/10.1016/j.jss.2022.111576.
7. Toufaily, E.; Zalan, T. In blockchain we trust? Demystifying the trust mechanism in blockchain ecosystems. *Technol. Forecast. Soc. Chang.* **2024**, *206*, 123574. https://doi.org/10.1016/j.techfore.2024.123574.
8. De Filippi, P.; Mannan, M.; Reijers, W. Blockchain as a confidence machine: The problem of trust and challenges of governance. *Technol. Soc.* **2020**, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284.

9. Belchior, R.; Süßenguth, J.; Feng, Q.; et al. A brief history of blockchain interoperability. *Commun. ACM* **2024**, *67*, 62–69. https://doi.org/10.1145/3648607.
10. Lumineau, F.; Wang, W.; Schilke, O. Blockchain Governance—A New Way of Organizing Collaborations? *Organ. Sci.* **2021**, *32*, 500–521. https://doi.org/10.1287/orsc.2020.1379.
11. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology, Zug, Switzerland, 20–22 June 2018; pp. 45–54. https://doi.org/10.1109/cvcbt.2018.00011.
12. Zhang, Y.; Kasahara, S.; Shen, Y.; et al. Smart contract-based access control for the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 1594–1605. https://doi.org/10.1109/jiot.2018.2847705.
13. Nofer, M.; Gomber, P.; Hinz, O.; et al. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187. https://doi.org/10.1007/s12599-017-0467-3.
14. Catalini, C.; Gans, J.S. Some simple economics of the blockchain. *Commun. ACM* **2020**, *63*, 80–90. https://doi.org/10.1145/3359552.
15. Yao, W.; Du, W.; Gu, J.; et al. Establishing a baseline for evaluating blockchain-based self-sovereign identity systems. In Proceedings of the BIOTC 2024, Fukuoka, Japan, 19–21 July 2024; pp. 108–119. https://doi.org/10.1145/3688225.3688239.
16. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer, 2019. https://doi.org/10.1007/978-3-030-03035-3.
17. Hardjono, T.; Smith, N. Decentralized Trusted Computing Base for Blockchain Infrastructure Security. *Front. Blockchain* **2019**, *2*, 24. https://doi.org/10.3389/fbloc.2019.00024.
18. Narayanan, A.; Bonneau, J.; Felten, E.; et al. *Bitcoin and Cryptocurrency Technologies*; Princeton University Press: Princeton, NJ, USA, 2016.
19. Shin, D.D.H. Blockchain: The emerging technology of digital trust. *Telemat. Inform.* **2019**, *45*, 101278. https://doi.org/10.1016/j.tele.2019.101278.
20. Becker, M.; Bodó, B. Trust in blockchain-based systems. *Internet Policy Rev.* **2021**, *10*, 1–10. https://doi.org/10.14763/2021.2.1555.
21. Hawlitschek, F.; Notheisen, B.; Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* **2018**, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005.
22. Islam, R.; Bose, R.; Roy, S.; et al. Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model. *Sci. Rep.* **2025**, *15*, 23454. https://doi.org/10.1038/s41598-025-06405-y.
23. Frizzo-Barker, J.; Chow-White, P.A.; Adams, P.R.; et al. Blockchain as a disruptive technology for business: A systematic review. *Int. J. Inf. Manag.* **2020**, *51*, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014.
24. Werbach, K. Trust, but verify: Why the blockchain needs the law. *Berkeley Technol. Law J.* **2018**, *33*, 487–550. https://doi.org/10.15779/Z38H41JM9N.
25. Risius, M.; Spohrer, K. A Blockchain Research Framework—What We (don't) Know, Where We Go from Here, and How We Will Get There. *Bus. Inf. Syst. Eng.* **2017**, *59*, 385–409. https://doi.org/10.1007/s12599-017-0506-0.
26. Lemieux, V.L. Trusting records: Is Blockchain technology the answer? *Rec. Manag. J.* **2016**, *26*, 110–139. https://doi.org/10.1108/rmj-12-2015-0042.
27. Xu, J.J.; Weber, I.; Staples, M. Trust in the machine: Blockchain as a socio-technical trust infrastructure. In Proceedings of the HICSS, Maui, HI, USA 8–11 January 2019.
28. Wang, W.; Hoang, D.T.; Hu, P.; et al. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. https://doi.org/10.1109/access.2019.2896108.
29. Wang, S.; Ouyang, L.; Yuan, Y.; et al. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019a**, *49*, 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123.
30. De Filippi, P.; Hassan, S. Blockchain technology as a regulatory technology: From code is law to law is code. *arXiv* **2018**, arXiv:1801.02507.
31. Alharby, M.; van Moorsel, A. Blockchain-based smart contracts: A systematic mapping study. *arXiv* **2017**, arXiv:1710.06372.
32. Mendling, J.; Weber, I.; van der Aalst, W.; et al. Blockchains for Business Process Management—Challenges and Opportunities. *ACM Trans. Manag. Inf. Syst.* **2018**, *9*, 4:1–4:16. https://doi.org/10.1145/3183367.
33. De Filippi, P.; Wright, A. *Blockchain and the Law: The Rule of Code*; Harvard University Press: Cambridge, MA, USA, 2018. https://doi.org/10.4159/9780674985933.
34. Singh, R.; Gupta, A.; Mittal, P. A Systematic Literature Review on Blockchain-based Smart Contracts: Platforms, Applications, and Challenges. *Distrib. Ledger Technol. Res. Pract.* **2026**, *5*, 1–36. https://doi.org/10.1145/3704741.

35. Ante, L. Smart contracts on the blockchain: A bibliometric analysis and review. *Telemat. Inform.* **2021**, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519.
36. Khan, M.A.; Salah, K.; Ioannidis, S.; et al. Blockchain for Internet of Things: Applications, challenges, and opportunities. *Comput. Netw.* **2021a**, *194*, 108141. https://doi.org/10.1016/j.comnet.2021.108141.
37. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; et al. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-Peer Netw. Appl.* **2021b**, *14*, 2901–2925. https://doi.org/10.1007/s12083-021-01127-0.
38. Luu, L.; Chu, D.H.; Olickel, H.; et al. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 254–269. https://doi.org/10.1145/2976749.2978309.
39. Nikolic, I.; Kolluri, A.; Sergey, I.; et al. Finding the greedy, prodigal, and suicidal contracts at scale. In Proceedings of the 34th Annual Computer Security Applications Conference, San Juan, Puerto Rico, 3–7 December 2018; pp. 653–663. https://doi.org/10.1145/3274694.3274743.
40. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on Ethereum smart contracts (SoK). In *Principles of Security and Trust*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 164–186. https://doi.org/10.1007/978-3-662-54455-6_8.
41. Mense, A.; Flatscher, M. Security vulnerabilities in Ethereum smart contracts. In Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & Services, Yogyakarta, Indonesia, 19–21 November 2018; pp. 375–380. https://doi.org/10.1145/3282373.3282419.
42. Vigliotti, M.G. What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts. *Front. Blockchain* **2021**, *3*, 553671. https://doi.org/10.3389/fbloc.2020.553671.
43. Capocasale, V.; Perboli, G. Standardizing Smart Contracts. *IEEE Access* **2022**, *10*, 91203–91212. https://doi.org/10.1109/access.2022.3202550.
44. Taherdoost, H. Smart contracts in blockchain technology: A critical review. *Information* **2023**, *14*, 117. https://doi.org/10.3390/info14020117.
45. Kadioglu Kumtepe, C.C. Unpacking the technology of trust: Establishing trust and fairness in online dispute resolution through blockchain and smart contracts. *Int. J. Law Inf. Technol.* **2025**, *33*, eaaf017. https://doi.org/10.1093/ijlit/eaaf017.
46. Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain. Manag. Int. J.* **2018**, *23*, 545–559. https://doi.org/10.1108/scm-01-2018-0029.
47. Schardong, F.; Custódio, R. Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors* **2022**, *22*, 5641. https://doi.org/10.3390/s22155641.
48. Ferdous, M.S.; Chowdhury, F.; Alassafi, M.O. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* **2019**, *7*, 103059–103079. https://doi.org/10.1109/access.2019.2931173.
49. Zaeem, R.N.; Barber, K.S. Blockchain-based self-sovereign identity: Survey, requirements, use cases, and comparative study. *IEEE Internet Things J.* **2021**, *8*, 4316–4336. https://doi.org/10.1109/jiot.2020.3032479.
50. Ou, H.H.; Chen, G.Y.; Lin, I.C. A Self-Sovereign Identity Blockchain Framework for Access Control and Transparency in Financial Institutions. *Cryptography* **2025**, *9*, 9. https://doi.org/10.3390/cryptography9010009.
51. Nair, A.J.; Manohar, S.; Rao, A.B.S. Self sovereign identity in e-governance: Blockchain solutions for fintech compliance and citizen-centric financial services. *Humanit. Soc. Sci. Commun.* **2025**, *12*, 1562. https://doi.org/10.1057/s41599-025-05880-y.
52. Al-Bassam, M. SCPKI: A smart contract-based PKI and identity system. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 35–40. https://doi.org/10.1145/3055518.3055530.
53. Pava-Díaz, R.A.; Gil-Ruiz, J.; López-Sarmiento, D.A. Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation. *Front. Blockchain* **2024**, *7*, 1443362. https://doi.org/10.3389/fbloc.2024.1443362.
54. Puthal, D.; Malik, N.; Mohanty, S.P.; et al. The Blockchain as a Decentralized Security Framework [Future Directions]. *IEEE Consum. Electron. Mag.* **2018**, *7*, 18–21. https://doi.org/10.1109/mce.2017.2776459.
55. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; et al. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. https://doi.org/10.1080/00207543.2018.1533261.
56. Queiroz, M.M.; Fosso Wamba, S.; De Bourmont, M.; et al. Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. *Int. J. Prod. Res.* **2021**, *59*, 6087–6103. https://doi.org/10.1080/00207543.2020.1803511.

57. Malgonde, O.S.; Padmanabhan, B.; Mithas, S. How to Mitigate Misinformation Diffusion on Blockchain-Based Decentralized Social Network Platforms? Insights From an Agent-Based Simulation Model. *J. Oper. Manag.* **2025**, *71*, 1068–1084. https://doi.org/10.1002/joom.70007.
58. Kausar, F.; Asif, H.M.; Hussain, S.; et al. A Review on Blockchain-Based Trust and Reputation Schemes in Metaverse Environments. *Cryptography* **2025**, *9*, 74. https://doi.org/10.3390/cryptography9040074.
59. Deng, W.; Huang, T.; Wang, H. A Review of the Key Technology in a Blockchain Building Decentralized Trust Platform. *Mathematics* **2023**, *11*, 101. https://doi.org/10.3390/math11010101.
60. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; et al. A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv.* **2021**, *54*, 168. https://doi.org/10.1145/3471140.
61. Zheng, Z.; Xie, S.; Dai, H.; et al. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. https://doi.org/10.1109/bigdatacongress.2017.85.
62. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. https://doi.org/10.1109/access.2019.2936094.
63. Pournader, M.; Shi, Y.; Seuring, S.; et al. Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *Int. J. Prod. Res.* **2020**, *58*, 2063–2081. https://doi.org/10.1080/00207543.2019.1650976.
64. Kotey, S.D.; Tchao, E.T.; Ahmed, A.R.; et al. Blockchain interoperability: The state of heterogeneous blockchain-to-blockchain communication. *IET Commun.* **2023**, *17*, 891–914. https://doi.org/10.1049/cmu2.12594.
65. Ren, K.; Ho, N.M.; Loghin, D.; et al. Interoperability in blockchain: A survey. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 12750–12769. https://doi.org/10.1109/tkde.2023.3275220.
66. Qasse, I.A.; Abu Talib, M.; Nasir, Q. Inter blockchain communication: A survey. In Proceedings of the 6th Annual International Conference on Arab Women in Computing, ArabWIC 2019, Rabat, Morocco, 7–9 March 2019; pp. 2:1–2:6. https://doi.org/10.1145/3333165.3333167.
67. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; et al. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet Things J.* **2021**, *8*, 881–888. https://doi.org/10.1109/jiot.2020.3008906.
68. Lin, S.Y.; Zhang, L.; Li, J.; et al. A survey of application research based on blockchain smart contract. *Wirel. Netw.* **2022**, *28*, 635–690. https://doi.org/10.1007/s11276-021-02874-x.
69. Wang, Y.; Han, J.H.; Beynon-Davies, P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain. Manag.* **2019b**, *24*, 62–84. https://doi.org/10.1108/scm-03-2018-0148.
70. Anthony Jnr, B. Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise-a standardized architecture perspective. *Enterp. Inf. Syst.* **2024**, *18*, 2296647. https://doi.org/10.1080/17517575.2023.2296647.
71. Wang, G.; Wang, Q.; Chen, S. Exploring blockchains interoperability: A systematic survey. *ACM Comput. Surv.* **2023**, *55*, 1–38. https://doi.org/10.1145/3582882.
72. Herlihy, M. Blockchains from a distributed computing perspective. *Commun. ACM* **2019**, *62*, 78–85. https://doi.org/10.1145/3209623.
73. Lin, I.C.; Liao, T.C. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. https://doi.org/10.6633/ijns.201709.19(5).01.
74. Li, W.; Liu, Z.; Chen, J.; et al. Towards blockchain interoperability: A comprehensive survey on cross-chain solutions. *Blockchain Res. Appl.* **2025**, *6*, 100286. https://doi.org/10.1016/j.bcra.2025.100286.
75. Siam, M.K.; Saha, B.; Hasan, M.M.; et al. Securing decentralized ecosystems: A comprehensive systematic review of blockchain vulnerabilities, attacks, and countermeasures and mitigation strategies. *Future Internet* **2025**, *17*, 183. https://doi.org/10.3390/fi17040183.
76. Kou, G.; Lu, Y. FinTech: A literature review of emerging financial technologies and applications. *Financ. Innov.* **2025**, *11*, 1–34. https://doi.org/10.1186/s40854-024-00668-6.
77. Li, X.; Jiang, P.; Chen, T.; et al. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020.
78. Gervais, A.; Karame, G.O.; Wüst, K.; et al. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16. https://doi.org/10.1145/2976749.2978341.
79. Viriyasitavat, W.; Xu, L.D.; Bi, Z.; et al. Blockchain technology for applications in Internet of Things: Mapping from system design perspective. *IEEE Internet Things J.* **2019**, *6*, 8155–8168. https://doi.org/10.1109/jiot.2019.2925825.

80. Caldarelli, G.; Ellul, J. The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach. *Appl. Sci.* **2021**, *11*, 7572. https://doi.org/10.3390/app11167572.
81. Liu, Y.; He, J.; Li, X.; et al. An overview of blockchain smart contract execution mechanism. *J. Ind. Inf. Integr.* **2024**, *41*, 100674. https://doi.org/10.1016/j.jii.2024.100674.
82. Dixit, A.; Singh, A.; Rahulamathavan, Y.; et al. FAST DATA: A Fair, Secure, and Trusted Decentralized IIoT Data Marketplace Enabled by Blockchain. *IEEE Internet Things J.* **2023**, *10*, 2934–2944. https://doi.org/10.1109/jiot.2021.3120640.
83. Schmeelk, S.; Kanabar, M.; Peterson, K.; et al. Electronic health records and blockchain interoperability requirements: A scoping review. *JAMIA Open* **2022**, *5*, ooac068. https://doi.org/10.1093/jamiaopen/ooac068.
84. Durneva, P.; Cousins, K.; Chen, M. The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review. *J. Med. Internet Res.* **2020**, *22*, e18619. https://doi.org/10.2196/18619.
85. Yli-Huumo, J.; Ko, D.; Choi, S.; et al. Where is current research on blockchain technology? A systematic review. *PLoS ONE* **2016**, *11*, e0163477. https://doi.org/10.1371/journal.pone.0163477.
86. Allen, R.H.; Sriram, R.D. The role of standards in innovation. *Technol. Forecast. Soc. Chang.* **2000**, *64*, 171–181. https://doi.org/10.1016/s0040-1625(99)00104-3.
87. Hughes, L.; Dwivedi, Y.K.; Misra, S.K.; et al. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005.
88. Jia, X.; Xu, J.; Han, M.; et al. International Standardization of Blockchain and Distributed Ledger Technology: Overlaps, Gaps and Challenges. *Comput. Model. Eng. Sci.* **2023**, *137*, 1491–1523. https://doi.org/10.32604/cmes.2023.026357.
89. De Filippi, P.; Wray, C.; Sileno, G. Smart contracts. *Internet Policy Rev.* **2021**, *10*, 1549. https://doi.org/10.14763/2021.2.1549.
90. Kud, A. Decentralized information platforms in public governance: Reconstruction of the modern democracy or comfort blinding? *Int. J. Public Adm.* **2023**, *46*, 195–221. https://doi.org/10.1080/01900692.2021.1993905.
91. Cong, L.W.; He, Z.; Li, J. Decentralized mining in centralized pools. *Rev. Financ. Stud.* **2021a**, *34*, 1191–1235. https://doi.org/10.1093/rfs/hhaa040.
92. Lacity, M.; Khan, S.; Yan, A. Review of the empirical business services literature on blockchain. *J. Strateg. Inf. Syst.* **2021**, *30*, 101663. https://doi.org/10.1016/j.jsis.2021.101663.
93. Hoffmann, I.; Jensen, N.; Cristescu, A. Decentralized governance for digital platforms: Architecture proposal for the mobility market to enhance data privacy and market diversity. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021. https://doi.org/10.1109/ccnc49032.2021.9369659.
94. Azaria, A.; Ekblaw, A.; Vieira, T.; et al. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data, Vienna, Austria, 22–24 August 2016; pp. 25–30. https://doi.org/10.1109/obd.2016.11.
95. Chen, Y.; Richter, J.I.; Patel, P.C. Decentralized governance of digital platforms. *J. Manag.* **2021**, *47*, 1305–1337. https://doi.org/10.1177/0149206320916755.
96. Reijers, W.; Wuisman, I.; Mannan, M.; et al. Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi* **2018**, *37*, 157–172. https://doi.org/10.1007/s11245-018-9626-5.
97. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2084–2123. https://doi.org/10.1109/comst.2016.2535718.
98. Reijers, W.; O'Brolcháin, F.; Haynes, P. Governance in Blockchain Technologies & Social Contract Theories. *Ledger* **2016**, *1*, 134–151. https://doi.org/10.5195/ledger.2016.62.
99. Atzori, M. Blockchain technology and decentralized governance: Is the state still necessary? *J. Gov. Regul.* **2017**, *6*, 45–62. https://doi.org/10.22495/jgr_v6_i1_p5.
100. Beck, R.; Müller-Bloch, C.; King, J.L. Governance in the Blockchain Economy: A Framework and Research Agenda. *J. Assoc. Inf. Syst.* **2018**, *19*, 1020–1034. https://doi.org/10.17705/1jais.00518.
101. Abbas, A.; Jain, S.; Hegde, N. Blockchain and IoT security: A survey. *IEEE Access* **2021**, *9*, 85386–85413. https://doi.org/10.1109/access.2021.3087282.
102. Cong, L.W.; Li, Y.; Wang, N. Tokenomics: Dynamic adoption and valuation. *Rev. Financ. Stud.* **2021b**, *34*, 1105–1155. https://doi.org/10.1093/rfs/hhaa089.

103. Santana, C.; Albareda, L. Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. *Technol. Forecast. Soc. Chang.* **2022**, *182*, 121806. https://doi.org/10.1016/j.techfore.2022.121806.
104. Bellavitis, C.; Fisch, C.; Momtaz, P.P. The rise of decentralized autonomous organizations (DAOs): A first empirical glimpse. *Ventur. Cap.* **2023**, *25*, 187–203. https://doi.org/10.1080/13691066.2022.2116797.
105. Rikken, O.K.; Janssen, M.F.W.H.A.; Roosenboom-Kwee, Z. Governance impacts of blockchain-based decentralized autonomous organizations: An empirical analysis. *Policy Des. Pract.* **2023**, *6*, 465–487. https://doi.org/10.1080/25741292.2023.2270220.
106. Ding, W.; Liang, X.; Hou, J.; et al. A novel approach for predictable governance of decentralized autonomous organizations based on parallel intelligence. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 3092–3103. https://doi.org/10.1109/tsmc.2022.3224250.
107. Schädler, L.; Lustenberger, M.; Spychiger, F. Analyzing decision-making in blockchain governance. *Front. Blockchain* **2023**, *6*, 1256651. https://doi.org/10.3389/fbloc.2023.1256651.
108. Nguyen, L.T.M.; Nguyen, P.T. The interplay between governance mechanisms of blockchain platforms. *Econ. Innov. New Technol.* **2025**, *34*, 367–391. https://doi.org/10.1080/10438599.2024.2346723.
109. Vella, G.; Gastaldi, L.; Appio, F.P. Non-algorithmic governance mechanisms of blockchain-based decentralized applications: Evidence from multiple cases. *Technovation* **2025**, *148*, 103332. https://doi.org/10.1016/j.technovation.2025.103332.
110. Singh, S.; Gaur, A.; Singh, D. Blockchain-based governance: Implications for organizational boundaries and structures. *Br. J. Manag.* **2024**, *35*, 1692–1699. https://doi.org/10.1111/1467-8551.12784.
111. Bendig, D.; Charlet, M. Opportunities and challenges of blockchain for multi-sided platforms. *Electron. Mark.* **2025**, *35*, 25. https://doi.org/10.1007/s12525-025-00765-z.
112. Kolade, O.; Adepoju, D.; Adegbile, A. Blockchains and the disruption of the sharing economy value chains. *Strateg. Chang.* **2022**, *31*, 137–145. https://doi.org/10.1002/jsc.2483.
113. Heimburg, V.; Alakbarov, H.; Wiesche, M. Governance of decentralized platform ecosystems. In *Transforming the Digitally Sustainable Enterprise*; Springer: Cham, Switzerland, 2025; Volume 3, pp. 97–112. https://doi.org/10.1007/978-3-031-80125-9_6.
114. Fasano, F.; Bartoli, C.; Cappa, F.; et al. Exploring the impact of AI on Web3 decentralized platform business model innovation. *J. Eng. Technol. Manag.* **2025**, *78*, 101911. https://doi.org/10.1016/j.jengtecman.2025.101911.
115. Diaz-Valdivia, A.; Poblet-Balcell, M. The governance of the ReFi ecosystem: Integrity in voluntary carbon markets as a common resource. *Int. J. Commons* **2025**, *19*, 100–119. https://doi.org/10.5334/ijc.1410.
116. Peck, M.E. Blockchain world—Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectr.* **2017**, *54*, 38–60. https://doi.org/10.1109/mspec.2017.8048838.
117. Yermack, D. Corporate governance and blockchains. *Rev. Financ.* **2017**, *21*, 7–31. https://doi.org/10.1093/rof/rfw074.
118. Sarker, I.; Datta, B. Re-designing the pension business processes for achieving technology-driven reforms through blockchain adoption: A proposed architecture. *Technol. Forecast. Soc. Chang.* **2022**, *174*, 121059. https://doi.org/10.1016/j.techfore.2021.121059.
119. Xie, J.; Tang, H.; Huang, T.; et al. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2794–2830. https://doi.org/10.1109/comst.2019.2899617.
120. Zouari, M.; Alon, I.; Shtudiner, Z. Ethereum: Past, present, and future. *J. Glob. Inf. Manag.* **2025**, *33*, 1–24. https://doi.org/10.4018/jgim.383938.
121. Gatteschi, V.; Lamberti, F.; Demartini, C.; et al. To Blockchain or Not to Blockchain: That Is the Question. *IT Prof.* **2018**, *20*, 62–74. https://doi.org/10.1109/mitp.2018.021921652.
122. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006.
123. Zheng, Z.; Xie, S.; Dai, H.; et al. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. https://doi.org/10.1504/ijwgs.2018.095647.
124. Treiblmaier, H. Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. *Front. Blockchain* **2019**, *2*, 3. https://doi.org/10.3389/fbloc.2019.00003.
125. Polcumpally, A.T.; Pandey, K.K.; Kumar, A.; et al. Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions. *Heliyon* **2024**, *10*, e32975. https://doi.org/10.1016/j.heliyon.2024.e32975.