Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.077332

REVIEW

A Survey of Multi-Blockchain: Architectures, Technologies, and Applications

Tsu-Yang Wu[1], Yehai Xue[1], Haonan Li[2], Saru Kumari[3] and Lip Yee Por[2,*]

[1]School of Artificial Intelligence/School of Future Technology, Nanjing University of Information Science and Technology, Nanjing, China

[2]Faculty of Computer Science and Information Technology, University Malaya, Kuala Lumpur, Malaysia

[3]Department of Mathematics, Chaudhary Charan Singh University, Meerut, India

*Corresponding Author: Lip Yee Por. Email: porlip@um.edu.my

Received: 07 December 2025; Accepted: 13 February 2026; Published: 09 April 2026

ABSTRACT: Blockchain technology, characterized by decentralization, transparency, and immutability, has been widely applied in areas such as supply chain tracking, medical data management, and the Internet of Things. However, single blockchain systems suffer from limitations in performance, scalability, and cross-chain interoperability, giving rise to the issue of "blockchain silos." To address the challenges of data and asset circulation among heterogeneous blockchain networks, both academia and industry have proposed multi-blockchain architectures. In this paper, we categorize current multi-blockchain systems from a network topology perspective into four types: parallel architecture, hierarchical architecture, hybrid architecture, and multi-blockchain networks. We systematically review the main cross-chain technologies, including main/side chains, relay chains, bridge nodes, cross-chain smart contracts, and hash time-locks. Furthermore, we summarize representative applications such as data exchange, transaction validation, medical data management, supply chain traceability, and IoT management. Finally, we also identify challenges, like cross-chain security, consensus compatibility, resource overhead, and decentralized coordination mechanisms. Meanwhile, we discuss future works, including lightweight relay networks, zero-knowledge proofs, modular chain architectures, and reinforcement learning-based scheduling. Through multi-dimensional technical analysis, we provide a systematic survey for the theoretical study and applications of multi-blockchain, facilitating the usage of multi-blockchain in the digital economy and trusted collaboration contexts.

KEYWORDS: Multi-blockchain; cross-chain technology; smart contracts; hash time-locked contracts

1 Introduction

Blockchain technology [1], with its inherent features of openness and immutability, serves as the foundation for distributed systems and has garnered increasing attention from researchers, enterprises, and industries. With the ongoing advancement of blockchain research, the technology has found applications in nearly every sector, including but not limited to supply chain tracing [2–4], healthcare [5,6], and IoT management [7–9]. As a distributed ledger technology, each block on a blockchain is cryptographically linked to its successor via hash values and appended to the ledger through consensus mechanisms such as Proof of Work (PoW) [10], Proof of Stake (PoS) [11], and Practical Byzantine Fault Tolerance (PBFT) [12]. Additionally, the integration of smart contracts enhances programmability and automates digital transactions.

As blockchain technology rapidly evolves, different platforms exhibit diverse designs and implementations, leading to challenges in direct data exchange and asset transfers, known as the "blockchain silo" problem [13]. The inherent limitations of single blockchain architectures in scalability, performance,

Copyright © 2026 The Authors. Published by Tech Science Press. This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

and functionality have become increasingly apparent [14]. In response, both academia and industry have developed various cross-chain solutions to achieve interoperability among disparate blockchains [15,16]. The Multi-Blockchain architecture has emerged as a novel paradigm, enabling the coexistence, collaboration, and exchange of data and assets across heterogeneous blockchain systems [17–19].

This study focuses on the technological underpinnings of Multi-Blockchain systems, examining them from the perspectives of network topology, cross-chain interoperability, and application domains. It also explores the challenges and potential research directions of Multi-Blockchain systems. The main contributions of this paper are as follows:

1 Topology-Based Taxonomy: We propose a novel taxonomy based on network topology (Parallel, Hierarchical, Hybrid, and Mesh) to systematically elucidate the evolutionary logic and structural distinctions of multi-chain architectures. This framework effectively resolves the issue of ambiguous classification boundaries prevalent in existing literature.
2 Trust-Centric Critical Analysis: Unlike previous surveys that merely enumerate technologies, we conduct a rigorous classification of cross-chain protocols into Trusted, Trust-minimized, and Trustless paradigms. We provide an in-depth dissection of the security assumptions and potential risks associated with each category, such as the centralization dilemmas inherent in relay chain structures.
3 Maturity-Aware Application Review: Beyond summarizing application scenarios, we establish a maturity assessment framework. This allows us to clearly distinguish between deployed production-grade systems (e.g., asset bridging) and academic prototypes still in the exploratory phase (e.g., healthcare privacy sharing), providing a pragmatic baseline for future research.
4 Prospects with Concrete Mechanisms: We identify Modular Data Availability Layers and Reinforcement Learning-based Dynamic Scheduling as pivotal research directions for addressing the scalability and efficiency bottlenecks in contemporary multi-chain ecosystems.

The remainder of this paper is structured as follows: Section 2 introduces the architecture of Multi-Blockchain systems. Section 3 reviews cross-chain technologies and interoperability mechanisms. Section 4 summarizes application scenarios. Section 5 discusses current challenges and future directions. Finally, Section 6 concludes the paper. The overall architecture is illustrated in Fig. 1.

2 Architectures of Multi-Blockchain Systems

Based on the network topology of mainstream Multi-Blockchain frameworks, as illustrated in Fig. 2, we classify Multi-Blockchain architectures into four categories: Parallel Blockchain Architectures [20,21], Hierarchical Blockchain Architectures [22,23], Hybrid Blockchain Architectures [6,24], and Multi-Blockchain Networks [25,26]. Each category is discussed in detail below.

It is important to note that the four architectural classifications discussed above are primarily idealized models based on network topology logic. In practical engineering deployments, the boundaries between these architectures are often blurred. For instance, the leaf layer of a hierarchical architecture may contain multiple sub-chains operating in parallel, while localized sections of a multi-chain network may exhibit transient hierarchical control relationships. Therefore, we conceptualize these classifications as 'archetypes' for understanding multi-chain systems, rather than as mutually exclusive physical implementations.

In order to systematically sort out the research status and development trend of multi-blockchain related technologies, this study is based on the IEEE Electronic Library (IEL), SCIE, ESI and Elsevier Science Direct databases. Combined with high-frequency association terms such as "Consensus Mechanism", "Cross-Chain Communication" and "Smart Contract", high-quality papers related to multi-blockchain in the past five years are retrieved as the theoretical basis source for reference in this paper. And by reading each paper, label

records are made for each paper according to: multi-blockchain architecture, cross-blockchain technology, application background of the paper, and shortcomings, and the knowledge graph is generated by Obsidian software (as shown in Fig. 3).

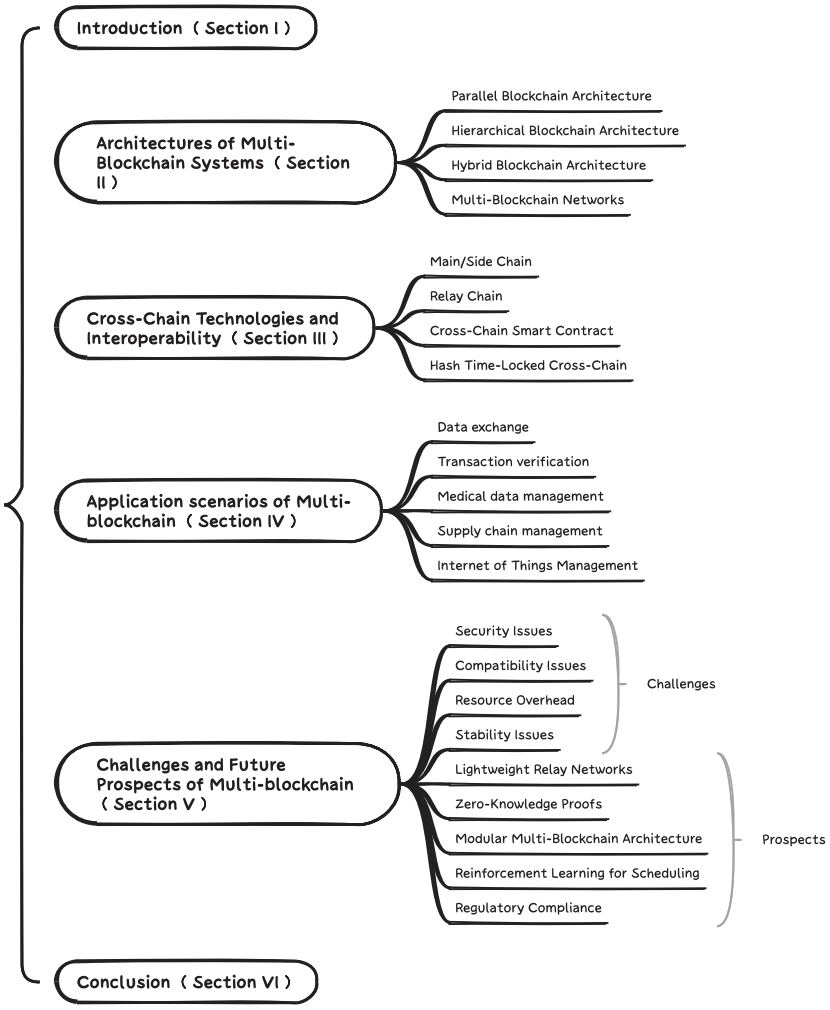

Figure 1: Overall architecture.

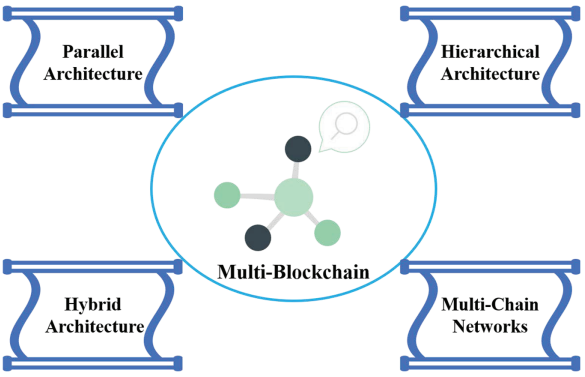

Figure 2: Classification of multi-blockchain architecture.

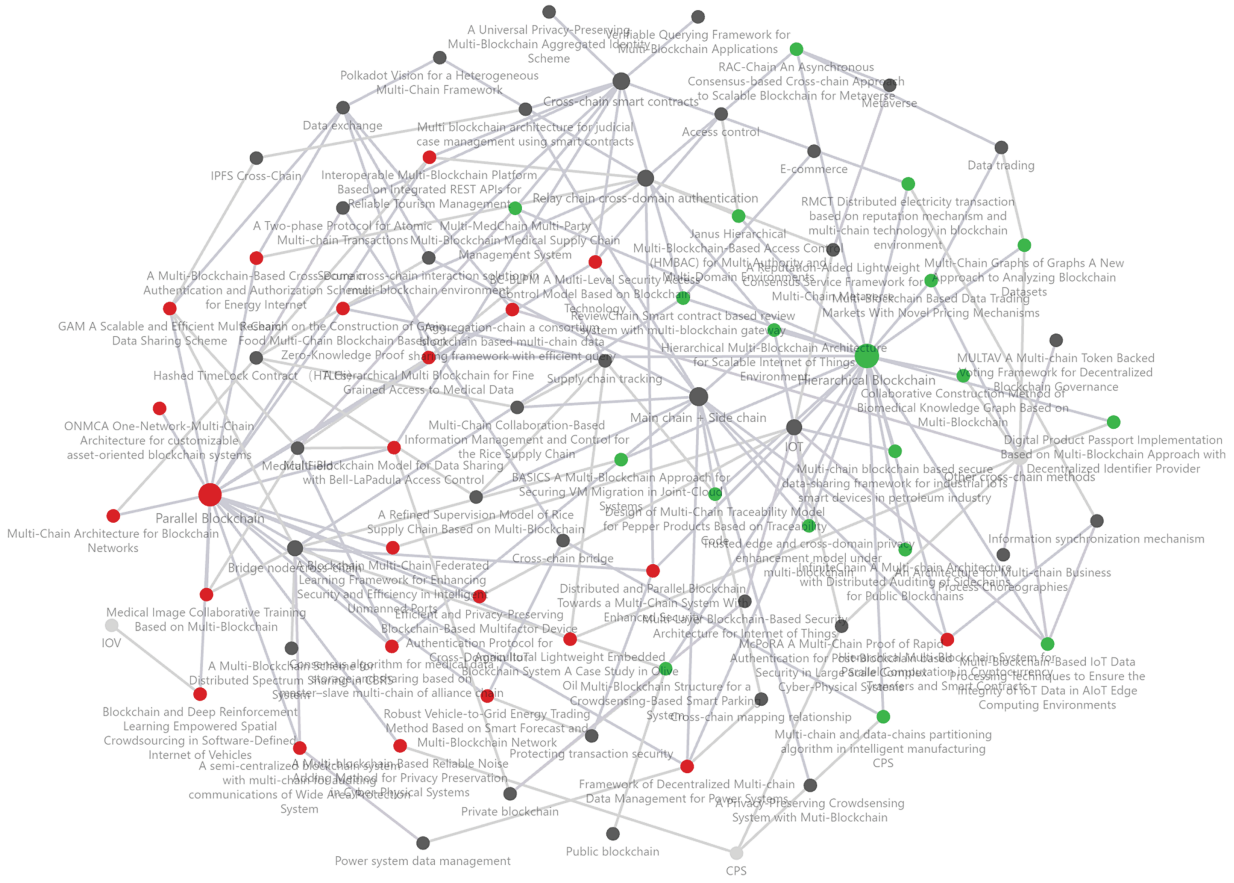

Figure 3: Knowledge graph among Multi-blockchain papers.

Fig. 3 presents the topics of multi-blockchain with the association network. For example, the clustering of red nodes represents all multi-blockchain algorithms using hierarchical architecture, and the connected nodes are the information of related papers. The cluster of green nodes represents papers that adopt parallel blockchain architectures. It can also be seen from the figure that a correlation between cross-chain technology and multi-blockchain architecture. The multi-blockchain related content summarized in this paper is not independent, and different cross-chain technologies and system architectures can be integrated to design the algorithm. Then it systematically reveals the research hotspots, technical difficulties and application directions in the field of multi-blockchain. Their clustering structure and connection strength provide visual evidence for related conclusions. On the one hand, the high density of connections of related multi-chain technologies indicates their dominance. On the other hand, the emergence of edge nodes also hints at the potential of emerging directions.

2.1 Parallel Blockchain Architecture

The Parallel Blockchain Architecture refers to the deployment of multiple functionally similar yet independent blockchains that operate concurrently to achieve system load balancing. As shown in Fig. 4, there can exist multiple entities a, b, c in system A, which belong to the level relation among themselves and together form system A. Communication channels are allowed between entities, but they exist independently of each other in the architecture. On this basis, the parallel blockchain structure is to establish its corresponding blockchain for each entity, and the blockchain here allows the use of different blockchain types to

adapt to different needs. For the whole system, the structure still belongs to the multi-blockchain structure, but for different blockchains, the correlation between them is not strong. The parallel blockchain structure is suitable for application in the management of different power enterprises in smart grid, the management of different medical institutions in the medical field, and the management of different trading platforms in cross-chain transactions.

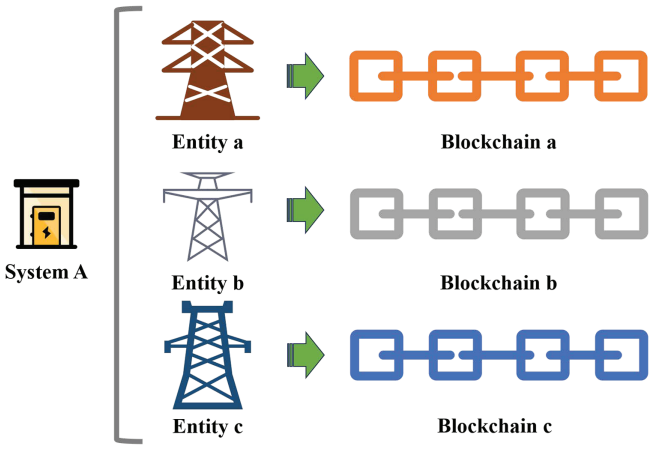

Figure 4: Parallel blockchain structure diagram.

For instance, the ONMCA architecture [27] enables customized digital asset management by establishing several independent blockchains within a single network—using a state chain for asset management and a contract chain for script execution. Zhang et al. [28] proposed separate blockchains for different IIoT domains to store domain-specific information and facilitate cross-domain authentication. Wang et al. [29] proposed individual blockchains for each participating entity in the Frequency Regulation Market (FRM). Although these blockchains are not entirely isolated and support basic data sharing, the entities they represent remain relatively independent from a structural perspective. The STEB system [30] applies two consortium blockchains separately for service provider authorization and transaction data publication, thereby decentralizing traditional service platforms. Liang et al. [31] introduced V2GFTN, a decentralized smart system connecting energy suppliers, consumers, and campus-based V2G networks via parallel blockchain architectures. Several studies adopt similar parallel architectures in semi-supervised learning [32] and blockchain systems [33,34]. Additionally, Refs. [35–37] have explored related topologies in multi-task and medical applications. These are not elaborated here due to similarity in architecture.

2.2 Hierarchical Blockchain Architecture

Not all Multi-Blockchain systems are composed of mutually independent chains; some feature hierarchical relationships among blockchains. As shown in Fig. 5, the entities in the system are distinguished as upstream entity A, midstream entity B, and downstream entity C. Upstream, midstream and downstream can be understood as a hierarchical management system in a scenario. A related operation can be performed on a midstream entity in a record of an upstream entity and a related operation can be performed on a downstream entity in a record of a midstream entity. The blockchains corresponding to entities at different levels also have corresponding hierarchical relationships to realize the relevance between entities required in specific scenarios. The hierarchical blockchain structure is suitable for the following scenarios: in the supply chain tracking task, for the origin, processing, sales of raw materials and so on. The management of

background operating systems for Internet of Things (IoT) devices; In the power system, the management of power transmission equipment and power consumption entities in power supply enterprises.

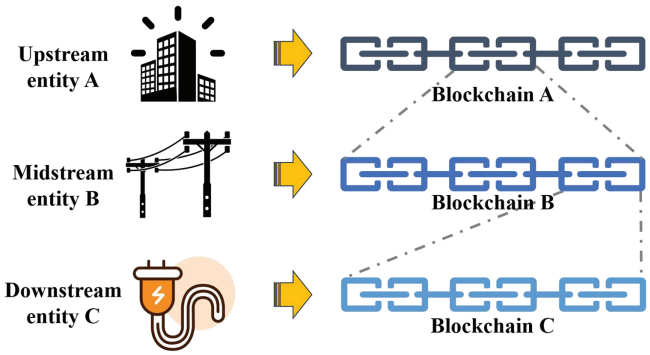

Figure 5: Hierarchical blockchain structure diagram.

For example, the RAC-Chain model [38] introduces an asynchronous consensus-based consortium blockchain, in which a relay chain handles gateway transmission and simplified payment verification, while lower-level application chains provide services to the metaverse environment. Saini et al. [5] designed a multi-layered blockchain framework for the healthcare supply chain, including user, local, and global chain layers. The local layer manages the full supply lifecycle—raw materials, production, transportation, distribution—while the global layer facilitates transaction validation and dynamic control among stakeholders. Li et al. [39] applied a hierarchical architecture in cyber-physical systems (CPS) using a communication chain to interconnect multiple data chains, which improved system concurrency and reduced storage requirements compared to traditional single-chain designs. Similar hierarchical approaches are found in other works [40–44]. Although hierarchical Multi-Blockchain architectures offer adaptability to various application scenarios, they often require cross-layer communication protocols and interchain mechanisms to facilitate interaction across different layers. These cross-chain technologies are discussed in Section 3.

2.3 Hybrid Blockchain Architecture

Some Multi-Blockchain designs combine both parallel and hierarchical architectures. Typically, the interaction process is divided into hierarchical levels, within which parallel chains are deployed for specific entities. For instance, Malamas et al. [45] proposed a fine-grained access control model using an intermediary blockchain as a proxy to manage multiple parallel domain-specific blockchains. The proxy chain serves as the access interface for users, while the domain chains correspond to specific application areas such as healthcare, supply chains, and energy. All transactions on domain chains are synchronized and verified via the proxy chain, ensuring global trust and immutability. In similar healthcare data exchange scenarios, a relay proxy blockchain is used to manage multiple parallel domain chains. In the power systems domain, Kong et al. [24] proposed a Multi-Blockchain architecture that partitions the system into autonomous blockchain subsystems. These subsystems, while initially independent, allow for dynamic network restructuring to optimize hierarchical organization.

2.4 Multi-Blockchain Networks

A distinctive category of Multi-Blockchain systems involves the integration of token relationships across different chains to form an interconnected blockchain network. As shown in Fig. 6, the top half belongs to the local region, which corresponds to the entities managed by different blockchains. The entities in each

blockchain can be associated in different ways, and their geometric relationships and related information can be reflected in the blockchain constructed by a Directed Acyclic Graph (DAG). In Fig. 6, the lower half is the global area, which corresponds to the association between different blockchains. The association connection across different blockchains is realized through the tokens used by the blockchain. The structure between different blockchains also allows for a mesh structure. Through this multi-blockchain network structure, the relationship between multiple entities in complex scenarios can be mapped to the multi-blockchain structure, and then the management of entities in complex scenarios can be realized by multi-blockchain.

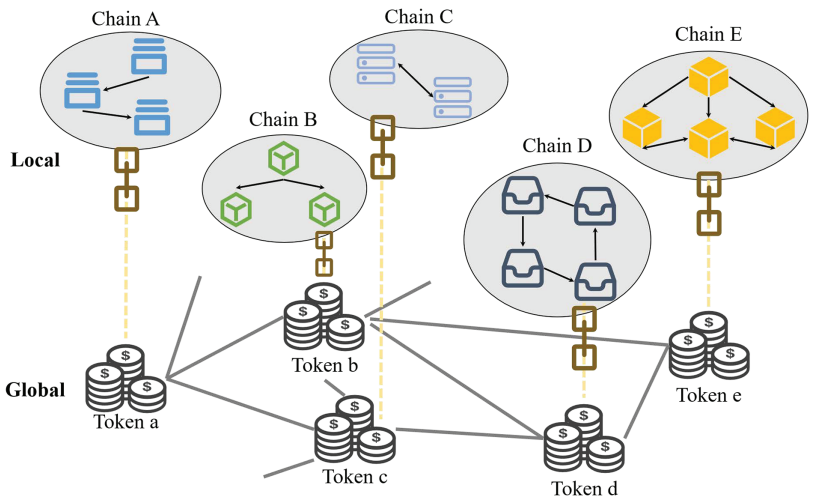

Figure 6: Multi-blockchain network diagram.

Luo et al. [25] introduced the Graphs of Graphs (GoG) model, which aggregates token transaction data from various platforms into a multi-chain graph structure, thereby enabling network-level analysis. Fan et al. [26] proposed the MULTAV voting framework, where token holders across different blockchain systems participate in cross-chain governance voting. This framework enhances security and coordination in decentralized blockchain management by allowing multi-chain voting based on existing token ownership.

2.5 Summary of This Section

Following the detailed exposition of each architecture, we synthesize their characteristics to provide a holistic view of the ecosystem. Table 1 outlines a comparative summary of the four architectures, contrasting their performance regarding scalability, complexity, and distinct application domains. This overview serves to clarify the specific utility of each design, demonstrating how different topological structures influence the overall efficiency and complexity of cross-chain interactions.

Table 1: Comparative analysis of multi-blockchain architectures.

Architecture	Topology	Scalability	Interoperability Complexity	Typical Use Case
Parallel	Linear; Strong inter-chain independence.	High; Easy to scale with parallel processing.	Low; Less interaction.	Asset management between independent entities.

(Continued)

Table 1 (continued)

Architecture	Topology	Scalability	Interoperability Complexity	Typical Use Case
Hierarchical	Hierarchical structure; It exists a master-slave relationship	Medium; It is limited by the throughput of the root chain or the upper chain.	Medium; It needs to handle cross-layer state synchronization.	Supply chain traceability, regulatory audits.
Hybrid	It is a nested structure, combining parallelism and layering.	Very high; It can flexibly adapt to different needs.	High; It is necessary to maintain multiple cross-chain protocols	Complex data sharing, cross-domain identity authentication.
Multi-Chain Network	Graph/DAG structure	High; It is dynamically linked.	Very high; It needs to handle complex routing and consensus heterogeneity.	Decentralized governance (DAO), metaverse.

3 Cross-Chain Technologies and Interoperability

Cross-chain technology refers to communication mechanisms that enable different blockchains to share data or assets. Cross-chain operations enable collaboration between disparate blockchains for complex tasks. Such interoperability includes data exchange, asset transfers, transaction confirmations, and synchronization. As illustrated in Fig. 7, primary cross-chain technologies include main/side chain models [46–48], relay chains [8,49,50], bridge nodes [36,42], cross-chain smart contracts [51–53], and Hash Time-Locked Contracts (HTLCs) [54,55].

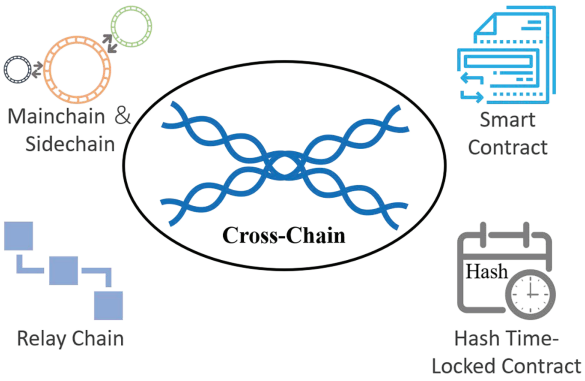

Figure 7: Cross-chain technologies.

To critically evaluate the security boundaries of diverse cross-chain mechanisms, we establish a classification framework based on Trust Models. Depending on the verification logic and reliance on third parties, cross-chain technologies can be categorized into three types:

1. **Trusted (Centralized):** Relies on a specific set of external verifiers or a trusted intermediary to validate transactions. Users must trust the honesty of these entities.
2. **Trust-minimized (Hybrid/Crypto-economic):** Reduces trust assumptions by introducing economic incentives (e.g., staking, slashing) or fraud proofs. Security relies on the assumption that at least one verifier is honest (1-of-N) or that rational actors will not forfeit their stake.
3. **Trustless (Cryptographic):** Relies purely on cryptographic proofs (e.g., ZK-proofs, Merkle proofs) and the underlying consensus of the source chain. No external trust is required beyond the source and destination chains themselves.

Table 2 delineates the spectrum of cross-chain technologies specifically through the lens of verification mechanisms and their associated trust assumptions. While the industry often categorizes protocols into 'Trusted', 'Trust-minimized', and 'Trustless', a rigorous cryptoeconomic analysis requires more nuance. Specifically, the architectures labeled as 'Trustless' (Relay Chains and ZK-Bridges) are more accurately defined as 'Consensus-Verifying'. Their security does not rely on external third parties, but rather is predicated on the consensus integrity of the source chain and the soundness of cryptographic primitives (e.g., ZK-SNARKs). Furthermore, the table distinguishes between Interactive Verification (e.g., Optimistic models and HTLCs), which imposes distinct liveness assumptions on users or watchtowers to prevent fraud, and Non-Interactive Verification (e.g., ZK-Bridges), which mathematically proves state validity without requiring a challenge period. This classification highlights the inherent trade-off between latency, computational cost, and the reliance on synchronous network assumptions.

Table 2: Comparative analysis of cross-chain technologies based on trust models.

Trust Model	Technology Category	Representative Mechanisms/Projects	Trust Assumption	Key Security Risks
Trusted	Bridge Nodes/Notary Schemes	Multi-sig Wallets, Centralized Exchanges (CEX), Early Bridge Solutions	Honest Majority: Assumes the majority of the selected committee/nodes are honest.	Centralization and Collusion: Vulnerable to private key theft or collusion among the small set of validators.
Trust-minimized	Hash Time-Locked Contracts (HTLC)	Lightning Network, Atomic Swaps	Rationality: Assumes participants act rationally to claim funds; relies on synchronous clocks.	Liveness Failure: Funds can be locked if parties go offline.
Trust-minimized	Optimistic Relays	Optimistic Rollup Bridges, Nomad Bridge	1-of-N Honesty: Assumes at least one watcher will submit a fraud proof during the challenge period.	Smart contract logic bugs in fraud proof verification.

(Continued)

Table 2 (continued)

Trust Model	Technology Category	Representative Mechanisms/Projects	Trust Assumption	Key Security Risks
Trustless	Relay Chains (Light Clients)	Cosmos IBC, BTC Relay, Polkadot XCM	Consensus Integrity: Assumes the source chain's consensus is secure. Light clients verify block headers on-chain.	Complexity in maintaining light clients for dynamic validator sets.
Trustless	ZK-Bridges (Succinct Light Client)	ZkBridge, Succinct Labs	Math/Cryptography: Relies on the soundness of Zero-Knowledge Proof circuits.	Bugs in ZK circuits; extremely high computational cost for proof generation.

3.1 Main/Side Chain Cross-Chain Technology

Sidechains typically implement asset transfer via two-way pegs, moving assets from the main chain to the sidechain to alleviate the main chain's load while preserving its security. In specific application contexts, main/side chain models offer more efficient services. The core mechanism relies on the main chain validating the sidechain's state. For example, Deng et al. [56] enhanced the SFPoW algorithm with a sliding window model for proof generation, ensuring decentralization and reducing communication and verification costs through COSI dual signatures. Zendoo [57] proposed a generic cross-chain protocol allowing main chains to communicate with diverse sidechains without requiring knowledge of their internal structures, thereby achieving timeline decoupling. Yin et al. [58] introduced Ge-Co, a versatile sidechain structure supporting multiple consensus algorithms (e.g., PoW and PoS) with optimally succinct proofs. Proof-of-Wait [59] suggests using verifiable random functions for fair, decentralized sidechain node selection to communicate with the main chain. Fast transfer methods in PoS sidechains [60] optimize committee selection and voting to shorten voting cycles. In terms of main chain security, the PSSC algorithm [61] uses smart contract-based staking and penalties to shift validation from the main chain to the sidechain, mitigating fork risks. Similar main/side chain solutions are found in [62,63].

From the perspective of trust models, Main/Side chain technologies act as a spectrum. Traditional implementations utilizing Federated Pegs fall under the Trusted model, as they require users to trust a permissioned group of validators. However, advanced solutions like Zendoo [57] allow the main chain to verify sidechain states via zk-SNARKs without knowing the internal details, effectively shifting the paradigm towards a Trustless model based on cryptographic proofs.

3.2 Relay Chain Cross-Chain Technology

Relay chains, such as Cosmos IBC, typically adopt a Trustless model by utilizing on-chain light clients to verify block headers from connected zones. Relay chains act as bridges connecting different blockchains, enabling data transfer and synchronization. Fig. 8 shows the cross-chain scheme of relay chain with Cosmos asset exchange as an example. Zone blockchains represent many different blockchains that have cross-chain communication requirements; Hub is a relay chain operated by a trusted third-party service company, which

is generally established by a public chain. The blockchain and the relay chain communicate through the cross-chain information transfer protocol (such as Inter-Blockchain Communication, IBC), and the relay chain Hub handles the cross-chain tasks between the Zone blockchains. It should be noted that there is not only one relay chain. For example, there can exist two relay chain hubs in the graph to handle cross-chain work between blockchain Zone5 and blockchain Zone6.

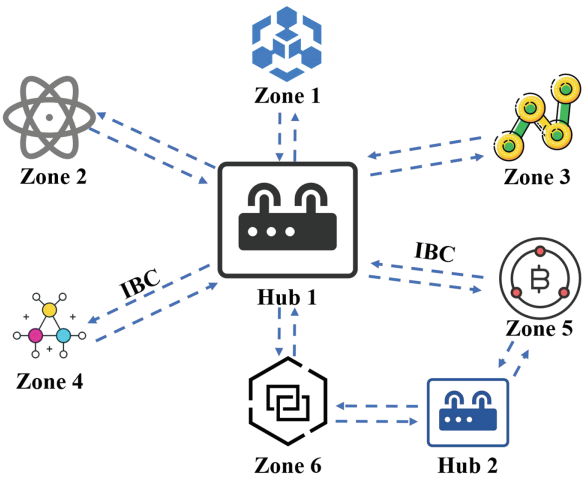

Figure 8: Diagram of the relay chain cross-chain.

It is noteworthy that, although light client-based relay technologies (e.g., IBC) are classified as 'Trustless' at the verification layer in Table 2—meaning the destination chain directly verifies the source chain's consensus proofs without reliance on third-party signatures—the relay chain structure introduces specific centralization risks at the network topology level. Functioning as the central node of a star topology, the Relay Chain (Hub) constitutes a single point of structural dependency. The security of the Hub is therefore paramount, presenting two distinct challenges:

Liveness Failure: Should the Hub's validator set cease block production or succumb to a DDoS attack, cross-chain communication among all connected Zones would be severed.

Censorship Risks: While the Hub is cryptographically constrained from tampering with transaction payloads, it retains censorship authority, possessing the capacity to selectively refuse packet transmission from specific Zones.

Consequently, while the Relay Chain architecture facilitates connectivity, it necessitates that participants maintain rigorous scrutiny over the validator governance of the Hub.

For instance, Liu et al. [64] proposed the DP-Chain framework, which uses a coordination layer maintaining a directed acyclic graph ledger to synchronize chain state updates across regions without relying on trusted third parties. In the energy internet domain, supervisory chains [49] serve as relay chains to record cross-domain authentication information for auditing and validation. Xia et al. [8] employed a relay chain between source and target chains for transaction relaying and validation, incorporating a reputation system to enhance throughput and security.

Similarly, bridge nodes can transfer state information between blockchains. Bridge nodes often fall into the Trusted category, especially when implemented as a multi-signature federation. Wu et al. [65] proposed the Virtual Group approach, where selected proxy nodes form virtual groups that combine on-chain authorization with off-chain data transfer for efficient cross-chain data sharing.

3.3 Cross-Chain Smart Contract Technology

Cross-chain smart contract technology refers to protocols where different blockchains achieve interoperability through smart contracts. A significant challenge lies in ensuring compatibility and security given underlying differences among blockchains. For instance, ZkBridge [66] leverages zero-knowledge proofs to eliminate dependence on relay chains or bridge nodes, achieving efficient and secure trustless communication. Sun et al. [67] proposed an identity aggregation scheme linking wallet accounts across blockchains to verified identities while preserving privacy. Wilson et al. [68] developed a verifiable querying framework that supports parallel queries across multiple blockchains while protecting data privacy and integrity. Chong and Law [69] designed a Multi-Blockchain EHR sharing system, with separate smart contracts for client access, access control, and storage, enabling cross-chain data retrieval and synchronization.

The security of cross-chain smart contracts depends heavily on the underlying verification logic. Early implementations often used multi-signature schemes to manage asset custody, which classifies them as Trusted systems with centralization risks. In contrast, recent innovations such as ZkBridge [66] utilize smart contracts to verify zero-knowledge proofs of block headers. This approach eliminates the need for trusted third parties, categorizing it as a Trustless solution that relies solely on mathematical soundness.

3.4 Hash Time-Locked Cross-Chain Technology

Hash locking ensures the atomicity and consistency of cross-chain transactions by allowing operations to succeed or fail simultaneously across blockchains. HTLC contracts guarantee that assets or information can be securely synchronized across blockchains. The principle is shown in Fig. 9, Alice and Bob each have a blockchain, and the two blockchains can use different tokens. Now Alice wants to trade A for Bob for B. The cross-chain process using Hash-Time-Locked Cross-Chain is as follows:

1 Alice will generate a random number s and calculate its hash h.
2 Alice sends the hash value h to Bob.
3 Alice will generate A transaction TX on her blockchain to lock the transaction A.
4 When Bob verifies that transaction A is locked, a transaction is generated to lock transaction B.
5 At this time, Alice can send a random number s to Bob, and obtain the transaction content B after hash verification.
6 Finally, after obtaining the random number s, Bob sends s to Alice's smart contract to obtain the transaction content A.

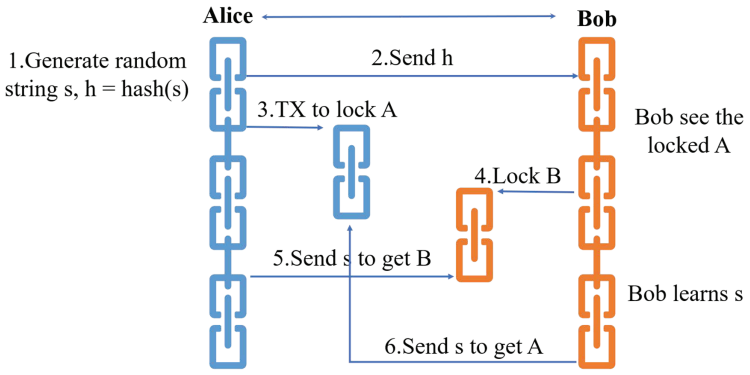

Figure 9: The principle of Hash-Time-Locked Cross-Chain (HTLC).

Many scholars have carried out related research using this technology. Zhang et al. [52] applied HTLC to a tourism management system to ensure cross-chain transactional consistency while protecting participant identities and data privacy through encryption. Cheng et al. [55] used HTLCs to decentralize the lock, validation, and unlocking phases of cross-chain interactions, mitigating centralized risks. Lu et al. [51] discussed a two-phase protocol ensuring secure message transmission and state updates for atomic multi-blockchain transactions, even though it does not explicitly rely on HTLCs.

3.5 Consensus Heterogeneity and Finality

A fundamental challenge in cross-chain interoperability lies in the misalignment of consensus mechanisms between the Source Chain and the Target Chain, specifically regarding the divergent definitions of "Transaction Finality." Existing cross-chain protocols must address two primary categories of conflict:

1. Probabilistic vs. Deterministic Finality: Chains employing PoW consensus (e.g., Bitcoin, Ethereum 1.0) exhibit only probabilistic finality, making them susceptible to chain reorganization (or "reorgs"). A critical security risk arises if the source chain undergoes a rollback after a cross-chain operation (such as asset unlocking) has already been executed on the target chain. This irreversibility on the target side, coupled with the reversion on the source side, exposes the system to severe double-spending attacks. Mitigation: Cross-chain protocols must implement confirmation lag mechanisms (e.g., waiting for 6 block confirmations) or integrate finality gadgets (such as Polkadot's GRANDPA protocol [50]). These measures are essential to ensure the source chain state is effectively irreversible before triggering the cross-chain signal.

2. Atomicity Failure: In interactions between heterogeneous chains, state inconsistency occurs if a transaction fails on the target chain while the corresponding assets remain locked on the source chain.

While Hash Time-Locked Contracts (HTLCs) [54,55] utilize cryptographic primitives to provide a degree of atomicity, they impose stringent liveness requirements on node availability. A more advanced approach involves utilizing a Relay Chain as a unified settlement layer (or finality arbiter) to coordinate state synchronization across heterogeneous consensus systems.

4 Application Scenarios of Multi-Blockchain

Owing to their dynamic architectures and secure cross-chain mechanisms, Multi-Blockchain systems are widely applicable in diverse fields. As depicted in Fig. 10, prominent application domains include data exchange [49,50,55,65], transaction verification [31,40,41,70,71], medical data management [5,36,69], supply chain management [47,54,72], and IoT management [73,74].

4.1 Data Exchange

There have been many schemes [75–78] that combine blockchain technology with data exchange, and this more secure and transparent way of data exchange occupies a large proportion in blockchain applications. However, with the increase of the number of entities exchanging data and the increasing types of data, a single blockchain structure is difficult to adapt to complex data exchange scenarios.

Multi-Blockchain architectures, through heterogeneous chain collaboration and atomic cross-chain operations, address the issues of single points of failure and data silos in centralized platforms. Compared to centralized data markets, Multi-Blockchain-based platforms offer enhanced security and trust. In the energy and electric IoT sectors, cross-domain data exchange requires secure authentication mechanisms. Liu et al. [49] proposed a cross-domain authentication scheme based on Multi-Blockchain, enhancing the security of energy internet data exchanges. The Polkadot architecture [50] separates consensus and state

transition mechanisms to achieve interoperability and parallel processing among heterogeneous blockchains, supporting cross-chain transactions and data sharing.

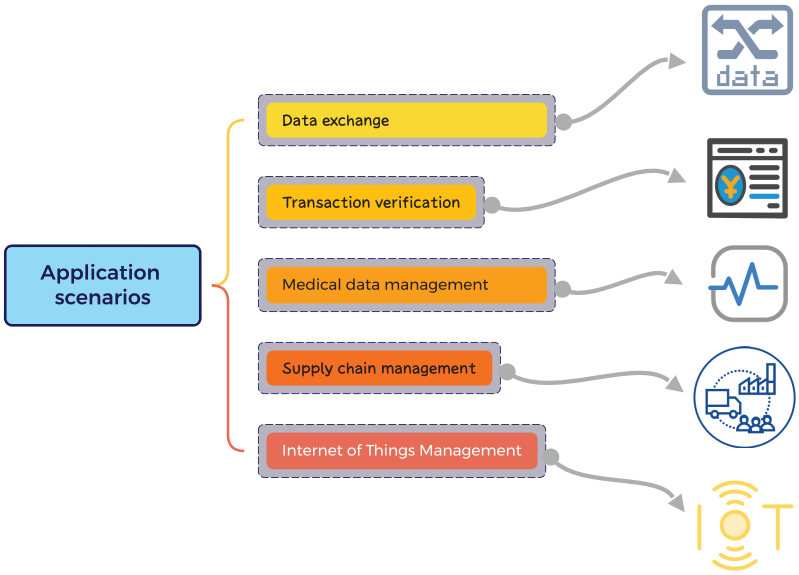

Figure 10: Application scenarios of multi-blockchain.

4.2 Transaction Verification

In the transaction scenario, how to verify the identity of the transaction parties and the ownership of the transaction object is an inevitable problem before the transaction. Blockchain has natural advantages in dealing with transaction verification problems due to its immutability and transparency. There have been many studies on the combination of single blockchain and transaction verification [79,80], and multi-blockchain is more able to handle the verification task in complex transaction scenarios.

Multi-Blockchain systems optimize transaction verification through hierarchical validation and lightweight consensus, offloading computation-intensive tasks onto specialized chains to enhance security and efficiency. Hwang et al. [41] proposed a multi-chain architecture with distributed auditing mechanisms, addressing bottlenecks in blockchain applications for commercial transactions. Li et al. [70] designed a secure, efficient, and fair data trading market using a Multi-Blockchain architecture and customized pricing mechanisms. Lee [71] developed the HMBS framework, applying sharding techniques to parallelize cryptocurrency transfers and smart contract executions, thereby overcoming performance bottlenecks.

4.3 Medical Data Management

There are a large number of studies on the combination of blockchain technology in the medical field [81–83]. However, there are relatively few studies using multi-blockchain architecture.

Through fine-grained access control and cross-institution data interoperability, Multi-Blockchain systems address the tension between medical data sharing and privacy protection. Zhang et al. [36] proposed MBDML, a collaborative privacy-preserving machine learning system for medical images. Saini et al. [5] applied Multi-Blockchain technology to improve data transparency, traceability, and security during the COVID-19 pandemic. Chong and Law [69] developed a Multi-Blockchain EHR sharing system allowing healthcare professionals to dynamically access global patient health records via service-level agreements.

4.4 Supply Chain Management

In the supply chain tracking task, it is necessary to track the production place of raw materials, production and processing, and the final flow place of products. The traceability and traceability capabilities of blockchain technology make it have great advantages in dealing with supply chain management tasks. Many studies have also been carried out on this basis [84–87]. The combination of multi-blockchain and supply chain is more of an improvement of the structure of a single blockchain, and there is no essential difference in technology.

Multi-Blockchain systems enhance transparency and traceability in supply chains through multi-level data recording and integration across supply stages. Peng et al. [47] combined Multi-Blockchain, digital signatures, hash locking, identity resolution, and smart contracts to manage rice supply chain information. Ktari et al. [72] developed a Multi-Blockchain traceability system for the Tunisian olive oil industry, integrating IoT technologies and smart contracts to ensure product authenticity and provenance.

4.5 Internet of Things (IoT) Management

In the Internet of Things management scenario, a single blockchain structure can only exist as a simple data storage tool, such as the simple application of blockchain in the Internet of Vehicles (IoV) scenario [88–91]. When the number of users and hardware enterprises in the Internet of things increases rapidly, the number of corresponding devices and sensors will also increase rapidly. At this point, the simple blockchain structure will not be able to handle complex logistics management tasks. Multi-blockchain, with its various blockchain architectures and different secure cross-chain technologies, occupies a place in the technical scheme adopted by iot management.

Through device identity management and edge computing collaboration, Multi-Blockchain systems address IoT security and scalability challenges. Honar Pajooh et al. [73] used a multi-layer blockchain architecture based on K-anonymous clustering to enhance local authentication and authorization in IoT networks. Xie and Li [92] applied a federated learning framework across multiple blockchains to improve data privacy and system efficiency in intelligent unmanned ports, optimizing model aggregation and reducing communication overhead.

4.6 Summary of This Section

As illustrated in Table 3, the current landscape of multi-chain applications exhibits a distinct polarization. Systems centered on asset exchange (e.g., Polkadot, Cosmos) have entered a mature production phase, underpinning billions of dollars in economic value. In contrast, domains requiring complex data governance—such as healthcare, supply chain, and IoT—remain predominantly at the stage of academic prototypes or simulation verification. These implementations are primarily constrained by challenges regarding regulatory compliance for cross-chain data privacy and the bottlenecks associated with on-chaining off-chain data (the Oracle problem).

Table 3: Maturity assessment of representative multi-blockchain applications.

Domain	Project/Reference	Status	Key Function
Data/Asset Exchange	Cosmos (IBC)/Polkadot [50]	Production	Cross-chain asset transfer, decentralized trading

(Continued)

Table 3 (continued)

Domain	Project/Reference	Status	Key Function
Data/Asset Exchange	BitBTC/Wrapped BTC [56]	Production	Asset anchoring and cross-chain mapping
Supply Chain	Peng et al. [47] (Rice Supply Chain)	Academic Prototype	Agricultural Product Traceability and Regulatory Audit
Medical Data	Saini et al. [5] (Multi-MedChain)	Academic Prototype	Fine-grained privacy access control
IoT Management	Zhang et al. [28] (IIoT Auth)	Conceptual/Simulation	Cross-domain device identity authentication
Transaction Verification	ZkBridge [66]	Pilot/Early Access	Block header verification based on zero-knowledge proof

5 Challenges and Future Prospects of Multi-Blockchain

Cross-Chain Security Vulnerabilities and Attack Vectors

Cross-chain bridges have emerged as the single most vulnerable component within the blockchain ecosystem. In contrast to intra-chain consensus attacks (e.g., 51% attacks), inter-chain systems are exposed to significantly more intricate attack vectors. We categorize the primary security risks as follows:

Private Key Compromise and Centralization Risks: Many bridges operating on the 'Trusted Model' rely heavily on multi-signature (multisig) schemes. Should an adversary compromise the private keys of a threshold majority of signers, they can illicitly drain the locked assets. Case Study: The 2022 Ronin Bridge exploit, where attackers utilized social engineering to compromise five out of nine validator private keys [93].

Smart Contract Logic Vulnerabilities: Cross-chain contracts entail complex logic regarding permission management and message serialization, increasing the probability of bugs. Case Study: The Poly Network attack, wherein the attacker exploited a logical flaw in the privilege verification function to forcibly register themselves as a 'Keeper,' thereby authorizing unauthorized asset transfers [94].

Fraud Proof Failures: Within 'Optimistic Verification' models, misconfigurations in the fraud proof mechanism can enable attackers to forge invalid Merkle Roots. Case Study: The Nomad Bridge hack ($190 million), caused by an initialization parameter error during a contract upgrade, which resulted in the system automatically accepting all transactions as valid [95].

Despite offering significant advantages in scalability, Multi-Blockchain systems face considerable challenges:

1 Cross-Chain Security: Issues such as 51% attacks and vulnerabilities in cross-chain bridges remain unresolved [18].
2 Consensus and Smart Contract Compatibility: Achieving cooperative operations across chains with heterogeneous consensus mechanisms is complex. Smart contracts' inability to call external processes [96] and the technical infeasibility of migrating smart contracts across chains [18] are persistent problems.

3 Resource Overhead: How to reduce the threshold for the use of multi-blockchain and make it lightweight is also a big challenge. Maintaining Multi-Blockchain systems incurs significant communication, computation, and storage costs [97]. The overall implementation of multi-blockchain architecture is difficult. Organizations need to coordinate and synchronize across multiple blockchains, which also requires additional resources and effort [98].
4 Decentralization: Although Multi-Blockchain reduces single-chain centralization, coordinating multiple blockchains often requires centralized decision-making mechanisms [7].
5 System Stability: High data throughput can destabilize the system if migration delays become unbounded [99]. Additionally, block verification latency increases with data block size [100].

At present, the multi-blockchain system is moving from technology stack to landing application. The technological breakthrough of multi-blockchain can not be separated from the synchronous evolution of governance framework and social cognition. The feasible development directions in the future are as follows:

1 **Lightweight Relay Networks:** Compared with the high overhead of traditional cross-chain Bridges, a relay network with light nodes can be introduced. The method of employing Merkle Proof-based relay mechanisms to reduce cross-chain communication latency and gas costs.
2 **Improved HTLC Protocol:** Researchers can try to achieve atomic exchange across multiple blockchains to further improve the success rate of blockchain synchronization.
3 **Zero-Knowledge Proofs:** Industrial application of zero-knowledge proofs to lower the cost of cross-chain transaction verification, supporting Solidity and Rust-based contracts.
4 **Modular Multi-Blockchain Architectures:** Future multi-chain systems will evolve from monolithic structures to decoupled architectures driven by modularity. Flexible composition of different blockchains to enable customized execution layers with lightweight node requirements. The modular multi-blockchain architecture will also allow developers to design custom execution layers, where a network of light nodes only needs to download block headers to complete data validation. Specifically, the Data Availability Layer (e.g., Celestia) will be isolated to exclusively handle transaction data storage, while the Execution Layer can be implemented as customized Rollups. This architecture enables developers to achieve low-cost cross-chain verification through Data Availability Sampling (DAS) without compromising security.
5 **Reinforcement Learning for Scheduling:** Reinforcement learning models can also be introduced in multi-blockchain architectures. The model is able to analyze transaction bandwidth data on different blockchains in real time. The model can dynamically select optimal transaction paths, maintaining transaction success rates during periods of Ethereum congestion. Existing cross-chain routing protocols predominantly employ static strategies. By incorporating Deep Reinforcement Learning (DRL) models, cross-chain transaction processing can be formulated as a multi-objective optimization problem:
State: Current metrics across chains, including Gas fees and validator latency.
Action: Selecting the optimal relay path or cross-chain bridge.
Reward: Maximizing the transaction success rate while minimizing total costs.
Such intelligent scheduling mechanisms are critical for high-frequency cross-chain scenarios, such as arbitrage and cross-chain payments.
6 **Regulatory Compliance:** Developing real-time monitoring systems for cross-chain asset flows and multi-chain asset tracking under regulatory frameworks.

6 Conclusion

This paper provides a comprehensive review of Multi-Blockchain system architectures and cross-chain technologies. Key findings include:

1 **Architectural Diversity:** Parallel blockchains support load balancing, hierarchical blockchains facilitate layered cooperation, and hybrid architectures optimize complex scenarios.
2 **Critical Role of Cross-Chain Technologies:** Main/side chain pegs secure asset transfers; relay chains and HTLC protocols enable atomic operations across heterogeneous blockchains; smart contracts and bridge nodes advance decentralized interoperability.
3 **Extensive Application Potential:** Multi-Blockchain systems demonstrate significant advantages in data sharing, transaction verification, medical collaboration, supply chain traceability, and IoT management.

Additionally, we have thoroughly analyzed challenges such as cross-chain security risks, consensus protocol heterogeneity, resource overhead, and decentralization difficulties. Promising directions for future research include lightweight relay networks, zero-knowledge cross-chain proofs, modular architectures, and reinforcement learning-based scheduling.

Overall, Multi-Blockchain technology offers significant potential to enhance the scalability and interoperability of blockchain systems. Continued research on standardized protocols, security auditing, and cross-chain programming models will be essential for widespread adoption across diverse industrial ecosystems.

Acknowledgement: None.

Funding Statement: This work was supported by the Startup Foundation for Introducing Talent of Nanjing University of Information Science and Technology.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Tsu-Yang Wu and Yehai Xue; algorithm organization, Tsu-Yang Wu and Yehai Xue; paper analysis, Saru Kumari and Lip Yee Por; investigation, Haonan Li and Lip Yee Por; writing—original draft preparation, Yehai Xue. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data are contained within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ressi D, Romanello R, Piazza C, Rossi S. AI-enhanced blockchain technology: a review of advancements and opportunities. J Netw Comput Appl. 2024;225:103858. doi:10.1016/j.jnca.2024.103858.
2. Li J, Wang Z, Guan S, Cao Y. ProChain: a privacy-preserving blockchain-based supply chain traceability system model. Comput Indust Eng. 2024;187:109831. doi:10.1016/j.cie.2023.109831.
3. Zhang Y, Wu X, Ge H, Jiang Y, Sun Z, Ji X, et al. A blockchain-based traceability model for grain and oil food supply chain. Foods. 2023;12(17):3235. doi:10.3390/foods12173235.
4. Ahmed S, Broek Nt. Blockchain could boost food security. Nature. 2017;550(7674):43. doi:10.1038/550043e.
5. Saini A, Shaghaghi A, Huang Z, Kanhere SS. Multi-MedChain: multi-party multi-blockchain medical supply chain management system. In: 2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT); 2024 Jul 24–26; Melbourne, Australia. p. 153–9. doi:10.1109/aiot63253.2024.00038.
6. Malamas V, Kotzanikolaou P, Dasaklis TK, Burmester M. A hierarchical multi blockchain for fine grained access to medical data. IEEE Access. 2020;8:134393–412. doi:10.1109/access.2020.3011201.
7. Alkhodair A, Mohanty S, Kougianos E, Puthal D. McPoRA: a multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems. In: 2020 IEEE computer society annual symposium on VLSI (ISVLSI); 2020 Jul 6–8; Limassol, Cyprus. p. 446–51.

8. Xia P, Li J, Shi L, Cao B, Tan W, Weng J, et al. A reputation-aided lightweight consensus service framework for multi-chain metaverse. IEEE Netw. 2024;38(6):201–10. doi:10.1109/mnet.2024.3382346.
9. Zhang C, Zhu L, Xu C, Sharif K. PRVB: achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle. IEEE Trans Vehic Technol. 2020;70(1):831–43.
10. Jakobsson M, Juels A. Proofs of work and bread pudding protocols. In: Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99); 1999 Sep 20–21; Leuven, Belgium. Springer; 1999. p. 258–72.
11. Saleh F. Blockchain without waste: proof-of-stake. Rev Finan Stud. 2021;34(3):1156–90. doi:10.1093/rfs/hhaa075.
12. Du MX, Ma XF, Zhang Z, Wang XW, Chen QJ. A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC); 2017 Oct 5–8; Banff, AB, Canada. p. 2567–72.
13. Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Qual Manag J. 2018;25(1):64–5. doi:10.1080/10686967.2018.1404373.
14. Liang Z, Jiang R, Yang M. Cross-chain overview: development, mechanisms, protocols, security, and challenges. In: International Conference on Blockchain and Trustworthy Systems; 2024 Jul 12–17; Hangzhou, China. Singapore: Springer; 2024. p. 31–48.
15. Ou W, Huang S, Zheng J, Zhang Q, Zeng G, Han W. An overview on cross-chain: mechanism, platforms, challenges and advances. Comput Netw. 2022;218:109378. doi:10.1016/j.comnet.2022.109378.
16. Schaad A, Reski T, Winzenried O. Integration of a secure physical element as a trusted oracle in a hyperledger blockchain. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications; 2019 Jul 26–28; Prague, Czech Republic. 2019. p. 498–503. doi:10.5220/0007957104980503.
17. Kan L, Wei Y, Muhammad AH, Siyuan W, Gao LC, Kai H. A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C); 2018 Jul 16–20; Lisbon, Portugal. p. 139–45.
18. Ladleif J, Friedow C, Weske M. An architecture for multi-chain business process choreographies. In: Business Information Systems: 23rd International Conference, BIS 2020; 2020 Jun 8–10; Colorado Springs, CO, USA. p. 184–96.
19. Schulz KF, Freund D. A multichain architecture for distributed supply chain design in industry 4.0. In: Business Information Systems Workshops. Cham, Switzerland: Springer International Publishing; 2018. p. 277–88.
20. Wang G, Huang X, Li Y, Zuo F, He X. A multi-blockchain based reliable noise adding method for privacy preservation in cyber-physical systems. In: Proceedings of International Conference on Image, Vision and Intelligent Systems 2022 (ICIVIS 2022); 2022 Aug 15–17; Singapore: Springer; 2022. p. 811–20.
21. Qu L, Wen F, Huang H, Wang Z. Aggregation-chain: a consortium blockchain based multi-chain data sharing framework with efficient query. Clust Comput. 2025;28(1):1–16. doi:10.1007/s10586-024-04777-w.
22. Hulea M, Miron R, Muresan V. Digital product passport implementation based on multi-blockchain approach with decentralized identifier provider. Appl Sci. 2024;14(11):4874. doi:10.3390/app14114874.
23. Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet Things. 2023;24:100969. doi:10.1016/j.iot.2023.100969.
24. Kong X, Zhang J, Wang H, Shu J. Framework of decentralized multi-chain data management for power systems. CSEE J Pow Energy Syst. 2019;6(2):458–68. doi:10.17775/cseejpes.2018.00820.
25. Luo B, Zhang Z, Wang Q, He B. Multi-chain graphs of graphs: a new approach to analyzing blockchain datasets. Adv Neural Inform Process Syst. 2024;37:28490–514.
26. Fan X, Chai Q, Zhong Z. Multav: A multi-chain token backed voting framework for decentralized blockchain governance. In: Blockchain–ICBC 2020. Cham, Switzerland: Springer International; 2020. p. 33–47. doi:10.1007/978-3-030-59638-5_3.
27. Wang L, Zhou W, Zuo L, Liu H, Ying W. ONMCA: one-network-multi-chain architecture for customizable asset-oriented blockchain systems. Peer Peer Netw Appl. 2024;17(4):1914–33. doi:10.1007/s12083-024-01698-8.

28. Zhang Y, Li B, Wu J, Liu B, Chen R, Chang J. Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. IEEE Internet Things J. 2022;9(22):22501–15. doi:10.1109/jiot.2022.3176192.
29. Wang Q, Luo Z, Liu K, Ding T, Shen X, Mo X, et al. A multiblockchain-oriented decentralized market framework for frequency regulation service. IEEE Trans Indust Inform. 2021;17(12):8219–29. doi:10.1109/tii.2021.3062623.
30. Liu W, Feng W, Huang M, Xu Y, Zheng X. STEB: a secure service trading ecosystem based on blockchain. PLoS One. 2022;17(6):e0267914. doi:10.1371/journal.pone.0267914.
31. Liang Y, Wang Z, Abdallah AB. Robust vehicle-to-grid energy trading method based on smart forecast and multi-blockchain network. IEEE Access. 2024;12:8135–53. doi:10.1109/access.2024.3352631.
32. Wang Y, Li J, Yan Y, Chen X, Yu F, Zhao S, et al. A semi-centralized blockchain system with multi-chain for auditing communications of Wide Area Protection System. PLoS One. 2021;16(1):e0245560. doi:10.1371/journal.pone.0245560.
33. Lin H, Garg S, Hu J, Kaddoum G, Peng M, Hossain MS. Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles. IEEE Trans Intell Transport Syst. 2020;22(6):3755–64. doi:10.1109/tits.2020.3025247.
34. Yu X, Shu Z, Li Q, Huang J. BC-BLPM: a multi-level security access control model based on blockchain technology. China Commun. 2021;18(2):110–35. doi:10.23919/jcc.2021.02.008.
35. Košťál K. Multi-chain architecture for blockchain networks. Inform Sci Technol. 2020;12(2):8–14.
36. Zhang W, Wang Q, Li M. Medical image collaborative training based on multi-blockchain. In: 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM); 2019 Nov 18–21; San Diego, CA, USA. p. 590–7.
37. Zhang B, Xu J, Wang X, Zhao Z, Chen S, Zhang X. Research on the construction of grain food multi-chain blockchain based on zero-knowledge proof. Foods. 2023;12(8):1600. doi:10.3390/foods12081600.
38. Xie T, Gai K, Zhu L, Wang S, Zhang Z. Rac-chain: an asynchronous consensus-based cross-chain approach to scalable blockchain for metaverse. ACM Trans Multim Comput Commun Appl. 2024;20(7):1–24.
39. Li S, Xiao H, Qiao J. Multi-chain and data-chains partitioning algorithm in intelligent manufacturing CPS. J Cloud Comput. 2021;10(1):1–10. doi:10.1186/s13677-021-00227-9.
40. Lv S, Zhang X, Wang J, Xiong W, Yang L. RMCT: distributed electricity transaction based on reputation mechanism and multi-chain technology in blockchain environment. Elect Power Syst Res. 2025;243:111516. doi:10.1016/j.epsr.2025.111516.
41. Hwang GH, Chen PH, Lu CH, Chiu C, Lin HC, Jheng AJ. InfiniteChain: a multi-chain architecture with distributed auditing of sidechains for public blockchains. In: Blockchain–ICBC 2018: First International Conference, Held as Part of the Services Conference Federation, SCF 2018; 2018 Jun 25–30; Seattle, WA, USA: Springer; 2018. p. 47–60.
42. Kim M, Kim Y. Multi-blockchain structure for a crowdsensing-based smart parking system. Future Internet. 2020;12(5):90.
43. Wang J, Xie Z, Xin H, Li P, Zhang Y, Xiong X, et al. Collaborative construction method of biomedical knowledge graph based on multi-blockchain. Distrib Ledger Technol Res Pract. 2024;3(4):1–23. doi:10.1145/3674153.
44. Jin W, Zheng M, Liu P. Design of multi-chain traceability model for pepper products based on traceability code. Appl Sci. 2024;14(9):3809. doi:10.3390/app14093809.
45. Malamas V, Palaiologos G, Kotzanikolaou P, Burmester M, Glynos D. Hierarchical multi-blockchain-based access control (HMBAC) for multi-authority and multi-domain environments. Appl Sci. 2022;13(1):566. doi:10.3390/app13010566.
46. Huang MM, Yuan LY, Xue P, Zhou C. Trusted edge and cross-domain privacy enhancement model under multi-blockchain. Comput Netw. 2023;234:109881. doi:10.2139/ssrn.4350232.
47. Peng X, Zhang X, Wang X, Li H, Xu J, Zhao Z. Multi-chain collaboration-based information management and control for the rice supply chain. Agriculture. 2022;12(5):689. doi:10.3390/agriculture12050689.
48. Zhang Y, Zhao F. Consensus algorithm for medical data storage and sharing based on master-slave multi-chain of alliance chain. High-Confid Comput. 2023;3(3):100122. doi:10.1016/j.hcc.2023.100122.

49. Liu D, Liu X, Wang R, Zhang H, Zhang F, Sun L, et al. A multi-blockchain-based cross-domain authentication and authorization scheme for energy internet. Wirel Commun Mob Comput. 2023;2023:4778967. doi:10.1155/2023/4778967.
50. Wood G. Polkadot: vision for a heterogeneous multi-chain framework. White Paper. 2016;21(2327):4662.
51. Lu H, Jajoo A, Namjoshi KS. A two-phase protocol for atomic multi-chain transactions. In: Proceedings of the ACM Conext-2024 Workshop on the Decentralization of the Internet; 2024 Dec 9–12; Los Angeles, CA, USA. p. 21–7.
52. Zhang L, Hang L, Jin W, Kim D. Interoperable multi-blockchain platform based on integrated REST APIs for reliable tourism management. Electronics. 2021;10(23):2990. doi:10.3390/electronics10232990.
53. Alyas T, Abbas Q, Niazi S, Alqahtany SS, Alghamdi T, Alzahrani A, et al. Multi blockchain architecture for judicial case management using smart contracts. Sci Rep. 2025;15(1):8471. doi:10.1038/s41598-025-92842-8.
54. Peng X, Zhang X, Wang X, Xu J, Li H, Zhao Z, et al. A refined supervision model of rice supply chain based on multi-blockchain. Foods. 2022;11(18):2785. doi:10.3390/foods11182785.
55. Cheng L, Lv Z, Alfarraj O, Tolba A, Yu X, Ren Y. Secure cross-chain interaction solution in multi-blockchain environment. Heliyon. 2024;10(7):e28861. doi:10.1016/j.heliyon.2024.e28861.
56. Deng Z, Tang C, Li T, Zeng Z, Abla P, He D. SFPoW: constructing secure and flexible proof-of-work sidechains for cross-chain interoperability with wrapped assets. IEEE Trans Comput. 2025;74(7):2278–92. doi:10.1109/TC.2025.3558040.
57. Garoffolo A, Kaidalov D, Oliynykov R. Zendoo: a zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2020 Nov 29–Dec 1; Singapore. p. 1257–62.
58. Yin L, Xu J, Liang K, Zhang Z. Sidechains with optimally succinct proof. IEEE Trans Depend Secure Comput. 2023;21(4):3375–89. doi:10.1109/tdsc.2023.3328430.
59. Gai F, Niu J, Tabatabaee SA, Feng C, Jalalzai M. Cumulus: a secure BFT-based sidechain for off-chain scaling. In: 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS). IEEE; 2021 Jun 25–28; Tokyo, Japan. p. 1–6.
60. Yin L, Xu J, Tang Q. Sidechains with fast cross-chain transfers. IEEE Trans Depend Secure Comput. 2021;19(6):3925–40. doi:10.1109/tdsc.2021.3114151.
61. Deng Z, Li T, Tang C, He D, Zheng Z. PSSC: practical and secure sidechain construction for heterogeneous blockchains orienting IoT. IEEE Internet Things J. 2023;11(3):4600–13. doi:10.1109/JIOT.2023.3302291.
62. Oktian YE, Lee SG, Lee HJ. Hierarchical multi-blockchain architecture for scalable internet of things environment. Electronics. 2020;9(6):1050. doi:10.3390/electronics9061050.
63. Peng T, Liu J, Chen J, Wang G. A privacy-preserving crowdsensing system with muti-blockchain. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2020 Dec 29–2021 Jan 1; Guangzhou, China. p. 1944–9.
64. Liu W, Cao B, Peng M, Li B. Distributed and parallel blockchain: towards a multi-chain system with enhanced security. IEEE Trans Depend Secure Comput. 2025;22(1):723–39. doi:10.1109/TDSC.2024.3417531.
65. Wu Z, Wang Y, Wang L. GAM: a scalable and efficient multi-chain data sharing scheme. Inform Process Manag. 2025;62(3):104004. doi:10.1016/j.ipm.2024.104004.
66. Xie T, Zhang J, Cheng Z, Zhang F, Zhang Y, Jia Y, et al. zkbridge: trustless cross-chain bridges made practical. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security; 2022 Nov 7–11; Los Angeles, CA, USA. p. 3003–17.
67. Sun N, Zhang Y, Liu Y. A universal privacy-preserving multi-blockchain aggregated identity scheme. Appl Sci. 2023;13(6):3806. doi:10.3390/app13063806.
68. Wilson S, Adu-Duodu K, Li Y, Sham R, Solaiman E, Rana O, et al. Verifiable querying framework for multi-blockchain applications. In: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2024 May 27–31. Dublin, Ireland. p. 250–3.
69. Chong H, Law KE. Multi-blockchain model for data sharing with bell-lapadula access control. In: 2023 IEEE International Conference on Blockchain (Blockchain). IEEE; 2023 Dec 17–21; Danzhou, China. p. 55–61.

70. Li J, Li J, Wang X, Qin R, Yuan Y, Wang FY. Multi-blockchain based data trading markets with novel pricing mechanisms. IEEE/CAA J Automat Sinica. 2023;10(12):2222–32. doi:10.1109/jas.2023.123963.
71. Lee NY. Hierarchical multi-blockchain system for parallel computation in cryptocurrency transfers and smart contracts. Appl Sci. 2021;11(21):10173. doi:10.3390/app112110173.
72. Ktari J, Frikha T, Chaabane F, Hamdi M, Hamam H. Agricultural lightweight embedded blockchain system: a case study in olive oil. Electronics. 2022;11(20):3394. doi:10.3390/electronics11203394.
73. Honar Pajooh H, Rashid M, Alam F, Demidenko S. Multi-layer blockchain-based security architecture for internet of things. Sensors. 2021;21(3):772. doi:10.3390/s21030772.
74. Cao Y, Ku CS, Kumar R, Khan A. Privacy and trust in blockchain-federated intrusion detection systems: taxonomy, challenges and perspectives. J Reliab Secure Comput. 2025;1(1):4–24. doi:10.62762/jrsc.2025.399812.
75. Chen JN, Wang JD, Tao KH, Zhou YP, Li HY. Application of proxy signature scheme based on blockchain in multi cloud storage. J Netw Intell. 2024;9(2):1072–87.
76. Zheng BK, Zhu LH, Shen M, Gao F, Zhang C, Li YD, et al. Scalable and privacy-preserving data sharing based on blockchain. J Comput Sci Technol. 2018;33:557–67. doi:10.1007/s11390-018-1840-5.
77. Nguyen TL, Nguyen L, Hoang T, Bandara D, Wang Q, Lu Q, et al. Blockchain-empowered trustworthy data sharing: fundamentals, applications, and challenges. ACM Comput Surv. 2025;57(8):1–36.
78. Li T, Wang H, He D, Yu J. Blockchain-based privacy-preserving and rewarding private data sharing for IoT. IEEE Internet Things J. 2022;9(16):15138–49. doi:10.1109/jiot.2022.3147925.
79. Chen CM, Xiong Z, Wu TY, Kumari S, Alenazi MJF. Protecting virtual economies: a blockchain-based anti-phishing authentication protocol for metaverse applications. IEEE Internet Things J. 2025;12(13):24244–58.
80. Chen CM, Xiang B, Pan Z, Amoon M, Agarwal K. Green supply chain management for digital assets in the metaverse: leveraging blockchain and AIoT. IEEE Internet Things J. 2025;12(19):39419–32. doi:10.1109/jiot.2025.3564299.
81. Liu S, Wang Z, Kumari S, Lv J, Chen CM. Provably secure anti-phishing scheme for medical information in smart healthcare. IEEE Internet Things J. 2024;11(23):38086–97. doi:10.1109/jiot.2024.3445375.
82. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. J Med Syst. 2018;42:1–13. doi:10.1007/s10916-018-0997-3.
83. Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: efficient and secure medical data sharing via blockchain. J Med Syst. 2018;42:1–11.
84. Chen TH, Chew CJ, Lee JS. Preserving privacy and traceability in car-sharing blockchain based on attribute cryptosystem. J Internet Technol. 2024;25(2):175–84. doi:10.53106/160792642024032502001.
85. Dutta P, Choi TM, Somani S, Butala R. Blockchain technology in supply chain operations: applications, challenges and research opportunities. Trans Res Part E Logist Transport Rev. 2020;142:102067. doi:10.1016/j.tre.2020.102067.
86. Azzi R, Chamoun RK, Sokhn M. The power of a blockchain-based supply chain. Comput Indust Eng. 2019;135:582–92. doi:10.1016/j.cie.2019.06.042.
87. Saberi S, Kouhizadeh M, Sarkis J, Shen L. Blockchain technology and its relationships to sustainable supply chain management. Int J Product Res. 2019;57(7):2117–35. doi:10.1080/00207543.2018.1533261.
88. Wang H, Zhang F, Shen Z, Liu P, Liu K. Blockchain-based IVPPA scheme for pseudonym privacy protection in internet of vehicles. J Netw Intell. 2024;9(2):1260–77.
89. Sharma V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). IEEE Commun Lett. 2018;23(2):246–9. doi:10.1109/lcomm.2018.2883629.
90. Karim SM, Habbal A, Chaudhry SA, Irshad A. BSDCE-IoV: blockchain-based secure data collection and exchange scheme for IoV in 5G environment. IEEE Access. 2023;11:36158–75. doi:10.1109/ACCESS.2023.3265959.
91. Devi A, Rathee G, Saini H. Secure blockchain-Internet of Vehicles (B-IoV) mechanism using DPSO and M-ITA algorithms. J Inf Secur Appl. 2022;64(3):103094. doi:10.1016/j.jisa.2021.103094.
92. Xie Z, Li Z. A blockchain multi-chain federated learning framework for enhancing security and efficiency in intelligent unmanned ports. Electronics. 2024;13(24):4926. doi:10.3390/electronics13244926.
93. Ronin Network. Back to building: ronin security breach postmortem; 2022 [cited 2026 Jan 1]. Available from: https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364.

94. Poly Network. The poly network exploit analysis; 2023 [cited 2026 Jan 1]. Available from: https://polynetwork.medium.com/the-poly-network-exploit-analysis-b0a77aff6078.
95. Immunefi. Hack analysis: Nomad Bridge, August 2022; 2022 [cited 2026 Jan 1]. Available from: https://medium.com/immunefi/hack-analysis-nomad-bridge-august-2022-5aa63d53814a.
96. Wang K, Zhang Z, Kim HS. ReviewChain: smart contract based review system with multi-blockchain gateway. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018 Jul 30–Aug 3; Halifax, NS, Canada. p. 1521–6.
97. Cheng Z, Liang Y, Zhao Y, Wang S, Sun C. A multi-blockchain scheme for distributed spectrum sharing in CBRS system. IEEE Trans Cognit Commun Netw. 2023;9(2):266–80. doi:10.1109/tccn.2023.3235789.
98. Pillai B, Biswas K, Hóu Z, Muthukkumarasamy V. The burn-to-claim cross-blockchain asset transfer protocol. In: 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS). Singapore: IEEE; 2020. p. 119–24. doi:10.1109/ICECCS51672.2020.00021.
99. Velloso PB, Morales DC, Nguyen TMT, Pujolle G. Basics: a multi-blockchain approach for securing VM migration in joint-cloud systems. In: 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC); 2023 Oct 28–31; Singapore. p. 523–8.
100. Sim SH, Jeong YS. Multi-blockchain-based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments. Sensors. 2021;21(10):3515. doi:10.3390/s21103515.