Blockchain: Research and Applications 6 (2025) 100286

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Review Article

Towards blockchain interoperability: a comprehensive survey on cross-chain solutions

Wenqing Li [a,b], Zhenguang Liu [a,*], Jianhai Chen [a], Zhe Liu [c], Qinming He [a]

[a] College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China
[b] Goplus Security, Hangzhou 310027, China
[c] Zhejiang Lab, Hangzhou 311121, China

ARTICLE INFO

Keywords:
Blockchain
Interoperability
Cross-chain communication

ABSTRACT

The rapid expansion of decentralized finance (DeFi) applications has catalyzed the emergence of new blockchain systems at an unprecedented pace. However, these systems are largely evolving in isolation, hindering the development of a cohesive ecosystem where value and data can flow seamlessly across networks. Blockchain interoperability technologies are introduced to break down these communication barriers and facilitate effective interactions between different blockchain systems. In recent years, numerous approaches and solutions to blockchain interoperability have been proposed. While some reviews have attempted to categorize cross-chain solutions based on blockchain standards and architectures, a more in-depth analysis is warranted. In this work, we investigate mainstream cross-chain solutions from the perspective of their principles, applications, protocols, and performance. To clarify the concept of blockchain interoperability, we propose a conceptual model that characterizes both asset interoperability and data interoperability. Furthermore, we introduce a hierarchical architecture to categorize and analyze representative cross-chain solutions, covering both academic research and industrial implementations. To maximize the utility of this review for a wide audience, we also highlight open challenges and identify future directions in the field of blockchain interoperability, expecting to provide a comprehensive overview of cross-chain solutions.

1. Introduction

Blockchain technology serves as a revolutionary force to reshape finance and industry by introducing the paradigm of a decentralized ledger. Powered by cryptography and peer-to-peer (P2P) networks, blockchain enables the sharing of secure information and the trading of assets among multiple parties that do not trust each other. Blockchain was originally proposed as an infrastructure for Bitcoin [1] and has since expanded its scope far beyond P2P payment systems. In addition, the emergence of smart contracts has made blockchain programmable [2]. Nowadays, the programmable blockchain has been widely investigated and developed to allow anonymous contract signatures and automated execution. Recent years have witnessed a dramatic rise in the popularity of decentralized applications (DApps). This has led to the collaboration of blockchain with a variety of domains, including smart healthcare [3], Internet of Things (IoT) [4], artificial intelligence [5], and metaverse [6]. However, as DApps experience explosive growth, a single blockchain struggles to cope with such complex application scenarios. In this context, it is crucial to apply the cooperation of multiple chains, namely, cross-chain operations.

As blockchain technology evolves, we are witnessing the introduction of new types of blockchain systems, each with different consensus protocols and unique designs to support diverse applications. Unfortunately, the fundamental architecture of blockchain constrains these protocols to operate in isolated silos; thus, they are developed independently. As a result, separate ecosystems have emerged, lacking interoperability with each other. Recognizing this problem, blockchain interoperability technology has attracted significant interest from both academia and industry. It has the potential to find a way out of heterogeneous blockchain implementations, address different application scenarios, and bridge the gap caused by the lack of unified blockchain development and standardized cross-chain communication.

* Corresponding author.
E-mail addresses: lwqfighting@zju.edu.cn (W. Li), liuzhenguang2008@gmail.com (Z. Liu), chenjh919@zju.edu.cn (J. Chen), zhe.liu@zhejianglab.com (Z. Liu), hqm@zju.edu.cn (Q. He).

https://doi.org/10.1016/j.bcra.2025.100286
Received 27 February 2024; Received in revised form 7 December 2024; Accepted 13 December 2024

Available online 7 April 2025

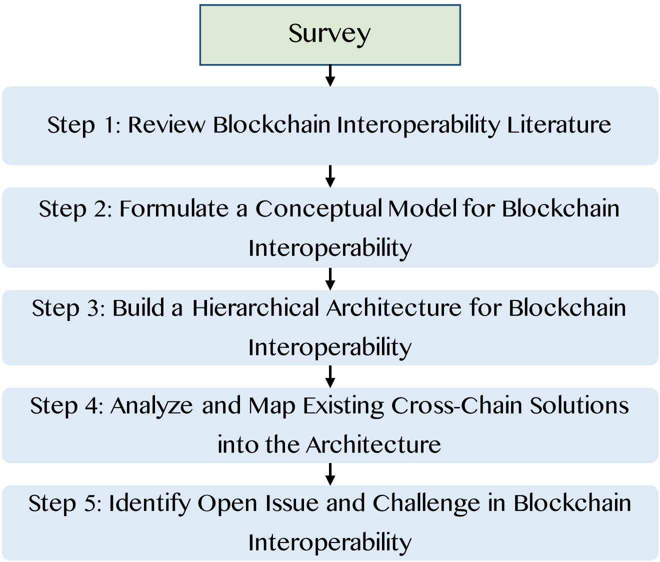
Survey
Step 1: Review Blockchain Interoperability Literature
Step 2: Formulate a Conceptual Model for Blockchain Interoperability
Step 3: Build a Hierarchical Architecture for Blockchain Interoperability
Step 4: Analyze and Map Existing Cross-Chain Solutions into the Architecture
Step 5: Identify Open Issue and Challenge in Blockchain Interoperability

Fig. 1. Review procedure for blockchain interoperability.

Different blockchains have distinct application scenarios. It is not feasible to fulfill all distributed computing needs with a single blockchain. Therefore, it is critical to address the data interoperability of different blockchains. Given the differences between blockchain systems and traditional network systems, blockchain interoperability technology should ensure that the technical characteristics of the blockchain are not compromised. Interoperability for cross-chain communication, cross-chain validation, and cross-chain consensus remains a challenge, and there is a lack of a well-defined artifact that can be used as a guideline for developing cross-chain solutions.

The issue of interoperability has long been difficult to address in a consistent and comprehensive manner. Public information systems have been developed independently, without coordination, adding to this complexity. As blockchain technology continues to evolve, the creation of a unified protocol or standard remains a significant challenge. Several factors contribute to the complexity of achieving blockchain interoperability, with security being a fundamental concern. Specifically, it is critical to ensure that transactions on one ledger can be verified by another and that consensus can be achieved between different systems. Blockchains vary widely in their frameworks, protocols, tokens, consensus mechanisms, programming languages, and governance structures, requiring efforts to enable interaction between them.

Methodology. Research on blockchain interoperability is expanding rapidly in both industry and academia. Terms such as cross-chain bridges (CCBs), cross-chain routing, and cross-chain communication protocols (CCCPs) are increasingly prevalent in various documents and discussions. Therefore, clarifying the concepts and architecture of the blockchain interoperability domain is essential for the efficient development and improvement of cross-chain technology, which is crucial for realizing the vision of an open and distributed computing network. While existing efforts have surveyed current cross-chain solutions and provided classifications based on different interoperability characteristics, they often lack a deep understanding of the interoperability across different layers of blockchain systems. In this paper, we conduct an in-depth review of cross-chain technologies, where Fig. 1 describes the applied review process. Specifically, through a comprehensive review of the blockchain interoperability literature, we explore the similarities and differences in the philosophy and implementation of these solutions and then propose a conceptual model for blockchain interoperability. This model provides a foundation for future conceptual and empirical studies. Thereafter, we present a hierarchical architecture for blockchain interoperability, based on the principle of design science research (DSR) [7]. We map existing cross-chain solutions into a three-layer framework—the network layer, the transaction layer, and the contract layer—and discuss them accordingly. Finally, we identify several open issues and challenges in the area of blockchain interoperability. We anticipate that our work provides valuable recommendations for practitioners seeking effective solutions to facilitate blockchain interoperability.

Contribution. In this work, we provide a comprehensive review of blockchain interoperability by investigating mainstream cross-chain solutions. Our survey aims to provide a holistic understanding of this field, and the key contributions can be summarized as follows:

- We conduct a comprehensive review of current advancements in blockchain interoperability, carefully analyzing and comparing state-of-the-art solutions. This analysis results in a detailed classification of cross-chain solutions based on their design and purpose.
- We develop a conceptual model to elucidate the fundamental aspects and core concepts of blockchain interoperability, dividing it into two key components: asset interoperability and data interoperability. Asset interoperability focuses on the migration and exchange of digital assets, while data interoperability encompasses cross-chain operations with general data transfer and integration.
- We introduce a hierarchical architecture for blockchain interoperability, categorizing existing cross-chain solutions into three levels: the network layer, the transaction layer, and the contract layer.
- We discuss several open issues and challenges in blockchain interoperability that require attention in future research and identify potential areas for further exploration of blockchain interoperability.

Paper organization. The remainder of the paper is organized as follows. First, we compare related work and reviews on blockchain interoperability in Section 2 and identify the unique perspectives of our work. To establish a solid foundation for understanding blockchain interoperability, we carefully survey related technologies and conceptualizations in Section 3. Section 4 introduces a conceptual model for understanding blockchain interoperability. In Section 5, we define a hierarchical architecture that maps existing cross-chain solutions to three levels in the blockchain system. Moreover, we present a detailed analysis and taxonomy of various cross-chain techniques, providing a systematic overview of the different approaches used to achieve blockchain interoperability. In Section 6, we discuss the similarities and differences between these cross-chain techniques, providing valuable insights into their respective strengths and limitations. In Section 7, we identify open issues and challenges that lie ahead and present future research directions in this area. We conclude the paper in Section 8.

2. Related work

In this section, we begin by reviewing the literature and studies related to blockchain interoperability from four key perspectives: principle, application, protocol, and performance. We then present a comparative analysis between our work and previous reviews, aiming to identify and emphasize the key contributions of our research. By positioning our review within the existing body of knowledge, we seek to demonstrate the unique value it adds to the field of blockchain interoperability.

Principle foundation. In 2016, Vitalik Buterin published a technical report on chain interoperability [8], in which he introduced a classification framework of mainstream cross-chain strategies that can be divided into three categories, namely, the notary scheme, sidechain, and hash-locking. The notary scheme involves the collaborative cross-chain operations facilitated by one or a group of trusted parties, while sidechains allow a blockchain system to read or verify data and states

Table 1
Comparison to related surveys on blockchain interoperability from different aspects, including cross-chain connector (CCC), multi-chain network (MCN), exchange (EX), cross-chain transfer protocol (CCTP), cross-chain bridge (CCB), and cross-chain application (CCA) [26–28].

Reference	Analysis model	Architecture			Fine-grained classification						Limitation discussion	Open challenge
		Network	Transaction	Contract	CCC	MCN	EX	CCTP	CCB	CCA		
Jin et al. [29]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✓
Bhatia et al. [10]	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗
Kannengießer et al. [26]	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Lohachab et al. [25]	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Belchior et al. [23]	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓
Llambias et al. [27]	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓
Zhu et al. [28]	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗
Ren et al. [30]	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓
This survey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

from another blockchain. Hash-locking, on the other hand, uses a hash-time-lock mechanism, where cross-chain operations are triggered by the disclosure of preimages during specific time scans. Since then, this pioneering classification framework has gained widespread popularity [9–12] and has become the dominant principle in the field of cross-chain communication. Subsequent research has dived further into specific categories within this framework [13,14], reflecting the growing research interest and advancement in the field of blockchain interoperability.

Application exploration. Given that blockchain interoperability is an application-driven technology, several surveys have explored cross-chain technologies from an application perspective. Schulte et al. [15] proposed a framework and outlined future research directions, focusing on cross-chain token transfer and cross-chain smart contracts. Lipton and Hardjono [16] analyzed blockchain interoperability within the decentralized finance (DeFi) ecosystem, advocating automated market makers (AMMs) as the optimal solution for intraoperability, while highlighting gateways and atomic exchanges as the most effective options for interoperability. Caldarelli [17] introduced the concept of the wrapped token, which separates the economic value represented by tokens from the operational costs of the underlying blockchain infrastructure. This work provides an overview of existing projects and their token issuance processes and explores the implications of centralization within blockchain systems. In addition, Haugum et al. [18] summarized the security and privacy challenges associated with blockchain and cross-chain technologies, identifying existing solutions and highlighting the limitations and shortcomings that need to be addressed.

Protocol construction. A number of existing classification methods for blockchain interoperability focus on the principles of the underlying cross-chain protocols. For example, Zamyatin et al. [19] proposed a framework for designing and evaluating CCCPs, with a particular emphasis on the inherent trust assumptions. They categorized generic CCCPs into three phases, i.e., commit, verify, and abort. For each phase, they provided a detailed analysis of the trust model, which may rely on a trusted third party (TTP). Similarly, Wang [20] discussed the basic principles for implementing blockchain interoperability, drawing on concepts like ACID [21] and SALT [22]. A distinction is made between cross-chain communications, which refer to processes between homogeneous and heterogeneous chains. Belchior et al. [23] conducted a literature review on blockchain interoperability and classified cross-chain schemes into three types, namely, public connectors, blockchain of blockchains, and hybrid connectors. They further classified public connectors into sidechains, notary schemes, and hash-time-lock contracts, and qualitatively evaluated these solutions based on asset management, trust establishment, cross-chain transaction realization, and extra-functional aspects. Additionally, they modeled blockchain interoperability using the ArchiMate modeling language [24], refactoring the layers of blockchain technology. In contrast, Lohachab et al. [25] provided a straightforward comparison of state-of-the-art cross-chain solutions, but they did not map these solutions to the blockchain architecture.

Performance evaluation. Several other studies have focused on evaluating the performance and capabilities of cross-chain projects. For example, Koens and Poll [31] assessed existing distributed ledger interoperability solutions by using multiple features, providing insights into the strengths and weaknesses of various cross-chain projects. Kazemi and Yazdinejad [32] aimed to develop requirement specifications for a blockchain interoperability platform. Their work also includes the development of open-source benchmark tools to facilitate performance and security research in blockchain interoperability. Mihaiu et al. [33] focused on the integrated management of cross-chain states and introduced the concept of cross-chain logic. They proposed a cross-chain evaluation framework that includes three metrics, i.e., end-to-end transaction latency, throughput, and overhead. This framework enables the assessment of cross-chain solutions based on their performance in these critical areas. Collectively, these studies contribute to the evaluation and advancement of cross-chain projects by providing evaluation metrics and valuable insights into the performance and capabilities of existing solutions.

Comparison to related literature review. Specifically, we compare our work with existing surveys that have focused on blockchain interoperability in several key aspects, as summarized in Table 1. For example, our study introduces a novel analysis model that conceptualizes both asset interoperability and data interoperability, with the goal of providing a comprehensive review that serves as a valuable reference for researchers. Unlike most of the aforementioned works, this paper not only introduces a new analytical model but also dives into a fine-grained classification of blockchain interoperability methods, providing a more detailed and nuanced exploration of this topic.

3. Background

In this section, we present the necessary background knowledge required to understand blockchain technology, including its foundation and operational mechanisms, as well as the core theories of blockchain interoperability.

3.1. A prime on blockchain technology

Blockchain technology [34] is a disruptive innovation that has the potential to transform industries by providing a secure, transparent, and decentralized method for recording transactions and managing data. Essentially, blockchain is a distributed ledger system where data are stored in blocks that are linked together in a chain. Once a block is added to the chain, it is nearly impossible to alter it without changing all the blocks. This immutability ensures that the data are secure and tamper-resistant.

Unlike traditional systems, where a central authority controls the database, blockchain operates on a P2P network where all participants maintain a copy of the ledger. This decentralization reduces the risk of data tampering, fraud, and single points of failure. Moreover, blockchain employs consensus mechanisms to validate and agree on the state of the ledger, ensuring that only legitimate transactions are added to the blockchain.

Beyond its initial application in cryptocurrencies like Bitcoin [1], blockchain has found use cases across various industries, such as DeFi [35], supply chain [36], and the IoT [37]. In addition, blockchain supports smart contracts, which are self-executing contracts with terms directly written into the code. Smart contracts represent digital agreements with coded rules that can be enforced autonomously without the need for a trusted intermediary. Once deployed, smart contracts are uploaded to the blockchain and distributed to all participating nodes [38].

In particular, blockchains can be divided into two types based on their access and openness [39].

- A permissioned blockchain restricts access to the network and typically involves a defined group of participants. It operates more like a controlled environment where the identity of participants is verified, and specific permissions are required for transactions and operations.
- A permissionless blockchain is an open network where anyone can participate without needing approval. These blockchains are typically decentralized and public, allowing unrestricted access to the system.

In addition, depending on their use and requirements, blockchains have been categorized into three types: public, private, and consortium [40].

- Public blockchains are open and decentralized networks where anyone can participate as a node, validate transactions, or develop applications. These blockchains operate on a trustless model and rely on consensus mechanisms such as proof-of-work (PoW) or proof-of-stake (PoS).
- Private blockchains are closed networks where access is restricted to specific participants, typically within a single organization. These blockchains are centrally controlled and used for internal purposes.
- Consortium blockchains are semi-decentralized networks controlled by a group of organizations rather than a single entity. These blockchains combine the benefits of public and private blockchains.

3.2. Blockchain interoperability

By investigating several foundational studies on blockchain interoperability [23,30], we formulate our own definition of this concept as follows:

Definition 1 *(Blockchain interoperability)*. Blockchain interoperability refers to the ability of different blockchain networks to communicate, share data, and interact with each other. This capability enables the transfer of assets, information, and value across different blockchain platforms that may have distinct protocols, consensus mechanisms, and structures.

The core idea of blockchain interoperability is closely related to distributed computing algorithms that address the agreement problem among participating processes [41,42]. The critical difference between blockchain interoperability and traditional distributed databases lies in the security model of interconnected systems. In traditional distributed databases, all processes are expected to follow protocol rules, with the worst-case scenario being a crash. However, in distributed ledgers, where consensus is maintained by a committee, Byzantine failures must also be considered and managed.

Based on the formal definition of Bitcoin and Ethereum, Borkowski et al. [43] formalized the cross-blockchain proof problem by deriving the lemma of rooted blockchains. They showed that it is practically impossible to prove the existence of certain data on one blockchain from another. To address this, they proposed a conceptual protocol for transferring specific types of assets across blockchains, showing how reversing the traditional order of asset transactions can potentially overcome the cross-chain proof problem. Their protocol only requires the participation of selfish witnesses [44], who are incentivized by a reward mechanism. Lafourcade and Lombard-Platet [45] argued that, under this definition, it is impossible for a blockchain to interact with anything outside of itself. However, by relaxing the definition, the possibility of interoperable blockchains emerges, although this effectively leads to the creation of a blockchain with two ledgers.

For cross-chain classification, Buterin [8] used a cause-effect graph to define and classify blockchain interoperability types into forward causation, backward causation, and dependency. Additionally, Vo et al. [46] formalized the interactions between consortium blockchains as a dependency graph. Herlihy [47] systematically analyzed the theoretical foundations of atomic cross-chain swap (ACCS) protocols, modeling the cross-chain swap process using a directed graph. They presented an ACCS protocol for this graph in the form of a hash-time locking contract. They also proved that an ACCS protocol exists if and only if the graph is strongly connected and the leader is the set of feedback vertices. However, their work does not dive into the fine-grained details of swap strategies and implementations. Zamyatin et al. [19] formalized the underlying research problem of cross-chain communication and related it to the fair exchange problem [48], demonstrating that it is impossible to achieve without a TTP. Collectively, these theoretical contributions provide a comprehensive guide to design protocols that bridge numerous distributed ledgers available today, aiming to facilitate clearer communication between academia, community, and industry.

4. Conceptual model

Put briefly, blockchain interoperability can be described as the ability of two or more blockchain systems to operate together, despite differences in their networks, consensus mechanisms, and smart contract languages. To clarify this definition, we examine materials related to blockchain interoperability and empirically observe that they can be modularly decomposed using a layered model. Inspired by this, we introduce a conceptual model that provides a holistic understanding of blockchain interoperability. Fig. 2 illustrates the conceptual model, which is designed to construct, analyze, and evaluate cross-chain solutions. Below, we first define the conceptual model from the perspective of understanding blockchain interoperability, followed by describing the details of the four components.

Definition 2 *(Conceptual model)*. A conceptual model is formulated to understand blockchain interoperability. Specifically, it (1) abstracts the concepts of data and asset interoperability by categorizing the different types of interoperability, (2) summarizes the evaluation metrics of blockchain interoperability by identifying its fundamental characteristics, and (3) continuously refines the evaluation metrics based on the evaluation of data and asset interoperability methods.

In the following, we elaborate on the conceptual model by introducing its four parts: type, ACID principle, construction, and evaluation.

4.1. Type

Particularly, blockchain interoperability can be summarized in four aspects, i.e., equipment, syntactic, semantic, and organizational, based on existing standards [49–51].

- Equipment interoperability is the ability to exchange data between infrastructure equipment produced by different vendors. This is primarily concerned with hardware components and protocols that enable machine-to-machine communication.

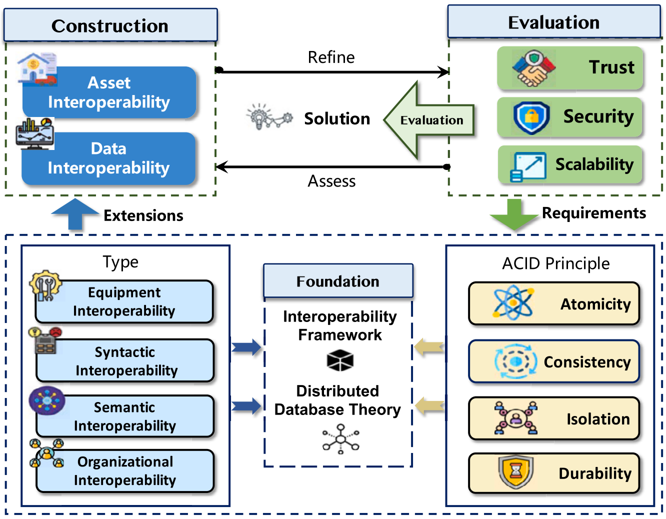

Fig. 2. The conceptual model for blockchain interoperability.

- Syntactic interoperability refers to the capability to interpret exchanged data even when different syntaxes are used. This involves the interpretation of various data formats and the conversion between different encoding or decoding mechanisms.
- Semantic interoperability is the ability to achieve a common understanding of the exchanged data, allowing for meaningful information exchange beyond mere data transfer.
- Organizational interoperability pertains to the ability to communicate and exchange information between different organizations.

4.2. *ACID principle*

In addition, the distributed nature of blockchain networks requires careful consideration of distributed data consistency during information exchange between blockchains. To ensure the reliability of these interactions, the ACID principle—which includes atomicity, consistency, isolation, and durability—is applied, similar to traditional database transactions.

- Atomicity ensures that a transaction is an indivisible unit of work, meaning that either all operations within the transaction are completed or none are.
- Consistency guarantees that the integrity constraints of the database are maintained before and after a transaction. This ensures that database transactions do not compromise the integrity of the relational data or the consistency of the business logic. When multiple transactions are accessed concurrently, they are isolated from each other, ensuring that one transaction does not affect the operations of another.
- Isolation ensures that in a concurrent environment, when different transactions manipulate the same data simultaneously, each transaction has its own complete data space. Changes made by concurrent transactions must be isolated from those made by any other concurrent transactions. When a transaction views data updates, it either sees the data as it was before another transaction modified it or after the modification was fully completed, never in an intermediate state.
- Durability ensures that once a transaction is completed, its changes to the database are permanent and cannot be rolled back.

4.3. *Construction*

The construction component summarizes two main categories: asset interoperability and data interoperability.

4.3.1. *Asset interoperability*

Asset interoperability involves the transfer and exchange of assets between two or more parties. An asset is a digital representation of value in various forms, including goods, services, currencies, and financial instruments such as stocks and bonds. On the blockchain, assets are primarily represented as tokens—such as Bitcoin or Ether—which can be securely stored and traded using cryptographic keys.

Asset interoperability is the initial driving force behind research on blockchain interoperability, centered around a fundamental question: How can users use Bitcoin to transact with other, subsequently developed blockchains? Specific scenarios [52] include the following: 1) Cross-chain asset transfer within the same account. For example, a user holds the same identity on two different blockchains (e.g., using the same public–private key pair) and wants to transfer an asset, such as Bitcoin, from blockchain A to blockchain B while maintaining ownership. 2) Cross-chain asset transactions between different accounts. For instance, user A seeks to exchange Ethereum (ETH) with user B's stablecoin (USDT) on another blockchain. 3) Cross-chain asset refunds. A user initiates a cross-chain asset transfer, but the transaction fails due to network disruptions, insufficient fees, or other issues. In this case, the assets must be refunded to the user's original account. Currently, three methods are used to achieve asset interoperability:

- Locking/destruction and minting. This method accomplishes asset transfer by locking or destroying assets on the source chain and minting corresponding assets on the target chain.
- Atomic cross-chain exchange. This approach directly converts assets on the source chain into assets on the target chain without requiring a TTP.
- Liquidity exchange. This method allows users to directly exchange native assets on another chain by establishing liquidity pools across different chains. A liquidity pool is a collection of funds locked in a smart contract and provided by liquidity providers.

Asset interoperability addresses the challenge of enabling users on different blockchains to trade with each other, ensuring that assets can be transferred and exchanged fairly across multiple blockchain networks.

4.3.2. *Data interoperability*

Data interoperability refers to the process of transferring and interacting with data across multiple blockchains. With the advent of smart contract technology, blockchain has evolved from a tamper-proof distributed ledger to a trusted state machine, broadening the scope of blockchain interoperability beyond asset transfer. Data interoperability enables the exchange of information between blockchains, facilitating more complex cross-chain logic, including cross-chain smart contracts and cross-chain oracles.

A cross-chain smart contract is a DApp consisting of multiple smart contracts deployed on different blockchain systems. Each contract on a different chain performs specific tasks, and they can communicate and cooperate to execute the overall application functionality. This approach allows cross-chain smart contracts to leverage the unique strengths of different blockchains. For example, the high throughput of one blockchain can be used for low-latency transactions, while the security features of another blockchain can be used to protect user privacy. Specifically, there are two main invocations in cross-chain smart contracts. In a coordinated commitment model, an external coordinator (such as a trusted party, decentralized oracle, or middleware) is responsible for independently invoking smart contracts on different blockchains. In a non-coordinated commitment model, a smart contract on a source chain interacts directly with another smart contract on a target chain using mechanisms such as relayers or inter-blockchain messaging protocols [53].

A cross-chain oracle is an application that obtains, verifies, and transmits external information to a smart contract running on the blockchain. Due to the deterministic nature of blockchain systems, smart contracts can typically access only on-chain data. Cross-chain oracles provide a mechanism to trigger smart contract functionality using off-chain data. Depending on their function, cross-chain oracles can be categorized into: (i) input oracles, which retrieve external data for on-chain contracts; (ii) output oracles, which send information from the blockchain to off-chain applications; (iii) computational oracles, which perform computational tasks off-chain.

4.4. Evaluation

Notably, to effectively construct asset and data interoperability, the evaluation component introduces three metrics to assess a cross-chain solution. Trust reflects the trust model of the cross-chain solutions. Security includes various aspects, such as data security, network security, and asset security, during the cross-chain process, while the scalability measures the ability of cross-chain solutions to be compatible with different blockchains.

- Trust focuses on the reliability and integrity of cross-chain processes. It evaluates how well participants can depend on the system without requiring central intermediaries. For example, the relay chain provides a trusted central hub for interconnecting various blockchains without intermediaries [54].
- Security assesses the robustness of cross-chain mechanisms against threats such as double-spending, replay attacks, and malicious actors. This ensures data integrity and protection throughout the interoperability process. For example, secure channels and proofs can be used to ensure safe asset transfers between blockchains with inter-blockchain communication (IBC) [55].
- Scalability measures how well the interoperability framework handles an increasing number of transactions, participants, or connected blockchains without compromising performance. For example, the cross-chain bridge (CCB) facilitates fast and cost-effective asset transfers across Ethereum-compatible blockchains [56].

5. Hierarchical analysis of cross-chain solutions

5.1. Three-layer architecture of the blockchain system

In this paper, we cast the blockchain architecture into a three-level structure, i.e., the network layer, the consensus layer, and the contract layer. Fig. 3 presents an overview of the three layers and the data interaction between them in a simplified way. While some blockchain interoperability studies [25] have divided the blockchain architecture into additional layers, such as the message cache layer and the gateway layer, we highlight that these layers can be included in our proposed three-layer architecture. For example, the network layer in our framework encompasses both the message cache and gateway layers, while the contract layer includes the data and application layers.

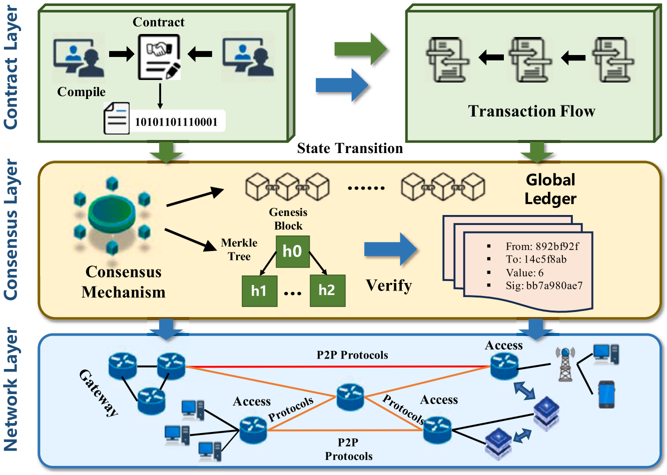

Fig. 3. The three-layer architecture of the blockchain system.

5.1.1. Network layer

The network layer includes elements such as node roles, network topology, and communication protocols between blockchain nodes. It is responsible for maintaining connections and transmitting messages in a distributed P2P network. Unlike centralized network systems, blockchain networks consist of distributed P2P nodes that work together to provide network services, with all nodes having equal status and no central authority. The Bitcoin network, which uses P2P technology, has nodes distributed across the internet, forming a flat, decentralized, reliable, and open network. P2P technology was initially used for file sharing, such as Nasper [57] and BitTorrent [58]. One of the main advantages of P2P architecture is its superior minimum distribution time compared to that of the client–server architecture. Here, the minimum distribution time refers to the shortest possible time required to fully distribute a piece of data from one or more source nodes to all participating nodes in the network. This means that the time required to distribute data over the network is inherently scalable; as the number of peer nodes increases, the minimum distribution time does not increase linearly but remains below a certain threshold [59].

In addition to P2P network protocols, the network layer of the blockchain includes node access protocols, mining pool protocols, and protocols related to other system components. These protocols are typically facilitated by gateway routing servers, which interface with the blockchain network protocols and extend network connectivity to individual nodes running different protocols. Although all nodes in a blockchain network hold equal status, they can be assigned specific roles based on their functions. For example, in the Bitcoin network [1], common node types include full nodes, light nodes, and mining nodes. Generally, a blockchain network is essentially a comprehensive network ecosystem that includes various types of nodes, gateway servers, network routers, and the necessary protocols for connectivity and communication. Each node not only verifies and propagates transaction information but also maintains connections with other peer nodes, ensuring the integrity and resilience of the network.

5.1.2. Consensus layer

The consensus layer is responsible for achieving distributed data consistency among blockchain nodes and is at the core of ensuring the integrity of the blockchain ledger. This layer includes consensus algorithms and the foundational security assumptions that underpin the network. In blockchain systems, data are redundantly stored in a distributed ledger as transactions, with the hash value of each transaction organized in a Merkle tree for transaction integrity verification [60]. The consensus mechanism, exemplified by PoW, allocates bookkeeping rights to nodes based on their computing resources, effectively increasing the cost for malicious actors and trading computing power for security. The higher the equity ratio, the greater the probability of obtaining bookkeeping rights. However, the demand for high computing power leads to the centralization of computing power, which reduces the decentralization of the blockchain network and the distribution of the network. Consensus algorithms such as Paxos [61] and its variants [62–64] achieve distributed data consistency through master–slave replication, allowing the network to continue functioning even when nodes fail or leave. However, these algorithms are less effective against malicious behavior by functioning nodes. On the other hand, algorithms such as practical Byzantine fault tolerance (PBFT) can tolerate malicious nodes as long as their number does not exceed one-third of the total nodes. PBFT is typically used in permissioned blockchains or databases. Additionally, incentive mechanisms are often implemented to reward positive behavior and penalize malicious actions, thereby promoting node efficiency and enhancing the overall security of the blockchain network.

5.1.3. Contract layer

The contract layer builds the execution environment for smart contracts and provides the foundation for users to develop applications based on the business logic. The concept of smart contracts was first proposed by Szabo [65]. In 2014, Wood [66] proposed a smart contract platform that enables distributed and trusted transactions on the blockchain. Transactions require the payment of a fee, commonly referred to as gas, which is associated with the execution of each instruction within a smart contract. In permissionless blockchains (e.g., Ethereum), gas fees serve to incentivize miners or validators and prevent abuse of computational resources. However, in permissioned blockchains, transaction fees may not be required or can be significantly reduced, as the controlled network often relies on alternative mechanisms for resource allocation and abuse prevention. Smart contracts are deterministic, indicating that their operations are triggered and executed exactly as specified when the contract conditions are met.

Ethereum employs stack-based bytecode to write smart contract code, which is executed on the Ethereum virtual machine (EVM). The operational state during execution can be represented as a tuple (*block_state*, transaction, message, code, memory, stack, program counter (pc), gas), where *block_state* refers to the global state, including all account and balance information. During each execution cycle, bytecode instructions are located using the pc, and the tuple is updated based on the content and result of the execution. In addition, there are many other smart contract platforms. For example, IBM's Hyperledger Fabric uses Docker containers to implement smart contracts and supports code written in the Go language [67]. Smart contracts simplify the development of consensus-based distributed applications, allowing users to create a variety of decentralized solutions.

A number of studies have advocated for integrating blockchain interoperability with the internet by establishing a standardized set of techniques and protocols [68,69]. Given that blockchain interoperability is still in its early stages and with the presence of numerous blockchain frameworks, there is an urgent need to develop a generic cross-chain standard that can accommodate the majority of existing blockchain systems. In this subsection, we first propose a hierarchical architecture for blockchain interoperability, which focuses on the different layers of blockchain technology and their corresponding protocol suites. We then use this architecture to systematize and classify existing cross-chain solutions, outline representative implementations, and discuss their practical considerations. Ultimately, this approach provides a comprehensive overview of blockchain interoperability, highlighting the challenges and opportunities in establishing a cohesive and widely adopted cross-chain standard.

5.2. Hierarchical architecture for blockchain interoperability

To provide a comprehensive overview of blockchain interoperability, we present a technical architecture designed for systematic study and classification. We adopt the DSR paradigm for information research [70,71], which includes six steps: problem identification, goal definition, design and development, demonstration, evaluation, and communication. As illustrated in Fig. 4, with the clear objective of creating a generic architecture applicable to different blockchain instantiations, we iteratively refine our design based on scientific literature. Specifically, we conduct an extensive literature review to identify the limitations of existing approaches [25,29] and incorporate established best practices in blockchain interoperability into our analysis.

Our proposed architecture is structured as a collection of technical layers that work together. As depicted in Fig. 5, the architecture is organized into three vertical layers: the network layer, the transaction layer, and the contract layer. Each layer comprises its own set of protocols, techniques, and abstractions that address different aspects of interoperability. By incorporating these fundamental layers of blockchain technology, our architecture effectively analyzes different cross-chain solutions. Additionally, this hierarchical structure helps practitioners gain a clearer understanding of the current state of cross-chain technology and make informed decisions about the most appropriate paths forward.

The different layers of the architecture work together to facilitate blockchain interoperability. Below, we introduce the functions of each layer.

Network layer. The network layer establishes the interconnection between independent blockchain networks or nodes. It uses CCCPs to

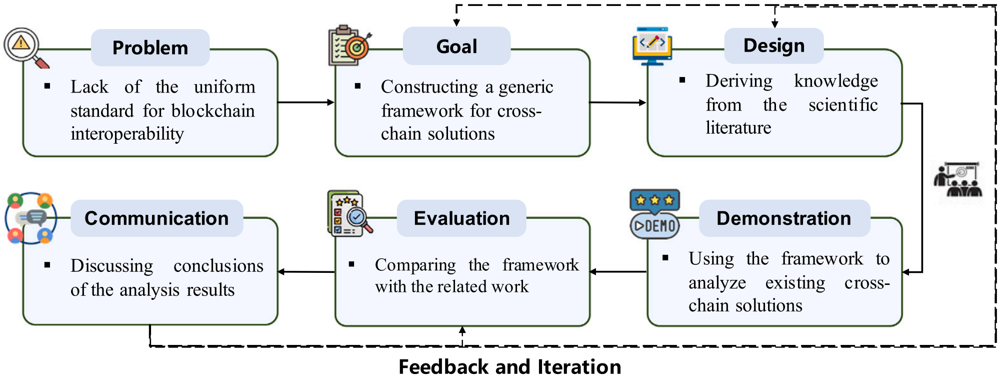
Problem
Lack of the uniform standard for blockchain interoperability
Goal
Constructing a generic framework for cross-chain solutions
Design
Deriving knowledge from the scientific literature
Communication
Discussing conclusions of the analysis results
Evaluation
Comparing the framework with the related work
Demonstration
Using the framework to analyze existing cross-chain solutions
DEMO
Feedback and Iteration

Fig. 4. The design science research (DSR) methodology for reviewing blockchain interoperability.

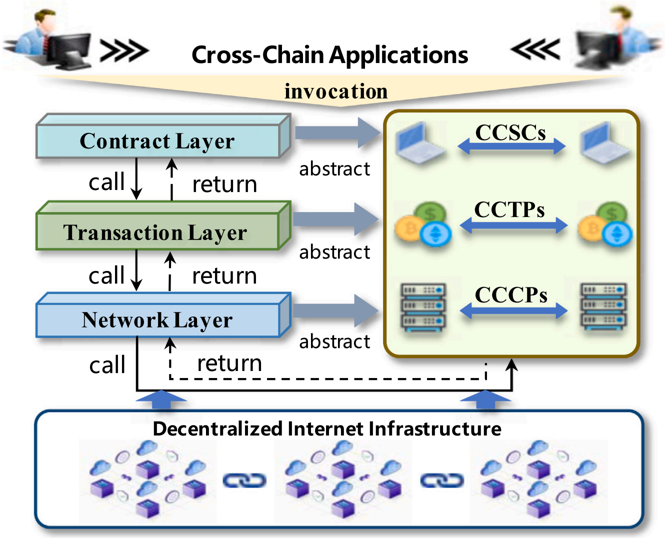

Fig. 5. The hierarchical architecture of blockchain interoperability.

standardize the construction of messages, define the meaning of fields, and outline detailed workflows. This layer is responsible for managing cross-chain communication and message transfer, maintaining connectivity and data synchronization between different blockchains and ensuring secure data transfer. It serves as the foundational layer that facilitates data exchange between different blockchain ecosystems.

Transaction layer. The transaction layer defines the rules and mechanisms for exchanging assets or information between accounts across different blockchains, primarily addressing asset interoperability through cross-chain transfer protocols (CCTPs) [72,73]. It oversees the transmission, verification, and validation of cross-chain transactions, ensuring their security and reliability. Key activities in this layer include verifying transaction signatures, recording timestamps, and preventing double-spending attacks. By maintaining the integrity of cross-chain transactions, the transaction layer ensures accurate and secure execution across multiple blockchain networks. While the network layer facilitates communication by transmitting messages, proofs, and events between blockchains, the transaction layer leverages this functionality to implement cross-chain protocols, such as asset transfers and trading. It relies on the network layer to monitor blockchain events, trigger corresponding actions, and synchronize states. This interaction spans the entire cross-chain processes, including transaction execution, event monitoring, failure recovery, and protocol finalization, thereby ensuring both operational efficiency and transaction integrity.

Contract layer. The contract layer enables interaction between DApps or external ports, leveraging cross-chain smart contracts (CCSCs) to facilitate versatile and flexible cross-chain operations. This layer manages operations related to smart contracts, allowing users to execute complex logic and conditional operations across different blockchains. The primary function of the contract layer is to execute and validate the terms and conditions of smart contracts, automatically triggering transactions or other on-chain operations once predefined conditions are met. The contract layer interacts closely with the transaction layer, particularly when a smart contract on one blockchain initiates or receives a transaction on another blockchain, with the transaction layer handling the subsequent processing.

The overall interoperability solution is built upon a layered architecture where each layer has distinct responsibilities. The network layer manages cross-chain communication by establishing the protocols necessary for data exchange between different blockchains. The transaction layer is responsible for executing and validating cross-chain transactions, ensuring that all asset transfers and exchanges are secure and accurate. The contract layer handles the management and execution of cross-chain smart contracts, enabling automated and complex operations that span multiple blockchain networks. These layers work in unison to ensure the security, validity, and automation of cross-chain asset transfers, ultimately enabling interoperability between disparate blockchain systems.

By applying the hierarchical architecture, we classify and analyze existing cross-chain solutions based on their specific functionalities, trust models, and security implications. By categorizing these solutions into distinct families, we can better understand their design rationales and use cases, which aids in reasoning about how each solution addresses the challenges of blockchain interoperability. This architecture allows for a more systematic evaluation of cross-chain technologies, providing insights into their effectiveness and potential for integration into broader blockchain ecosystems.

5.3. *Blockchain interoperability in the network layer*

In the network layer, disparate blockchain networks differ in their data structures, consensus algorithms, and transaction mechanisms, making communication between these systems a significant area of research. The network layer in blockchain interoperability abstracts the complexities involved in cross-chain communication, focusing on secure message transfer between different blockchain systems. This layer can be broadly divided into two categories: cross-chain connectors and multi-chain networks.

Cross-chain connectors are specialized protocols or mechanisms designed to facilitate communication between nodes in different blockchain networks. They handle the transmission of messages and data across distinct blockchains, ensuring that interactions between these networks are efficient and secure. These connectors often act as intermediaries, translating and relaying messages to ensure compatibility between different blockchain architectures. Multi-chain networks, on the other hand, provide a more comprehensive approach by establishing an overarching cross-chain ecosystem. This includes defining the blockchain network topology and inter-chain communication protocols necessary to enable interoperability across multiple blockchain platforms. Multi-chain networks aim to create a unified environment where different blockchains can interact seamlessly, allowing for greater scalability and flexibility in blockchain applications. The detailed results of the analysis are summarized in Table 2. Notably, we present the detailed analysis of each solution in Appendix A.1.

5.3.1. *Cross-chain connectors*

Cross-chain connectors facilitate cross-chain messaging by establishing hubs between blockchain networks or nodes. These hubs typically include routers, gateways, and associated protocols that regulate the message format and facilitate cross-chain messaging. By establishing these connections, cross-chain connectors enable communication between different blockchains, providing a critical foundation for achieving blockchain interoperability.

5.3.2. *Multi-chain networks*

A multi-chain network aims to create a decentralized infrastructure that connects different blockchains and enables communication between them. In this context, a multi-consensus model is often employed. This model involves the use of multiple consensus mechanisms across different interconnected blockchains, allowing the network to leverage the unique strengths of each algorithm. The goal is to address various requirements, including scalability, security, and transaction finality.

Table 2
Blockchain interoperability approaches in the network layer. ILP: interledger protocol; BFT: Byzantine fault tolerance; DPoS: delegated proof-of-stake; CCGP: cross-chain gateway protocol; CCRP: cross-chain router protocol; IBC: inter-blockchain communication; XCMP: cross-chain message passing; CCBP: cross-chain bridge protocol; LFT: loop fault tolerance; BTP: blockchain transmission protocol [74–76].

Categorie	Solution	Functionality		Trusted third party	Consensus	Protocol	Topology
		Asset	Data				
Cross-chain connector	ILP [77]	✓	✗	✓	BFT	Ledger-provided escrow	Connectors
	Axelar [74]	✓	✓	✗	DPoS and BFT	CCGP	Axelar blockchain
	Blockchain router [69]	✓	✓	✗	DS-PBFT	CCRP	Blockchain routers
Multi-chain network	Cosmos [78]	✓	✓	✗	Tendermint	IBC	Cosmos Hub
	Polkadot [79]	✓	✓	✗	Tendermint & HoneybadgerBFT	XCMP	Relay-chain
	Aion [75]	✓	✓	✗	Lightweight BFT-based protocol	CCBP	Aion network
	ICON [76]	✓	✓	✗	LFT	BTP	Nexus

Table 3
Blockchain interoperability approaches in the transaction layer.

Category	Solution	Reference
Cryptocurrency exchange	Centralized exchange	BTC relay [80] Polygon [81] Drivechain [82,83] XCLAIM [84]
	Decentralized exchange	Liquid [85] EtherDelta [86] Uniswap [87] 0x [88]
Cross-chain transaction protocol	Atomic cross-chain swap	HTLC [89] Arwen [90]
	Two-phase commit protocol	Wanchain [91]

Summary. Network-layer methods of cross-chain interoperability face challenges due to the complexity of coordinating multiple blockchains, latency issues from the time required to achieve consensus across different networks, and security risks from potential vulnerabilities in communication protocols or intermediary nodes. Additionally, these methods often lack standardization, making it difficult to ensure compatibility and integration across different blockchain platforms.

5.4. Blockchain interoperability in the transaction layer

Notably, the initial and still the most widely adopted application of blockchain technology is in finance, leading to the rapid growth of DeFi . By integrating classical financial theories, blockchain interoperability in the transaction layer enables efficient and cost-effective cross-chain asset transfers and exchanges. This type of interoperability is categorized into two main approaches: cryptocurrency exchanges and cross-chain transaction protocols. The details are summarized in Table 3. Notably, we have put the detailed analysis of each solution in Appendix A.2.

5.4.1. Cryptocurrency exchanges

Similar to traditional financial stock markets, cryptocurrency trading can be conducted through exchanges. There are two main types of exchanges for cross-chain trading: centralized exchanges (CEXs) and decentralized exchanges (DEXs).

Centralized exchange. CEXs facilitate cross-chain asset trading through a TTP and typically include a trade aggregation engine. Examples of popular CEX platforms include Coinbase [92], Kraken [93], and Binance [94]. In a CEX, users' wallets and private keys are managed by the exchange platform, meaning that the validity and execution of each transaction is centrally controlled by the exchange. Once users send their assets to a CEX, they relinquish direct control, as these assets are stored in a centralized database and held by a TTP until they are returned to the original account. While CEX platforms are known for their simplicity, speed, and strong liquidity, they also pose significant security risks due to their centralized structure [95].

Decentralized exchange. DEXs, on the other hand, provide only a trading aggregation service and do not take control of users' assets. Instead, users' assets are secured within open-source smart contracts, allowing users to initiate withdrawals at any time. In a DEX, trade orders from both parties are published on the blockchain, ensuring transparency and mitigating the risk of potential malicious market manipulation often associated with CEX platforms [96]. However, DEX platforms typically incur higher transaction fees and slower processing speeds compared to CEX platforms. Despite these drawbacks, DEX platforms have become increasingly popular in the realm of cross-chain projects. DEX platforms can be divided into two types based on their operating mechanisms: order-based DEX and liquidity pool-based DEX.

5.4.2. Cross-chain transaction protocol

Atomic cross-chain swap. The concept of ACCS was introduced by Tier Nolan in an online community forum [97], pioneering a method for two untrusted parties to securely exchange assets across different blockchains. The core principle behind ACCS is that either the exchange occurs as agreed, or both parties can recover their assets, thus ensuring a secure and atomic transaction.

Table 4
Blockchain interoperability approaches in the contract layer. SPV: simplified payment verification; BFT: Byzantine fault tolerance; PoS: proof-of-stake; API: Application Programming Interface; CTP: cross-chain transfer protocol; DPoS: delegated proof-of-stake.

Category	Solution	Reference	Functionality	Consensus
Cross-chain bridge	Proof-of-burn	Burn-to-claim [98,99]	Asset	BFT
	SPV proof	BTC relay [80]	Asset	BFT
		Polygon [81]	Asset	BFT
		Drivechain [82,83]	Asset	BFT
		XCLAIM [84]	Asset	BFT
	Multi-signature	Liquid [85]	Asset	BFT
		Wanchain [91]	Asset	Galaxy
	Proof-of-knowledge	Zendoo [100]	Asset	BFT
		Zk-Rollup [101]	Asset	BFT
		Way network [102]	Asset and data	BFT
		Polygon 2.0 [103]	Asset and data	PoS
Cross-chain application	Unified programming framework	HyperService [104]	Asset and data	BFT
		Overledger [105]	Asset and data	Customized
	Standard API	Bifröst [106]	Asset and data	Customized
	Application-level protocol	Axelar's CTP [107]	Asset and data	DPoS & BFT

Two-phase commit protocol. The two-phase commit (2PC) protocol involves a preparation phase where all participants signal readiness, followed by a commit phase where the transaction is finalized. If any participant fails to commit, the transaction is aborted across all chains.

Summary. Complex coordination of transactions across different blockchains can lead to increased latency and potential bottlenecks. The different transaction models and consensus mechanisms of different blockchains can create compatibility issues, making it difficult to ensure consistent transaction execution and state updates.

5.5. Blockchain interoperability in the contract layer

Smart contracts are essentially programs that are stored and executed on distributed ledgers, with their execution results agreed upon by multiple consensus participants before being recorded in blocks. The Turing completeness and robust programming capabilities of smart contracts enable blockchain systems to develop complex and versatile functionalities. In the context of blockchain interoperability, the contract layer plays a crucial role. Different blockchain platforms have developed various approaches to ensure that smart contracts can interact across multiple chains. This interoperability can be classified into several categories based on how smart contracts are integrated and executed across different blockchains. Below, we categorize contract layer blockchain interoperability into CCB and cross-chain application (CCA). For a more detailed breakdown, refer to Table 4. Notably, we present the detailed analysis of each solution in Appendix A.3.

5.5.1. Cross-chain bridge

A CCB can be defined as a set of applications designed to facilitate the transfer of assets across different blockchains by locking or destroying tokens on the source blockchain and unlocking or minting equivalent tokens on the destination blockchain. A crucial aspect of these cross-chain transfers is the state verification process, where the state of the destination blockchain is validated against the source blockchain. Below, we introduce four key types of CCB solutions—proof-of-burn (PoB), simplified payment verification (SPV) proof, multi-signature, and proof-of-knowledge—which represent the primary methods for constructing CCBs.

Proof-of-burn. PoB is used to destroy cryptocurrency in a verifiable manner, ensuring that the asset is permanently removed from circulation on the source chain [108]. This process begins by generating an unspendable cryptocurrency address on the source blockchain. Users then send assets to this address, effectively burning the assets. In return, they receive a PoB, which serves as evidence that the asset has been irrevocably destroyed. On the destination blockchain, users can verify that asset transfer has occurred by verifying the PoB.

Simplified payment verification proof. Since validating all block data is impractical for cross-chain communication, light client validation is the most commonly used approach. This method enables transaction verification without requiring access to or storage of the entire ledger. An SPV proof allows the target blockchain to confirm whether a transaction is successfully committed by examining the block header of the source blockchain. SPV proof bridges rely on lightweight clients that verify cross-chain transactions using Merkle proofs derived from blockchain headers instead of requiring the full blockchain [82,109,110].

Multi-signature. Multi-signature bridges involve a group of validators or custodians who collectively manage the cross-chain asset transfer process. A quorum of validators must sign off on each transaction for it to be considered valid. Validators monitor the source blockchain for relevant transactions. Once a consensus is reached, the corresponding transaction is executed on the target blockchain.

Proof-of-knowledge. CCBs facilitate the transfer of assets or data between different blockchains, but these processes inherently require trust. Proof-of-knowledge uses cryptographic proofs, such as zero-knowledge proofs (ZKPs), to validate the correctness of cross-chain transactions without revealing sensitive data. Proof-of-knowledge can be employed within CCBs to verify claims without revealing sensitive data and strengthen validation mechanisms. In addition, CCBs often involve relayers or validators that facilitate transactions across chains. Using proof-of-knowledge is able to prevent fraudulent claims.

5.5.2. Cross-chain application

We categorize CCAs into three main types: unified programming framework, standard application programming interface (API), and application-level protocol.

Unified programming framework. A unified programming framework provides developers with a consistent environment for building CCA. It acts as a middleware layer, simplifying the development process by providing standardized tools, libraries, and protocols for cross-chain functionality.

Standard API. A standard API provides a set of predefined interfaces for cross-chain interactions, enabling applications to access and use blockchain services in a uniform way. These APIs define how applications communicate with different blockchain networks without requiring knowledge of the underlying implementation.

Application-level protocol. Application-level protocols are tailored for specific use cases and define the rules and mechanisms for cross-chain interactions directly at the application layer. These protocols address the functional requirements of CCAs and often work on top of existing blockchain infrastructures.

Summary. The complexity of integrating smart contracts from different chains can lead to difficulties in maintaining atomicity and preventing race conditions during cross-chain operations. In addition, the lack of standardized frameworks for cross-chain smart contracts increases the risk of vulnerabilities and security breaches.

6. Discussion

In this section, we discuss the limitations of cross-chain solutions from the network, transaction, and contract layers. While existing reviews on blockchain interoperability, such as Refs. [25,29] have proposed multi-layered cross-chain frameworks, we argue that our proposed three-layer architecture is sufficient to analyze current cross-chain solutions. This can be attributed to the following factors.

- Most existing cross-chain solutions focus primarily on these three layers, which are central to blockchain interoperability.
- Furthermore, the additional layers defined in other studies can be subsumed within our three-layer model. For example, the network layer in our architecture encompasses both the message cache layer and the gateway layer [25], while the transaction layer includes the data layer and the consensus layer [29].

Network layer. CCCPs are essential for connecting different blockchains and facilitating message transmission between them. A basic approach is to use point-to-point connectors such as the interledger protocol (ILP) [77], which function as central hubs that process and route cross-chain data packets. ILP employs a ledger-provided escrow method for secure transactions. However, a more widely discussed method is cross-chain routing, where blockchain routers and routing protocols maintain cross-chain topologies and messages in a decentralized manner. Despite its distributed nature, this approach often relies on a relaying institution or a network of selected validators, raising concerns about decentralization and creating a trade-off.

As blockchain projects proliferate, distributed CCAs require a more robust resource pool to meet increasing throughput demands. This has led to the emergence of multi-chain networks, which use bridges and trustless protocols to foster a comprehensive cross-chain ecosystem. A multi-chain infrastructure, in particular, integrates different blockchain interfaces and facilitates data and value exchange across the network, allowing applications to operate on any connected blockchain.

A multi-chain infrastructure is a blockchain architecture that supports the interaction, communication, and interoperability of multiple independent blockchains within a unified framework. This infrastructure allows different blockchains—each with its protocols, consensus mechanisms, and functionalities—to connect, exchange data, and transfer value. Examples of such infrastructures include Cosmos, which uses the IBC protocol, and Polkadot, which uses cross-chain message passing (XCMP) to enable interactions between its parachains. Both systems provide standardized communication channels, although the concept of a multi-chain infrastructure can be extended to more heterogeneous approaches where different interfaces coexist.

From a technical perspective, the multi-chain network is similar to the horizontal partitioning of a database [111], where the data stored in a global database are divided into multiple databases with the same table structure. This division reduces the data volume in each database and allows it to be distributed across different physical servers, theoretically allowing unlimited horizontal scaling of the database. However, the challenge of adapting to different consensus mechanisms limits the widespread use of this approach. To address this, multi-chain network projects such as Cosmos [78] and Polkadot [79] have adopted a multi-consensus model to process on-chain data more efficiently. These models schedule consensus tasks across multiple blockchains, extending the performance of individual nodes. For instance, Polkadot uses a heterogeneous multi-consensus model through its relay chain and parachains, where each parachain can implement its consensus mechanism while interacting with the relay chain, which provides a unified security framework. This design allows different blockchains within the Polkadot ecosystem to maintain their unique consensus protocols while ensuring communication and transaction finality across chains. Similarly, Cosmos takes a multi-consensus model by enabling each blockchain within its network to operate independently with its consensus mechanism, while using the Tendermint consensus algorithm for the overarching IBC protocol. This implementation efficiently executes cross-chain operations by harmonizing different consensus protocols within a cohesive framework, promoting interoperability without compromising the individual autonomy of each blockchain.

Transaction layer. In the transaction layer, cross-chain solutions are critical to enable secure asset transfers, data exchanges, and interactions between different blockchain networks. This layer deals directly with the mechanics of transactions—how they are initiated, verified, and finalized across different blockchains. In the transaction layer, most DEXs, such as EtherDelta [86], 0x [88], and SparkSwap [112], are P2P trading systems that limit liquidity. On-chain protocols such as EtherDelta and 0x suffer from slow trade execution because they are limited by the speed at which blockchains confirm blocks.

One of the approaches is the ACCS. ACCS allows two parties to exchange assets across different blockchains without the need for a TTP. This method ensures that either both transactions are executed or neither is executed, thus maintaining the integrity of the exchange. However, while ACCS provides a trustless mechanism, it is often criticized for its inefficiency. This problem arises when one party deliberately delays or cancels the transaction, resulting in the temporary immobilization of assets, which can be both frustrating and economically damaging.

ACCS provides a trustless means of exchanging assets within a transaction, akin to a common payment. In ACCS, traders' assets are locked in smart contracts until the trade is either completed or the timeout period expires. The timeout mechanism is designed to prevent assets from being locked indefinitely, but to ensure safe trading, ACCS often uses timeout periods of several hours, which can lead to inefficiencies. This long duration can lead to "lock-up griefing", where one trader manipulates the other into locking assets unnecessarily, as discussed by Chesney et al. [113]. The synchronicity assumption of ACCS requires a timely response from smart contracts, which can cause race conditions. Therefore, in practical implementations, ACCS is often combined with other approaches to address usability and efficiency issues, as suggested by Tairi et al. [114].

Another important method is the use of multi-signature schemes in cross-chain transactions. Multi-signature requires multiple parties, often a consortium, to sign off on a transaction before it can be executed. This method enhances the security and trustworthiness of cross-chain transactions by ensuring that there is a majority approval for the transaction to proceed. However, relying on a consortium introduces a level of centralization, which may conflict with the decentralized ethos of many blockchain projects. Moreover, organizing and maintaining a trusted consortium can be challenging and may lead to governance issues over time.

Contract layer. In the contract layer, various algorithms and strategies have been proposed to validate states across heterogeneous blockchains, enabling cross-chain smart contracts. Given the redundancy and diversity of blockchain data, validation using blockchain light clients, such as two-way-peg, is a more practical approach to achieve independent cross-chain interactions without modifying the original blockchain protocols. Based on the assumption that confirmed blocks contain only valid transactions, as proposed in Ref. [1], it is sufficient to verify block headers and the transactions related to cross-chain operations rather than the entire blockchain. Block headers serve as metadata for the corresponding blocks, using Merkle trees to reference all transaction commitments within the block.

However, simple solutions such as SPV proofs result in proof complexity that is linear in the length of the blockchain. To address this, techniques have been developed that achieve sublinear complexity through probabilistic sampling. For example, non-interactive proofs of PoW [115,116] enable a poly-logarithmic number of block header verifications.

Despite these advancements, the assumption that blocks reaching consensus contain only valid transactions is both optimal and limited, as conflicting transactions may still be present and would need to be verified and rejected in full verification mode. To ensure the validity, proof-of-knowledge or fraud-proof mechanisms can be employed. Moreover, combining light client verification protocols with ZKPs can serve as an effective performance optimization method due to their compression properties.

However, the two-way-peg approach is limited by high transaction costs and long latency, as noted by Back et al. [117]. Additionally, this method is vulnerable to exploitation by powerful miners, who may attempt to steal assets from pegged blockchains. A multi-signature scheme addresses these issues by requiring a consortium to enforce trust among participants through multi-signature transactions. By requiring most consortium members to sign blocks, this approach prevents sidechain reorganizations and avoids any additional loss of security.

Summary. The network layer facilitates communication through protocols such as IBC and XCMP, leveraging multi-consensus models to strike a balance between scalability and security. The transaction layer focuses on secure and efficient asset exchanges, employing mechanisms such as atomic cross-chain swaps and multi-signature schemes, although these approaches involve trade-offs in decentralization and usability. The contract layer enables state validation across blockchains using lightweight client verification, fraud proofs, and ZKPs while dealing with challenges such as proof complexity and the risk of miner exploitation in two-way-peg systems. Collectively, these findings highlight the need for robust, decentralized, and scalable mechanisms to meet the growing demands of cross-chain ecosystems and to enable seamless interaction across diverse blockchain networks.

7. Open challenges and future directions

In this section, we identify the unresolved challenges associated with blockchain interoperability from the perspectives of security migration, trust enhancement, and scalability improvement. For each of these aspects, we suggest several potential research directions.

7.1. Security migration

The evolution of the internet has underscored an important lesson: technologies developed without sufficient attention to security are inevitably vulnerable to unforeseen threats. In the area of blockchain interoperability, we are able to integrate robust security measures before its widespread adoption occurs. While security concerns within single-chain ecosystems have been extensively studied, the rise of the cross-chain paradigm introduces new risk factors that could fundamentally alter the existing security model. Recent attacks on CCBs, resulting in losses amounting to hundreds of millions of dollars, have exposed the dangers associated with centrally managed and large-scale assets and their potential points of failure. These breaches are primarily attributed to vulnerabilities in back-end services, multi-signature schemes, and smart contracts. Therefore, it is imperative to improve the security of blockchain interoperability. This discussion focuses on three critical security aspects: cryptography standardization, privacy protection, and permission regulation.

Cryptography standardization. Independent blockchain systems often employ different cryptographic primitives, such as hashing algorithms, asymmetric cryptography algorithms, and digital signature algorithms. This variation in cryptographic implementations can introduce security vulnerabilities in the absence of reliable interaction protocols. For example, differences in the hash algorithms used within hash time locked contracts (HTLCs) could expose the system to preimage attacks. Establishing a unified set of blockchain cryptographic standards would mitigate these risks, reducing the need to bolster security across blockchains due to inconsistent cryptographic practices. While many cryptographic protocols are already well developed and widely deployed, cross-chain protocols still require further refinement. This ongoing need for improvement underscores the feasibility and effectiveness of establishing standardized protocols across blockchain systems.

Privacy protection. As a finance-driven system, the anonymity of accounts and transactions is critical in blockchain technology. Privacy protection has received considerable attention in both academia and industry. Sensitive data stored on ledgers can be secured using techniques such as anonymization, data desensitization, and differential privacy [118]. In addition, methods such as information hiding and address obfuscation ensure the traceability and unlinkability of large transactions. For example, coin-mixing technology [119,120] enhances privacy by severing the link between cryptocurrency senders and receivers, while the lightning network and onion routing provide additional protection [121,122]. However, the diversity of privacy mechanisms across different blockchains, the performance overhead they introduce, and the need for compatibility between these mechanisms pose significant challenges. Balancing security, performance, and consistency is essential for achieving effective privacy protection in cross-chain protocols.

Permission regulation. The varying permission rules across blockchains, such as public, consortium, and private, have a significant impact on the design and assignment of roles and functions for blockchain nodes. For example, public blockchains are more vulnerable to Sybil attacks compared to consortium or private blockchains, as they lack strict authentication mechanisms [123]. This underscores the need for interoperable blockchains to develop a unified permission management system. This system standardizes the identification and voting weights of nodes, whether based on work or stake, allowing for consistent measurement, comparison, and ranking. This approach requires a unified and robust security model to ensure reliable interoperability between different blockchain systems.

7.2. Trust enhancement

The predominant cross-chain implementations, such as notary schemes, sidechains or relays, and hash-locking, inherently depend on specific trust anchors that can affect the degree of decentralization of the system. Following previous work [20], we divide the trust model of cross-chain protocols into two main categories: a TTP and synchrony. Ref. [19] demonstrated that the development of trustless blockchain interoperability protocols without a TTP is fundamentally unattainable. Consequently, CEXs and DEXs remain the preferred methods for facilitating cross-chain transactions, with ACCSs employed as a complementary measure to mitigate trust issues. After a comprehensive analysis of existing cross-chain solutions, we identify several promising developments that could address and enhance these trust-related challenges.

Fine-grained trust model. To achieve decentralized cross-chain verification, a more refined trust model for blockchain interoperability is essential. Unlike traditional models, which often rely on a binary notion of trust, a fine-grained approach allows the specification of varying levels of trustworthiness for different entities, such as nodes, validators, and oracles. This nuanced approach allows cross-chain protocols to manage and mitigate risks associated with differing trust levels more effectively, thereby enhancing security, reducing reliance on centralized intermediaries, and enabling more seamless and secure interactions between diverse blockchain systems. This trust model can be derived from the formalization of decentralization levels within blockchains, taking into account factors such as the number of verification nodes, election methods, and multi-signature algorithms. Furthermore, an evaluation and feedback mechanism should be integrated to support and refine the development of blockchain interoperability, ensuring continuous improvement in trust management.

Trusted computing environment. Developing trustless cross-chain solutions that incorporate hardware security modules represents a key advancement in blockchain interoperability. A trusted computing environment ensures that the code and data involved in cross-chain transactions are protected from tampering and unauthorized access, thereby enhancing the overall security and reliability of the interoperability process. For example, Bentov et al. [124] facilitated real-time cross-chain cryptocurrency transactions using a trusted execution environment (TEE), which effectively mitigates front-running attacks—exploits that take advantage of blockchain latency, as discussed by Refs. [125,126]. Additionally, to increase trust in blockchain applications, Scheid et al. [106] proposed operating their system within the software guard extension (SGX) environment.

7.3. Scalability improvement

Several factors contribute to blockchain performance, including block size, confirmation time, and processing latency. Efficient communication between blockchains with different transaction speeds remains a significant challenge. In addition, while technologies such as sidechains and state channels aim to improve blockchain scalability, cross-chain technologies can introduce additional performance overhead. Below, we discuss scalability improvements for cross-chain interoperability in terms of virtualized consensus, hardware acceleration, blockchain-based network protocols, and token simplification.

Virtualized consensus. Currently, most cross-chain solutions focus on cross-chain communication, transactions, and smart contracts, leaving the cross-chain consensus layer uncovered. The prevailing approach typically involves bypassing the consensus layer or integrating a unified consensus mechanism. However, this strategy fails to leverage the significant benefits of diverse consensus practices, and the inherent limitations of a single consensus algorithm limit its flexibility. Therefore, it is essential to develop cross-consensus protocols that enable effective cross-chain transaction verification and confirmation. Virtualized consensus abstracts the consensus process, enabling different blockchains to reach an agreement without relying on a specific consensus algorithm. Furthermore, consensus virtualization can optimize resource utilization by partitioning consensus tasks and efficiently scheduling the verification process. With its inherent flexibility and scalability, virtualized consensus allows diverse blockchains to interact without compromising their unique consensus models, improving the overall interoperability and efficiency of cross-chain operations. Although the 2PC protocol, which achieves agreement across distributed systems, can be considered a form of virtualized consensus, it suffers from the significant drawback of message blocking.

Hardware acceleration. Hardware acceleration has become a key trend in blockchain system design and development. Using devices such as field programmable gate arrays (FPGAs) and graphics processing units (GPUs), blockchain accelerators can greatly improve the performance of transaction verification processes. By implementing cross-chain algorithms in hardware, accelerators can speed up cryptographic operations and transaction validation, thereby reducing latency and improving scalability. This optimization increases the performance of cross-chain interactions, ensuring secure and efficient communication between different blockchain systems. These advancements are critical for supporting large-scale DApps and enhancing blockchain interoperability.

Blockchain-based network protocols. Blockchain-based network protocols improve blockchain interoperability by establishing standardized communication frameworks that streamline data exchange and transaction processing between various blockchains. These protocols ensure consistent and secure interactions across different networks, reduce complexity, and enable more efficient cross-chain operations. By standardizing communication methods, these protocols facilitate the integration of disparate blockchain systems into a cohesive and interoperable ecosystem.

Token simplification. Unlike traditional systems, blockchain ecosystems require consideration of economic benefits, as evidenced by the proliferation of various cryptocurrencies leading to a fragmented market. Token simplification can address this challenge by standardizing token formats and reducing the complexity of token structures. This streamlining of digital asset representation and management facilitates efficient asset transfers and interactions across different blockchains. By minimizing compatibility issues and simplifying the cross-chain exchange process, token simplification is able to enhance interoperability and reduce friction in multi-chain environments.

8. Conclusions

In this survey, we explore recent trends in blockchain interoperability technologies, distinguish our work from previous studies, and provide a comprehensive summary of key principles, including blockchain technology, theoretical foundations, and a conceptual model. By examining the underlying technical aspects, we propose a layered blockchain interoperability architecture that provides a thorough overview of cross-chain technologies. This architecture maps existing solutions into three distinct layers, allowing us to detail the background, motivation, design, implementation, evaluation, and limitations of each cross-chain technique.

While existing solutions have advanced cross-chain asset transfers and data sharing, they often lack a unified approach to integrate different blockchain platforms. The architectural models analyzed in our survey suggest that the combination of secure cryptographic protocols, standardized APIs, and modular frameworks can significantly improve the interoperability landscape. However, further improvements are required, particularly in areas such as scalability, security, and ease of integration. Future efforts should prioritize the development of more robust frameworks that address not only the technical aspects of interoperability but also governance, regulatory compliance, and user adoption. By refining these models and broadening their applicability, the blockchain ecosystem can evolve into a more interconnected and efficient network.

CRediT authorship contribution statement

Wenqing Li: Writing – original draft, Methodology, Conceptualization. **Zhenguang Liu:** Writing – review & editing. **Jianhai Chen:** Visualization, Investigation. **Zhe Liu:** Writing – review & editing. **Qinming He:** Supervision.

Funding

This work was supported by the “Leading Goose Project Plan” of Zhejiang Province under Grant 2022C01086. We thank the anonymous reviewers for their constructive comments on improving this paper.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix. Supplementary material

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.bcra.2025.100286.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, 2008. (Accessed 5 December 2024).

[2] V. Buterin, A next-generation smart contract and decentralized application platform, https://courses.cs.duke.edu/spring23/compsci512/papers/ethereum.pdf, 2014. (Accessed 5 December 2024).

[3] M. Mettler, Blockchain technology in healthcare: the revolution starts here, in: Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2016, pp. 1–3, https://doi.org/10.1109/healthcom.2016.7749510.

[4] Q. Wang, X. Zhu, Y. Ni, et al., Blockchain for the iot and industrial iot: a review, Internet of Things 10 (2020) 100081, https://doi.org/10.1016/j.iot.2019.100081.

[5] T.N. Dinh, M.T. Thai, AI and blockchain: a disruptive integration, Computer 51 (9) (2018) 48–53, https://doi.org/10.1109/mc.2018.3620971.

[6] Q. Yang, Y. Zhao, H. Huang, et al., Fusing blockchain and AI with metaverse: a survey, IEEE Open J. Comput. Soc. 3 (2022) 122–136, https://doi.org/10.1109/OJCS.2022.3188249.

[7] J. Vom Brocke, A. Hevner, A. Maedche, Introduction to design science research, in: J. Brocke, A. Hevner, A. Maedche (Eds.), Des. Sci. Res. Cases, Springer, Cham, 2020, pp. 1–13, https://doi.org/10.1007/978-3-030-46781-4_1.

[8] V. Buterin, Chain interoperability, R3 Res. Pap. 9 (2016) 1–25.

[9] I.A. Qasse, M. Abu Talib, Q. Nasir, Inter blockchain communication: a survey, in: Proceedings of the ArabWIC 6th Annual International Conference Research Track, ACM, 2019, pp. 1–6, https://doi.org/10.1145/3333165.3333167.

[10] R. Bhatia, et al., Interoperability solutions for blockchain, in: Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), IEEE, 2020, pp. 381–385, https://doi.org/10.1109/icstcee49637.2020.9277054.

[11] S. Lin, Y. Kong, S. Nie, Overview of block chain cross chain technology, in: Proceedings of the 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), IEEE, 2021, pp. 357–360, https://doi.org/10.1109/icmtma52658.2021.00083.

[12] W. Ou, S. Huang, J. Zheng, et al., An overview on cross-chain: mechanism, platforms, challenges and advances, Comput. Netw. 218 (2022) 109378, https://doi.org/10.1016/j.comnet.2022.109378.

[13] A. Singh, K. Click, R.M. Parizi, et al., Sidechain technologies in blockchain networks: an examination and state-of-the-art review, J. Netw. Comput. Appl. 149 (2020) 102471, https://doi.org/10.1016/j.jnca.2019.102471.

[14] M. Borkowski, D. McDonald, C. Ritzer, et al., Towards atomic cross-chain token transfers: State of the art and open questions within tast, Distributed Systems Group TU Wien (Technische Universit at Wien), Report 8, 2018, https://doi.org/10.13140/RG.2.2.10769.48489.

[15] S. Schulte, M. Sigwart, P. Frauenthaler, et al., Towards blockchain interoperability, in: C.D. Ciccio, R. Gabryelczyk, L. García-Bañuelos, et al. (Eds.), Business Process Management: Blockchain and Central and Eastern Europe Forum, Springer, Cham, 2019, pp. 3–10, https://doi.org/10.1007/978-3-030-30429-4_1.

[16] A. Lipton, T. Hardjono, Blockchain intra- and interoperability, in: V. Babich, J.R. Birge, G. Hilary (Eds.), Innovative Technology at the Interface of Finance and Operations, Springer, Cham, 2022, pp. 1–30, https://doi.org/10.1007/978-3-030-81945-3_1.

[17] G. Caldarelli, Wrapping trust for interoperability: a preliminary study of wrapped tokens, Information 13 (1) (2021) 6, https://doi.org/10.3390/info13010006.

[18] T. Haugum, B. Hoff, M. Alsadi, et al., Security and privacy challenges in blockchain interoperability-a multivocal literature review, in: Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022, ACM, 2022, pp. 347–356, https://doi.org/10.1145/3530019.3531345.

[19] A. Zamyatin, M. Al-Bassam, D. Zindros, et al., SoK: communication across distributed ledgers, in: N. Borisov, C. Diaz (Eds.), Financial Cryptography and Data Security, Springer, Berlin, 2021, pp. 3–36, https://doi.org/10.1007/978-3-662-64331-0_1.

[20] G. Wang, Sok: Exploring blockchains interoperability, https://eprint.iacr.org/2021/537, 2021. (Accessed 5 December 2024).

[21] T. Härder, Dbms architecture–still an open problem, in: Datenbanksysteme in Business, Technologie und Web, 11. Fachtagung des GIFachbereichs "Datenbanken und Informationssysteme"(DBIS), Gesellschaft für Informatik eV, 2005, pp. 2–28.

[22] C. Xie, C. Su, M. Kapritsos, et al., Salt: combining {ACID} and {BASE} in a distributed database, in: Proceedings of 11th USENIX Symposium on Operating Systems Design and Implementation, ACM, 2014, pp. 495–509, https://doi.org/10.1145/3530019.3531345.

[23] R. Belchior, A. Vasconcelos, S. Guerreiro, et al., A survey on blockchain interoperability: past, present, and future trends, ACM Comput. Surv. 54 (8) (2021) 1–41, https://doi.org/10.1145/3471140.

[24] M.M. Lankhorst, H.A. Proper, H. Jonkers, The architecture of the archimate language, in: T. Halpin, J. Krogstie, S. Nurcan (Eds.), Enterprise, Business-Process and Information Systems Modeling, Springer, Berlin, 2009, pp. 367–380, https://doi.org/10.1007/978-3-642-01862-6_30.

[25] A. Lohachab, S. Garg, B. Kang, et al., Towards interconnected blockchains: a comprehensive review of the role of interoperability among disparate blockchains, ACM Comput. Surv. 54 (7) (2021) 1–39, https://doi.org/10.1145/3460287.

[26] N. Kannengießer, M. Pfister, M. Greulich, et al., Bridges between islands: Cross-chain technology for distributed ledger technology, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, ScholarSpace, 2020, pp. 5298–5307, https://doi.org/10.24251/HICSS.2020.652.

[27] G. Llambias, L. González, R. Ruggia, Blockchain interoperability: a feature-based classification framework and challenges ahead, CLEI Electron. J. 25 (3) (2022) 1-29, https://doi.org/10.19153/cleiej.25.3.4.

[28] S. Zhu, C. Chi, Y. Liu, A study on the challenges and solutions of blockchain interoperability, China Commun. 20 (6) (2023) 148–165, https://doi.org/10.23919/jcc.2023.00.026.

[29] H. Jin, X. Dai, J. Xiao, Towards a novel architecture for enabling interoperability amongst multiple blockchains, in: Proceedings of 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2018, pp. 1203–1211, https://doi.org/10.1109/ICDCS.2018.00120.

[30] K. Ren, N.-M. Ho, D. Loghin, et al., Interoperability in blockchain: a survey, IEEE Trans. Knowl. Data Eng. 35 (12) (2023) 12750–12769, https://doi.org/10.1109/tkde.2023.3275220.

[31] T. Koens, E. Poll, Assessing interoperability solutions for distributed ledgers, Pervasive Mob. Comput. 59 (2019) 101079, https://doi.org/10.1016/j.pmcj.2019.101079.

[32] M. Kazemi, A. Yazdinejad, Towards automated benchmark support for multi-blockchain interoperability-facilitating platforms, arXiv, 2021, preprint, arXiv:2103.03866.

[33] I. Mihaiu, R. Belchior, S. Scuri, et al., A framework to evaluate blockchain interoperability solutions, 2021, https://doi.org/10.36227/techrxiv.17093039.

[34] Z. Zheng, S. Xie, H.-N. Dai, et al., Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375, https://doi.org/10.1504/ijwgs.2018.095647.

[35] Y. Chen, C. Bellavitis, Blockchain disruption and decentralized finance: the rise of decentralized business models, J. Bus. Venturing Insights 13 (2020) e00151, https://doi.org/10.1016/j.jbvi.2019.e00151.

[36] P. Dutta, T.-M. Choi, S. Somani, et al., Blockchain technology in supply chain operations: applications, challenges and research opportunities, Transp. Res., Part E, Logist. Transp. Rev. 142 (2020) 102067, https://doi.org/10.1016/j.tre.2020.102067.

[37] X. Wang, X. Zha, W. Ni, et al., Survey on blockchain for Internet of things, Comput. Commun. 136 (2019) 10–29, https://doi.org/10.1016/j.comcom.2019.01.006.

[38] IBM, What are smart contracts on blockchain?, https://www.ibm.com/topics/smart-contracts. (Accessed 5 December 2024).

[39] A. Miller, Permissioned and permissionless blockchains, in: Blockchain for Distributed Systems Security, 2019, pp. 193–204, https://doi.org/10.1002/9781119519621.ch9.

[40] S. Bouraga, A taxonomy of blockchain consensus protocols: a survey and classification framework, Expert Syst. Appl. 168 (2021) 114384, https://doi.org/10.1016/j.eswa.2020.114384.

[41] P.A. Bernstein, V. Hadzilacos, N. Goodman, et al., Concurrency Control and Recovery in Database Systems, Addison-Wesley Publishing Company, Boston, 1987.

[42] O. Babaoglu, S. Toueg, Understanding non-blocking atomic commitment, Distrib. Syst. (1993) 147–168.

[43] M. Borkowski, C. Ritzer, D. McDonald, et al., Caught in chains: claim-first transactions for cross-blockchain asset transfers, in: Whitepaper, vol. 56, Technische Universität Wien, 2018, pp. 57–58, https://doi.org/10.13140/RG.2.2.24191.25769.

[44] M. Borkowski, C. Ritzer, S. Schulte, Deterministic witnesses for claim-first transactions, http://dsg.tuwien.ac.at/staff/mborkowski/pub/tast/tast-white-paper-3.pdf, 2018. (Accessed 5 December 2024).

[45] P. Lafourcade, M. Lombard-Platet, About blockchain interoperability, Inf. Process. Lett. 161 (2020) 105976, https://doi.org/10.1016/j.ipl.2020.105976.

[46] H.T. Vo, Z. Wang, D. Karunamoorthy, et al., Internet of blockchains: techniques and challenges ahead, in: Proceedings of 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), IEEE, 2018, pp. 1574–1581, https://doi.org/10.1109/cybermatics_2018.2018.00264.

[47] M. Herlihy, Atomic cross-chain swaps, in: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, ACM, 2018, pp. 245–254, https://doi.org/10.1145/3212734.3212736.

[48] N. Asokan, Fairness in electronic commerce, Ph.D Thesis, University of Waterloo, Waterloo, Ontario, Canada, 1998.

[49] NIFO, The European interoperability framework in detail, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail. (Accessed 5 August 2024).

[50] E. Morris, L. Levine, C. Meyers, et al., System of systems interoperability (sosi), Tech. Rep., Carnegie-Mellon Univ Pittsburgh PA Software Engineering INST, 2004.

[51] A. Tolk, J.A. Muguira, The levels of conceptual interoperability model, in: Proceedings of the 2003 Fall Simulation Interoperability Workshop, Citeseer, 2003, pp. 1–11.

[52] R. Belchior, L. Riley, T. Hardjono, et al., Do you need a distributed ledger technology interoperability solution?, Distrib. Ledger Technol.: Res. Pract. 2 (1) (2023) 1–37, https://doi.org/10.1145/3564532.

[53] G. Falazi, U. Breitenbücher, F. Leymann, et al., Cross-chain smart contract invocations: a systematic multi-vocal literature review, ACM Comput. Surv. 56 (6) (2024) 1–38, https://doi.org/10.1145/3638045.

[54] H. Wang, J. Wang, L. Liu, et al., Temporary relay: a more flexible way to cross chains, Peer-to-Peer Netw. Appl. 17 (5) (2024) 3489–3504, https://doi.org/10.1007/s12083-024-01762-3.

[55] Z. Chen, Y. Zhuo, Z.-B. Duan, et al., Inter-blockchain communication, DEStech Trans. Comput. Sci. Eng. (2017) 448–454, https://doi.org/10.12783/dtcse/cst2017/12539.

[56] P. Cuesta Arcos, Analysis of bridge-solutions for public blockchains, Master's thesis, Universitat Politècnica de Catalunya, 2023.

[57] A. Oram, Peer-to-Peer: Harnessing the Power of Disruptive Technologies, "O'Reilly Media, Inc.", 2001.

[58] J. Pouwelse, P. Garbacki, D. Epema, et al., The bittorrent p2p file-sharing system: measurements and analysis, in: M. Castro, R. Renesse (Eds.), Peer-to-Peer Systems IV, Springer, Berlin, 2005, pp. 205–216, https://doi.org/10.1007/11558989_19.

[59] R. Kumar, K.W. Ross, Optimal peer-assisted file distribution: single and multi-class problems, in: Proceedings of IEEE Workshop on Hot Topics in Web Systems and Technologies (HOTWEB'06), IEEE, 2006, pp. 1–14.

[60] R.C. Merkle, A digital signature based on a conventional encryption function, in: C. Pomerance (Ed.), Advances in Cryptology CRYPTO 87, Springer, Berlin, 1988, pp. 369–378, https://doi.org/10.1007/3-540-48184-2_32.

[61] L. Lamport, The part-time Parliament, ACM Trans. Comput. Syst. 16 (2) (1998) 133–169, https://doi.org/10.1145/279227.279229.

[62] L. Lamport, Paxos made simple, ACM SIGACT News (Distributed Computing Column) 32 (4) (2001) 51–58.

[63] L. Lamport, Fast paxos, Distrib. Comput. 19 (2) (2006) 79–103, https://doi.org/10.1007/s00446-006-0005-x.

[64] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: Proceedings of 2014 USENIX Annual Technical Conference (Usenix ATC 14), ACM, 2014, pp. 305–319.

[65] N. Szabo, Smart contracts: building blocks for digital markets, EXTROPY: J. Transhumanist Thought 18 (2) (1996) 28.

[66] G. Wood, Ethereum: a secure decentralised generalised transaction ledger, https://ethereum.github.io/yellowpaper/paper.pdf, 2014. (Accessed 7 October 2024).

[67] E. Androulaki, A. Barger, V. Bortnikov, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, ACM, 2018, pp. 1–15, https://doi.org/10.1145/3190508.3190538.

[68] T. Hardjono, A. Lipton, A. Pentland, Toward an interoperability architecture for blockchain autonomous systems, IEEE Trans. Eng. Manag. 67 (4) (2019) 1298–1309, https://doi.org/10.1109/tem.2019.2920154.

[69] H. Wang, Y. Cen, X. Li, Blockchain router: a cross-chain communication protocol, in: Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, ACM, 2017, pp. 94–97, https://doi.org/10.1145/3070617.3070634.

[70] A.R. Hevner, S.T. March, J. Park, et al., Design science in information systems research, Manag. Inf. Syst. Q. 28 (1) (2008) 75–105, https://doi.org/10.2307/25148625.

[71] K. Peffers, T. Tuunanen, M.A. Rothenberger, et al., A design science research methodology for information systems research, J. Manag. Inf. Syst. 24 (3) (2007) 45–77, https://doi.org/10.2753/mis0742-1222240302.

[72] A. Garoffolo, D. Kaidalov, R. Oliynykov, Trustless cross-chain communication for zendoo sidechains, arXiv, 2022, preprint, arXiv:2209.03907.

[73] S.D. Lerner, J.Á. Cid-Fuentes, J. Len, et al., Rsk: a bitcoin sidechain with stateful smart-contracts, in: Cryptology ePrint Archive, 2022.

[74] Axelar, Axelar network: connecting applications with blockchain ecosystems, https://axelar.network/axelar_whitepaper.pdf, 2021. (Accessed 5 August 2024).

[75] N.E.T. Matthew Spoke, Aion: enabling the decentralized Internet, https://www.allcryptowhitepapers.com/aion-whitepaper, 2017. (Accessed 5 August 2024).

[76] P.S. Min Kim, Icon, https://www.icon.foundation/projects, 2017. (Accessed 8 May 2024).

[77] S. Thomas, E. Schwartz, A protocol for interledger payments, https://interledger.org/interledger.pdf, 2015. (Accessed 5 August 2024).

[78] E.B. Jae Kwon, Cosmos: a network of distributed ledgers, https://cosmos.network, 2022. (Accessed 5 August 2024).

[79] G. Wood, Polkadot: vision for a heterogeneous multi-chain framework, White Pap. 21 (2016) 2327–4662.

[80] T. Nolan, Btc relay, https://github.com/ethereum/btcrelay, 2015. (Accessed 5 August 2024).

[81] Polygon, Ethereum's Internet of blockchains, https://docs.polygon.technology, 2021. (Accessed 5 August 2024).

[82] S.D. Lerner, Drivechains, sidechains and hybrid 2-way peg designs, https://docs.rsk.co/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf, 2016. (Accessed 5 August 2024).

[83] P. Sztorc, Drivechain, https://github.com/drivechain-project/docs/blob/master/bip1-hashrate-escrow.md, 2017. (Accessed 5 August 2024).

[84] A. Zamyatin, D. Harz, J. Lind, et al., Xclaim: trustless, interoperable, cryptocurrency-backed assets, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 193–210, https://doi.org/10.1109/sp.2019.00085.

[85] J. Nick, A. Poelstra, G. Sanders, Liquid: a bitcoin sidechain, https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf, 2018. (Accessed 5 August 2024).

[86] EherDelta, Etherdelta, https://etherdelta.com, 2016. (Accessed 5 August 2024).

[87] G. Angeris, H.-T. Kao, R. Chiang, et al., An analysis of uniswap markets, Cryptoeconomic Syst. 1 (1) (2021) 1–25, https://doi.org/10.21428/58320208.c9738e64.

[88] W. Warren, A. Bandeali, 0x: an open protocol for decentralized exchange on the Ethereum blockchain, https://github.com/0xProject/whitepaper, 2017. (Accessed 5 August 2024).

[89] Wiki, Hash time locked contracts, https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts, 2013. (Accessed 5 August 2024).

[90] E. Heilman, S. Lipmann, S. Goldberg, The arwen trading protocols, in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security, Springer, Cham, 2020, pp. 156–173, https://doi.org/10.1007/978-3-030-51280-4_10.

[91] W.F. LTD, Building super financial markets for the new digital economy, https://www.wanchain.org, 2017. (Accessed 5 August 2024).

[92] Coinbase, Cbeth white paper, https://www.coinbase.com/cbeth/whitepaper, 2022. (Accessed 5 August 2024).

[93] kraken, Kraken, https://www.kraken.com, 2013. (Accessed 5 August 2024).

[94] Binance, binance exchange, https://www.exodus.com/assets/docs/binance-coin-whitepaper.pdf, 2017. (Accessed 5 August 2024).

[95] A. Miller, Provable security for cryptocurrencies, Ph.D. thesis, University of Maryland, College Park, Washington, America, 2016.

[96] F. Schär, Decentralized finance: on blockchain- and smart contract-based financial markets, FRB of St. Louis Review 103 (2) (2021) 153–174, https://doi.org/10.20955/r.103.153-74.

[97] T. Nolan, Alt chains and atomic transfers, https://bitcointalk.org, 2013. (Accessed 5 August 2024).

[98] B. Pillai, K. Biswas, Z. Hóu, et al., The burn-to-claim cross-blockchain asset transfer protocol, in: Proceedings of 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS), IEEE, 2020, pp. 119–124, https://doi.org/10.1109/iceccs51672.2020.00021.

[99] B. Pillai, K. Biswas, Z. Hóu, et al., Burn-to-claim: an asset transfer protocol for blockchain interoperability, Comput. Netw. 200 (2021) 108495, https://doi.org/10.1016/j.comnet.2021.108495.

[100] A. Garoffolo, D. Kaidalov, R. Oliynykov, Zendoo: a zk-snark verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains, in: Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2020, pp. 1257–1262, https://doi.org/10.1109/icdcs47774.2020.00161.

[101] A. Gluchowski, Zk rollup: scaling with zero-knowledge proofs, https://blog.matter-labs.io, 2019. (Accessed 5 August 2024).

[102] Way Network, Way network, https://way-networks-organization.gitbook.io/way-network, 2023. (Accessed 5 August 2024).

[103] Polygon, The value layer of the Internet, https://polygon.technology, 2021. (Accessed 5 August 2024).

[104] Z. Liu, Y. Xiang, J. Shi, et al., Hyperservice: interoperability and programmability across heterogeneous blockchains, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2019, pp. 549–566, https://doi.org/10.1145/3319535.3355503.

[105] G. Verdian, P. Tasca, C. Paterson, et al., Quant overledger whitepaper, https://uploads-ssl.webflow.com/6006946fee85fda61f666256/60211c93f1cc59419c779c42_Quant_Overledger_Whitepaper_Sep_2019.pdf, 2018. (Accessed 5 May 2024).

[106] E.J. Scheid, T. Hegnauer, B. Rodrigues, et al., Bifröst: a modular blockchain interoperability api, in: Proceedings of 2019 IEEE 44th Conference on Local Computer Networks (LCN), IEEE, 2019, pp. 332–339, https://doi.org/10.1109/lcn44214.2019.8990860.

[107] R. Sheehan, Understanding axelar: a comprehensive overview, https://messari.io/report/understanding-axelar-a-comprehensive-overview, 2023. (Accessed 5 August 2024).

[108] K. Karantias, A. Kiayias, D. Zindros, Proof-of-burn, in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security, Springer, Cham, 2020, pp. 523–540, https://doi.org/10.1007/978-3-030-51280-4_28.

[109] P. Sztorc, Drivechain-the simple two way peg, https://www.truthcoin.info/blog/drivechain, 2015. (Accessed 5 May 2024).

[110] A. Kiayias, D. Zindros, Proof-of-work sidechains, in: A. Bracciali, J. Clark, F. Pintore, et al. (Eds.), Financial Cryptography and Data Security, Springer, Cham, 2020, pp. 21–34, https://doi.org/10.1007/978-3-030-43725-1_3.

[111] S. Ceri, M. Negri, G. Pelagatti, Horizontal data partitioning in database design, in: Proceedings of the 1982 ACM SIGMOD International Conference on Management of Data, ACM, 1982, pp. 128–136, https://doi.org/10.1145/582353.582376.

[112] I. Mat, B. Aldrick, Sparkdefi white paper, https://github.com/sparkpointio/sparkdefi-whitepaper/blob/main/WHITEPAPER.md, 2022. (Accessed 5 August 2024).

[113] T. Chesney, I. Coyne, B. Logan, et al., Griefing in virtual worlds: causes, casualties and coping strategies, Inf. Syst. J. 19 (6) (2009) 525–548, https://doi.org/10.1111/j.1365-2575.2009.00330.x.

[114] E. Tairi, P. Moreno-Sanchez, M. Maffei, A2l: anonymous atomic locks for scalability and interoperability in payment channel hubs, in: Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), IEEE, 2021, pp. 1834–1851, https://doi.org/10.1109/SP40001.2021.00111.

[115] A. Kiayias, N. Lamprou, A.-P. Stouka, Proofs of proofs of work with sublinear complexity, in: J. Clark, S. Meiklejohn, P. Ryan, et al. (Eds.), Financial Cryptography and Data Security: FC 2016 International Workshops, Springer, Berlin, 2016, pp. 61–78, https://doi.org/10.1007/978-3-662-53357-4_5.

[116] A. Kiayias, A. Miller, D. Zindros, Non-interactive proofs of proof-of-work, in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security: 24th International Conference, Springer, Cham, 2020, pp. 505–522, https://doi.org/10.1007/978-3-030-51280-4_27.

[117] A. Back, M. Corallo, L. Dashjr, et al., Enabling blockchain innovations with pegged sidechains, https://www.blockstream.com/sidechains.pdf, 2022. (Accessed 5 August 2024).

[118] C. Dwork, Differential privacy, in: M. Bugliesi, B. Preneel, V. Sassone, et al. (Eds.), Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Springer, Berlin, 2006, pp. 1–12, https://doi.org/10.1007/11787006_1.

[119] J. Bonneau, A. Narayanan, A. Miller, et al., Mixcoin: anonymity for bitcoin with accountable mixes, in: N. Christin, R. Safavi-Naini (Eds.), Financial Cryptography and Data Security: 18th International Conference, FC 2014, Springer, Berlin, 2014, pp. 486–504, https://doi.org/10.1007/978-3-662-45472-5_31.

[120] G. Maxwell, Coinswap: Transaction graph disjoint trustless trading, https://bitcointalk.org/index.php?topic=321228.0, 2013. (Accessed 5 August 2024).

[121] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments, https://lightning.network/lightning-network-paper.pdf, 2016. (Accessed 5 August 2024).

[122] M.G. Reed, P.F. Syverson, D.M. Goldschlag, Anonymous connections and onion routing, IEEE J. Sel. Areas Commun. 16 (4) (1998) 482–494, https://doi.org/10.1109/49.668972.

[123] J.R. Douceur, The sybil attack, in: P. Druschel, F. Kaashoek, A. Rowstron (Eds.), Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002, Springer, Berlin, 2022, pp. 251–260, https://doi.org/10.1007/3-540-45748-8_24.

[124] I. Bentov, Y. Ji, F. Zhang, et al., Tesseract: real-time cryptocurrency exchange using trusted hardware, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2019, pp. 1521–1538, https://doi.org/10.1145/3319535.3363221.

[125] S. Eskandari, S. Moosavi, J. Clark, Sok: transparent dishonesty: front-running attacks on blockchain, in: A. Bracciali, J. Clark, F. Pintore, et al. (Eds.), Financial Cryptography and Data Security, Springer, Cham, 2020, pp. 170–189, https://doi.org/10.1007/978-3-030-43725-1_13.

[126] P. Daian, S. Goldfeder, T. Kell, et al., Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, 2020, pp. 910–927, https://doi.org/10.1109/sp40000.2020.00040.