

Enhancing Blockchain Cross-Chain Interoperability: A Comprehensive Survey

Zhihong Deng[†], Chunming Tang^{†*}, Taotao Li[‡], Parhat Abla[§], Qi Chen[¶], Wei Liang^{||}, Debiao He^b

Abstract—Blockchain technology, introduced in 2008, has revolutionized data storage and transfer across sectors such as finance, healthcare, intelligent transportation, and the metaverse. However, the proliferation of blockchain systems has led to discrepancies in architectures, consensus mechanisms, and data standards, creating “data and value silos” that hinder the development of an integrated multi-chain ecosystem. Blockchain interoperability (a.k.a cross-chain interoperability) has thus emerged as a solution to enable seamless data and asset exchange across disparate blockchains. In this survey, we systematically analyze over 150 high-impact sources from academic journals, digital libraries, and grey literature to provide an in-depth examination of blockchain interoperability. By exploring the existing methods, technologies, and architectures, we offer a classification of interoperability approaches including Atomic Swaps, Sidechains, Light Clients, and so on, which represent the most comprehensive overview to date. Furthermore, we investigate the convergence of academic research with industry practices, underscoring the importance of collaborative efforts in advancing blockchain innovation. Finally, we identify key strategic insights, challenges, and future research trajectories in this field. Our findings aim to support researchers, policymakers, and industry leaders in understanding and harnessing the transformative potential of blockchain interoperability to address current challenges and drive forward a cohesive multi-chain ecosystem.

Index Terms—Survey, Blockchain, Interoperability, Cross-Chain, Internet Technologies

I. INTRODUCTION

Since its inception in 2008 [1], blockchain technology has rapidly evolved, finding applications across diverse fields such as finance [2], intelligent transportation [3], healthcare [4], Artificial Intelligence (AI) [5], and the metaverse [6]. This decentralized, transparent, and efficient distributed ledger technology has revolutionized modern data storage and transmission. However, as more blockchain systems emerge [7]–[11], significant disparities in underlying architectures, consensus mechanisms, smart contracts, and data formats have resulted in the formation of “data and value silos”

[†] School of Mathematics and Information Science, Guangzhou University, Guangzhou, China.

[‡] School of Software Engineering, Sun Yat-Sen University, Zhuhai, China.

[§] School of Software, South China Normal University, Foshan, China.

[¶] Institute of Artificial Intelligence, Guangzhou University, Guangzhou, China.

^{||} School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, China.

^b School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

* Corresponding author: ctang@gzhu.edu.cn.

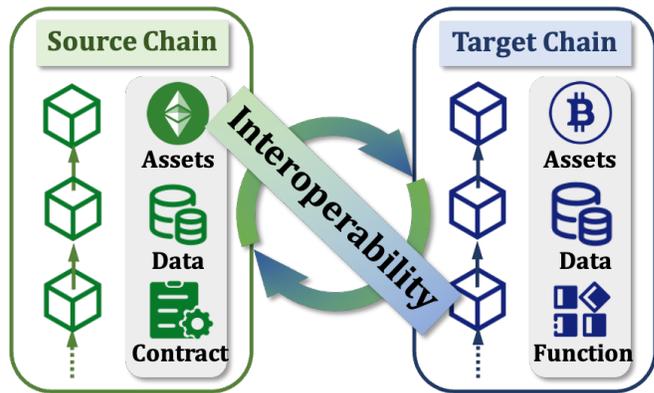


Fig. 1. Blockchain interoperability.

between systems. This fragmentation severely constrains the application potential of blockchain and impedes the development of a cohesive multi-chain ecosystem.

To address this issue, the concept of blockchain interoperability (or cross-chain interoperability, *CCI*) has emerged, aimed at facilitating seamless data and asset transfers between disparate blockchain systems. Some scholars argue that interoperability is a crucial factor in unlocking the full potential of blockchain technology [12]. As the scope of applications expands, the value and commitments of interoperability become increasingly apparent across various scenarios, including enhancing asset liquidity, reducing transaction costs, improving user experience, and breaking network silos, as outlined in Tab. I. However, achieving interoperability between blockchains introduces considerable complexity—not only does it require synchronizing multiple software components, but it also necessitates integrating diverse distributed systems while addressing unique challenges in security, liveness, data consistency, atomicity, and decentralization. This cross-chain collaboration primarily relies on interoperability mechanisms. Nevertheless, the implementation of interoperability faces numerous obstacles due to the diversity of blockchain systems in network structures, cryptographic primitives, and application contexts. Despite these challenges, academic contributions have yielded a variety of protocols [13]–[15], novel architectures [16]–[18], and practical applications [2]–[4], underscoring the importance of *CCI*.

A. Motivation

The significance of researching blockchain interoperability technologies cannot be overstated. Consider

TABLE I
A VISION OF INTEROPERABILITY COMMITMENTS.

Benefit	Description	Example Application
Enhancing Asset Liquidity	Liquidity fragmentation across blockchains hampers overall market efficiency. Cross-chain platforms address this issue by enabling seamless asset transfers between different chains, fostering a more unified and liquid cryptocurrency market. Enhanced liquidity allows users to select the most optimal platforms for trading and lending, thereby maximizing their investment returns.	Uniswap v3's recent integration of Layer 2 solutions [19], [20], such as Optimism and Arbitrum, has enabled users to transfer assets from the Ethereum mainnet to these Layer-2 networks via cross-chain bridge. This allows them to benefit from lower transaction fees and faster transaction speeds. Such liquidity migration empowers users to move funds swiftly and efficiently across different chains, thereby optimizing their investment strategies.
Reducing Transaction Costs	<i>CC1</i> enables the transfer of assets from blockchains with high transaction fees to those with lower fees, thereby reducing transaction costs for users. For digital finance users, this results in lower transaction friction and greater capital efficiency.	SushiSwap and Uniswap [21] offer interoperability solutions that allow users to trade and provide liquidity across multiple blockchains. Users can choose to conduct transactions on chains with lower fees, reducing transaction costs and enhancing the efficiency of capital utilization.
Improving User Experience	The frequent need to operate across diverse blockchain networks necessitates the management of multiple wallets and the navigation of intricate user interfaces. By integrating <i>CC1</i> , these challenges are significantly mitigated, providing users with a seamless and enhanced operational experience.	Protocols such as Axelar Network [22] facilitate cross-chain messaging, empowering developers to design applications capable of interacting with assets and data across disparate blockchain networks, thereby obviating the need for users to handle intricate infrastructure management.
Breaking Network Silos	In traditional blockchain systems, information is often isolated within individual chains, preventing direct communication between them. <i>CC1</i> technology breaks down these barriers, enabling the free exchange and sharing of information across different chains, leading to more efficient data collaboration.	The Cosmos network [23], through its IBC protocol, allows different blockchains to transmit information without the need for third parties. For instance, the source chain can send its state or data to target chain via IBC [24], enabling target chain to trigger its own smart contracts based on this information, thereby facilitating cross-chain data interaction.



Fig. 2. The most popular interoperability routes.

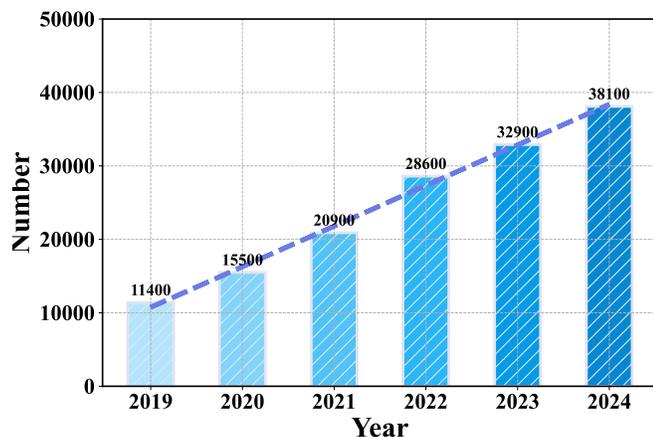


Fig. 3. The number of interoperability studies on Google Scholar over the past six years.

the following data: ① By the end of 2024, the total market capitalization of digital currencies is expected to reach \$2.32 trillion, encompassing over 9,982 digital currencies and at least 8,000 blockchains, with no fewer than 759 exchanges involved [25]. Fig. 2 illustrates the most prevalent digital currency interoperability routes. ② A Google Scholar search for the term “Blockchain

& Interoperability | Cross Chain” reveals over 219,000 relevant studies. As shown in Fig. 3, the number of research publications has steadily increased from 2019 to November 2024, with projections indicating a new peak in 2025. ③ Experts forecast that the global blockchain interoperability market will expand from \$375.46 million in 2024 to \$8.48 billion by the end of 2037, witnessing around anticipated annual growth rate of 27.1% [26]. This growth is primarily driven by the urgent demand for asset conversion, widespread adoption of decentralized applications (dApps) across industries, and ongoing improvements in regulation and standardization.

However, current solutions in the field are diverse and relatively fragmented, lacking systematic and comprehensive integration. This paper aims to conduct a fine-grained analysis of the existing literature, revealing current research characteristics and limitations while exploring future development potential. Additionally, we seek to foster interdisciplinary dialogue and collaboration, assisting researchers across various domains in recognizing the critical importance of blockchain interoperability in their work, thereby promoting more comprehensive and systematic research endeavors.

B. Research Paradigm

This survey employs a systematic literature review methodology to conduct an in-depth analysis of research on blockchain interoperability. The literature collection is centered on Google Scholar, which aggregates content from prominent digital libraries and conference proceedings (e.g., IEEE Xplore, ACM Digital Library, Springer Nature Lecture Notes), alongside gray literature sources (e.g., arXiv, Cryptology ePrint Archive) and other auxiliary resources (e.g., books and repositories like GitHub). By utilizing the keyword

Blockchain&(Interoperability|Cross-Chain)

in our search (as illustrated in Fig. 4), we restricted the time frame to publications from 2016 to 2024, prioritizing highly cited works relevant to the topic. Following an initial screening and quality assessment, over 150 pertinent studies were selected for in-depth analysis. We also acknowledge the limitations of our research methodology, including potential publication bias and the risk of omitting significant studies.

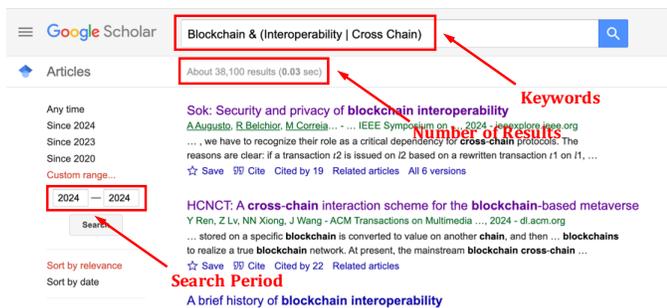


Fig. 4. Search Procedure in Google Scholar.

C. Related Works and Contributions

In recent years, numerous reviews addressing interoperability and cross-chain technologies have emerged. Augusto et al. [12] conducted the most comprehensive investigation to date on the security and privacy of blockchain systems. Belchior et al. [27] classified interoperability into Public Connectors, Blockchain of Blockchains, and Hybrid Connectors. Wang et al. [28] categorized it into chain-based, bridge-based, and dApp-based interoperability. Ren et al. [29] proposed a performance evaluation mechanism for interoperability approaches. Zamyatin et al. [30] systematically articulated cross-chain communication (CCC) protocol for the first time, formalizing the argument that the implementation of CCC is unachievable without a trusted third party. Additional relevant reviews include [31]–[36].

We summarize these surveys in Tab. II, evaluating each study from methodological, technical, and discussion perspectives. Furthermore, this paper expands upon the aforementioned research by providing a more comprehensive and systematic examination of the field,

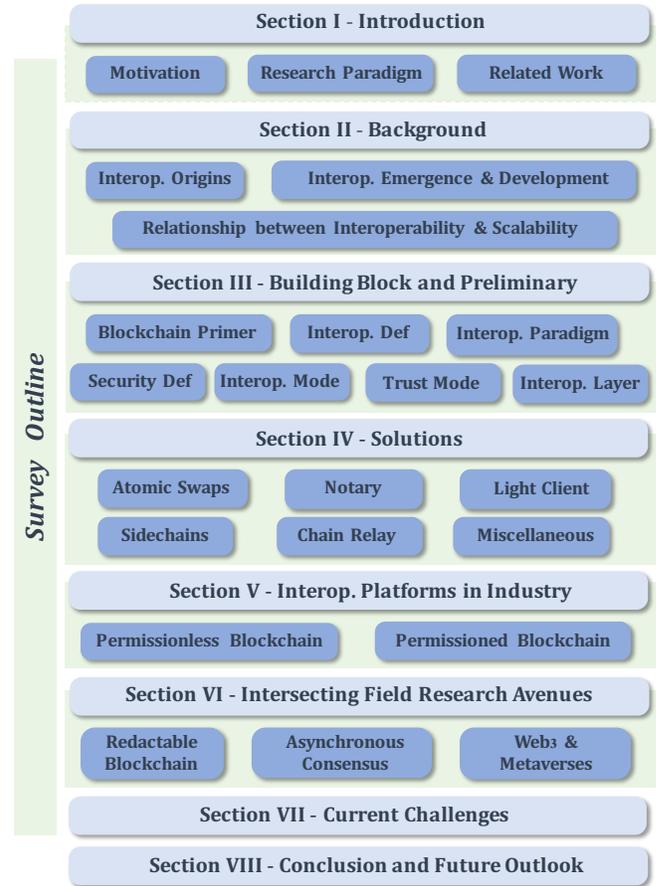


Fig. 5. Survey Outline.

with a particular focus on technology types, comparative analyses, and interdisciplinary research.

This survey provides the following **contributions**, which are outlined below:

- *Systematic Knowledge Construction.* This survey integrates and organizes existing literature, offering a comprehensive description that encompasses building blocks, methodologies, and architectural frameworks. We compare the characteristics and relationships of various technologies for scalability with interoperability and categorize interoperability techniques into native, local, and external validation mechanisms. Furthermore, we provide an in-depth analysis of no fewer than ten technology categories (including HTLC, Adaptor Signatures, Notary, Light Client, Sidechains, Chain Relay, and so on), representing the most extensive classification to date. This systematic construction of knowledge not only mitigates fragmentation within the field but also establishes a solid foundation for future research.
- *Academic and Industrial Collaboration.* This survey emphasizes the close relationship between academic research and industrial practice. By analyzing multiple classic interoperability platforms, we encourage collaborative efforts between academia and industry to advance the practical application and innovation of blockchain technology.

TABLE II
COMPARISON OF EXISTING SURVEYS AND OUR WORK.

Reference	Methodology				Technique Analysis					Discussion		
	SC	SD	GP	AM	TC	TT	CB	IC	IS	IF	IO	FC
Koens et al. (2019) [31]	○	○	○	▶	▶	▶	▶	▶	○	○	▶	○
Bhatia et al. (2020) [32]	○	○	○	▶	▶	▶	▶	▶	○	○	○	○
Belchior et al. (2021) [27]	●	▶	▶	●	▶	▶	●	▶	▶	○	●	●
Zamyatin et al. (2021) [30]	▶	●	●	●	▶	▶	▶	▶	○	○	●	●
Ou et al. (2022) [33]	○	○	○	▶	▶	▶	●	●	○	○	●	●
Ren et al. (2023) [29]	▶	▶	○	●	▶	▶	▶	●	○	○	▶	●
Kotey et al. (2023) [34]	●	○	○	▶	▶	▶	▶	●	○	▶	▶	○
Zhou et al. (2023) [35]	○	○	○	▶	▶	▶	▶	▶	○	○	○	▶
Wang et al. (2023) [28]	●	▶	●	●	▶	▶	▶	▶	○	○	●	●
Li et al. (2024) [36]	○	○	○	▶	▶	▶	▶	●	▶	○	●	●
Our Survey	●	●	●	●	●	●	●	●	●	●	●	●

★ Symbol. “covered” (● with blue background); “partially covered” (▶ with green background); “not covered” (○ with gray background).

★ Abbreviation. SC: Survey Comparison; SD: Security Definition; GP: Generic Paradigm; AM: Abstraction with Modeling; TC: Technology Coverage; TT: Technology Types; CB: Comparison between technologies; IC: Industry Case Analysis; IS: Interoperability vs. Scalability Comparison; IF: Intersecting Field Research Avenues; IO: Open Issues; FC: Future Challenges.

- *Strategic Insights.* This survey offers profound insights into the future development of blockchain interoperability, identifying key research directions and potential technological trends. We pay particular attention to areas such as editable blockchains, asynchronous consensus, and the metaverse, as well as challenges related to regulation and knowledge frameworks. These strategic insights aim to guide decision-makers, researchers, and industry leaders in making informed choices within the rapidly evolving technological landscape.

The organizational framework of this survey is depicted in Fig. 5.

II. BACKGROUND

A. Origins of Interoperability

Interoperability originated as early as the 1980s in the field of computer science [37], [38], primarily to address compatibility issues between systems, enabling different systems and applications to collaborate despite differences in hardware, operating systems, and programming languages. For example, classic standards like the TCP/IP protocol [39] and the OSI model [40] became the foundation for cross-system network communication. By the early 21st century, the widespread adoption of web services and cloud computing further advanced interoperability technologies. Web services provided standardized interfaces based on HTTP and XML [41], allowing applications to easily integrate over the network, while cloud computing, through virtualization and service-oriented technologies, enabled unified management and interaction between different applications in the internet environment [42]. The rise of Web 2.0 [43] further promoted API-based communication between systems, allowing different applications to interact and

share data in an open environment, laying the theoretical groundwork for future explorations in blockchain interoperability [44] and Web 3.0 [45]. Unsurprisingly, the principles established in the architecture of the Internet have guided the development of interoperability protocols and standards [46], with direct application to the blockchain domain. Given the trajectory of the Internet and computer networks throughout their historical development, the shift toward *CCI* is unsurprising. As a result, a global landscape of multi-chain blockchain networks [47], [48] connected by cross-chain solutions has gradually emerged [28], [29].

B. Emergence & Development of Interoperability

The exploration of interoperability technologies has been ongoing since the inception of Bitcoin [1]. The development of *CCI* can be divided into two distinct phases: Solo-Chain Stage and Multi-Chain Stage. Fig. 6 illustrates key events from the early stages of development to the present.

1) *Solo-Chain Stage (2012–2015):* As early as 2012, Ripple Labs proposed the InterLedger Protocol (ILP) [49], [50], which was formally implemented on the Ripple blockchain in 2015 [51]. The protocol introduced a third-party entity, termed Connector, to manage custody and transaction verification between cross-chain participants.

In 2013, Holan et al. [52] proposed the concept of atomic transfers based on the Bitcoin network and Alt chains. This approach utilized hash-locking technology, where a script was triggered upon the revelation of a hash pre-image, enabling atomic cross-chain operations across Bitcoin and other blockchain networks.

In 2014, BlockStream introduced the concept of pegged sidechains [53], utilizing a two-way peg mechanism to transfer crypto assets between the sidechain

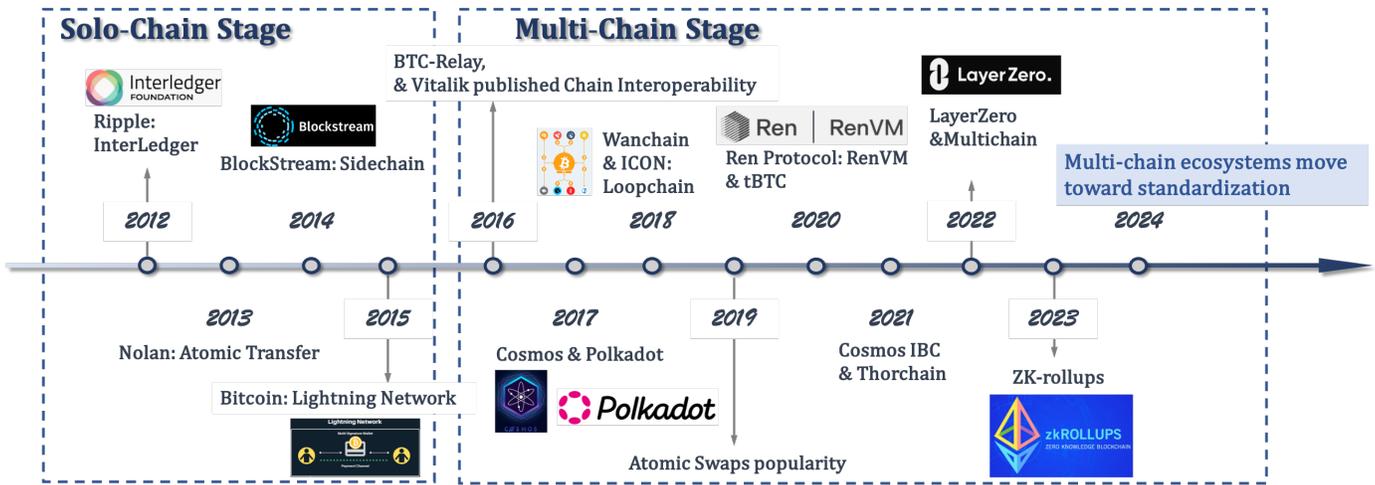


Fig. 6. Timeline: the development of interoperability.

and the main chain. This innovation enabled developers to create new blockchain systems on Bitcoin while maintaining interoperability with the Bitcoin network (By 2016, BlockStream further developed federated sidechains by introducing multi-signature technology, which reduced latency and enhanced interoperability between the sidechain and the main chain).

In 2015, Poon et al. introduced the concept of off-chain transaction technology in their Lightning Network whitepaper [13], which facilitated the transfer of value off-chain via micropayment channels [54]. This innovation significantly improved transaction efficiency within the Bitcoin ecosystem by providing a mechanism for intra-chain atomic cross-chain operations.

2) **Multi-Chain Stage (2016–Present):** In 2016, ConsenSys, an Ethereum blockchain software company, developed BTC Relay [55], allowing users to interact directly with the Bitcoin network via Ethereum, thus enabling cross-chain operations between ETH and BTC. BTC Relay’s implementation leveraged BTC block header information and Ethereum smart contract functionality to securely verify Bitcoin transactions without the need for third-party intermediaries. In the same year, Vitalik Buterin [56] provided an in-depth analysis of blockchain interoperability challenges.

In 2017, the Cosmos project published its whitepaper [23], outlining a vision for *CCI* using a Hub-and-Zone architecture. Shortly after, Tendermint [9] secured its first round of funding and began developing the Cosmos network. That same year, Polkadot introduced its whitepaper [57], presenting its parachain and relay chain architecture, along with key concepts such as shared security and Cross-Chain Message Passing (XCMP).

In 2018, Wanchain launched its mainnet, aiming to create a distributed “bank” that facilitates cross-chain asset and data transfers. By leveraging cross-chain smart contracts and privacy-preserving technologies, Wanchain achieved interoperability for various assets. ICON, also in 2018, released its Loopchain protocol [58],

which connected independent blockchains across multiple industries, enhancing cross-industry interoperability, particularly in finance, healthcare, and government applications.

Atomic swap technology [59] gained significant traction in 2019, becoming widely adopted within the cryptocurrency community. This advancement allowed direct, trustless exchanges of cryptocurrencies across different blockchains, fostering the growth of decentralized exchanges (DEXs) and cross-chain trading.

In 2020, Ren Protocol launched RenVM [60], a decentralized virtual machine enabling cross-chain transfers of crypto assets through distributed key management. RenVM facilitated the transfer of non-Ethereum assets, such as Bitcoin, to the Ethereum network, unlocking new opportunities for *decentralized finance* (DeFi) applications. Additionally, the tBTC project went live, allowing Bitcoin holders to mint ERC-20 tokens [61] on Ethereum without relying on trusted intermediaries, marking a significant step in cross-chain asset management.

THORchain’s mainnet launched in 2021, introducing a decentralized liquidity network that enabled native cross-chain asset swaps (e.g., BTC, ETH) without the need for wrapped tokens or intermediary chains. Meanwhile, Cosmos launched its Inter-Blockchain Communication (IBC) protocol [62], enabling seamless asset and data interoperability between blockchains and marking the maturation of the Cosmos ecosystem.

LayerZero Labs launched the LayerZero cross-chain communication protocol [63] in 2022, enabling smart contracts to transmit messages across different blockchains, while providing off-chain proof for cross-chain communication. LayerZero’s Omnichain protocol opened up new possibilities for cross-chain DeFi and NFT development. The same year, Anyswap rebranded as Multichain [64], expanding its cross-chain bridge capabilities to support a broader range of blockchain networks. Through its multi-chain architecture, Multichain became a critical infrastructure within the cross-chain

DeFi ecosystem.

In 2023, with advancements in ZK-Rollup technology [65], an increasing number of cross-chain bridges began adopting ZK-Rollups to enhance the security and efficiency of Layer-2 cross-chain transactions, driving further progress in blockchain interoperability and scalability.

By 2024, the growing demand for cross-chain interoperability led to the standardization of cross-chain communication protocols. Protocols such as Polkadot's XCMP and Cosmos' IBC gained widespread adoption, promoting the further integration of multi-chain ecosystems.

C. Relationship between Interoperability with Scalability

Blockchain trilemma, also known as "Scalability Trilemma" [66]–[68], is a concept that highlights the challenge of achieving a perfect balance among three critical characteristics: security, scalability, and decentralization. According to this trilemma, a blockchain can optimize only two of these properties simultaneously, often at the expense of the third. This is similar to the CAP theory [69] of traditional distributed systems. In practical terms, blockchain systems tend to focus on optimizing one or two of these aspects while making trade-offs with the third. For instance, Bitcoin [1] prioritizes decentralization and security but has limitations in scalability, leading to slower transaction times and higher fees. Some permissioned blockchains [70] may prioritize security and scalability but at the cost of decentralization, relying on fewer, trusted nodes to process transactions; Layer-2 solutions [68], [71] or alternative consensus mechanisms [72] aim to improve scalability while attempting to maintain security and decentralization, though achieving all three at high levels remains a significant challenge. Therefore, balancing and even achieving these three characteristics is particularly important for the future development of the blockchain to adapt to more complex and large-scale scenarios.

Exploring interoperability, as a pathway for computational offloading, is an effective approach that not only mitigates compromises in decentralization but also achieves a more balanced trade-off within the "blockchain trilemma". Consequently, we propose that: "Interoperability is an essential prerequisite for enabling service scalability".

CCI facilitates the seamless flow of assets across ecosystems, alleviating lock-in effects and promoting greater economic equity among users. Additionally, interoperability eliminates data and value silos, enhancing the collaborative synergy within blockchain communities while reducing data redundancy costs. For example, a token holder on one blockchain may participate in decentralized autonomous organization (DAO) voting on another [73]. Interoperability further allows applications to deploy across multiple chains, enabling data sharing and asset transfer beyond the constraints of any

single chain, thereby extending user reach and market potential. It also enhances system adaptability, allowing applications to align with evolving blockchain platforms and protocols to meet diverse user demands and support ecosystem-wide scalability. Moreover, interoperability can improve the security of specific blockchains by anchoring less secure chains to more secure ones through mechanisms like sidechains [74] or timestamping [75], thereby enabling the regular creation of security checkpoints.

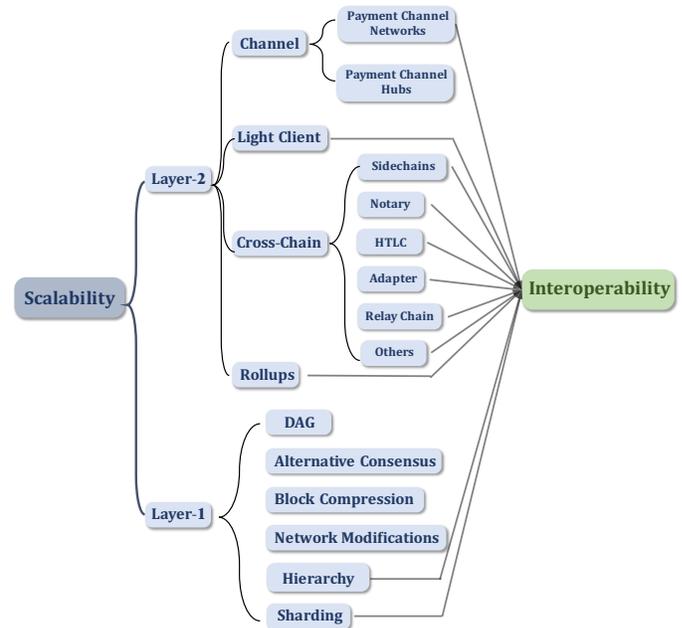


Fig. 7. The technical correlation between interoperability and scalability.

As illustrated in Fig. 7, our analysis of scalability technologies across Layer-1 and Layer-2 [68], [71] reveals that the technological foundations of interoperability are thoroughly embedded within scalability frameworks. A primary benefit of Layer-1 solutions is their foundational and holistic approach to improving blockchain performance. By addressing the root causes of performance issues through techniques such as sharding and hierarchy, Layer-1 solutions can lead to more sustainable improvements in interoperability and scalability. Conversely, Layer-2 solutions enhance blockchain functionality by adding supplementary layers or protocols atop existing blockchains, leaving the core blockchain protocols unchanged. This makes Layer-2 solutions generally easier to implement and adopt, offering greater flexibility in terms of interoperability and broader applicability.

On the whole, we contend that interoperability is indispensable for achieving scalability. This perspective is supported by a decade of extensive academic research [27]–[29], [68] and industry backing [76], [77], with many stakeholders viewing interoperability as a crucial enabler for large-scale adoption [78].

III. BUILDING BLOCK AND PRELIMINARY

In this section, we present the essential knowledge required to understand this survey. We begin by defining blockchain and interoperability. Following that, we present the definitions of security and the modes related to blockchain interoperability. Tab. III describes the symbols commonly used in this paper.

TABLE III
SYMBOL DESCRIPTION

Symbol	Description
\mathcal{S}	Source Chain
\mathcal{T}	Target Chain
$\mathcal{L}_{\mathcal{S}}$	the Ledger of \mathcal{S}
$\mathcal{L}_{\mathcal{T}}$	the Ledger of \mathcal{T}
Tx_CC	the Cross-Chain Transaction
CCI	Cross-Chain Interoperability
TTP	Trusted Third Party

A. A Primer on Blockchain

Blockchain Basic. Blockchain is a public ledger technology powering cryptocurrencies such as Bitcoin [1] and Ethereum [7]. It operates as a decentralized data structure, enabling dApps [79], smart contracts [80], and the recording of all network transactions. In this system, each node independently maintains a ledger copy, verifies peers, and can initiate, validate, and confirm transactions without a *Trusted Third Party* (TTP). This decentralized framework strengthens security and resilience, minimizing single points of failure and the risk of data tampering.

Definition 1 (Blockchain Structures). A blockchain includes the following data structures:

- **Transaction.** Which is the process of transferring cryptocurrency. It must specify the sender, recipient, transaction amount, and the sender's signature;
- **Block.** Which consists of two components: the header and the body. The former contains a set of transactions, while the latter records the hash of the previous block, version, nonce, the root of the Merkle tree, etc;
- **Chain.** Which is a sequence of blocks, where each block contains the previous block's hash, serving as a pointer to link them together, forming a chain. New blocks are always appended to the chain.

For simplicity, we use "blockchain" and "chain" interchangeably throughout this survey.

Blockchain Types. Blockchain can be categorized into two types based on network architecture and authorization requirements (see Fig. 8). When considering interactions between two chains of the same type, we define this as homogeneous interoperability, whereas interactions between different types of blockchains are referred to as heterogeneous interoperability. Typically, the latter is backwards compatible with the former.

Definition 2 (Permissionless Blockchain). In a permissionless blockchain system:

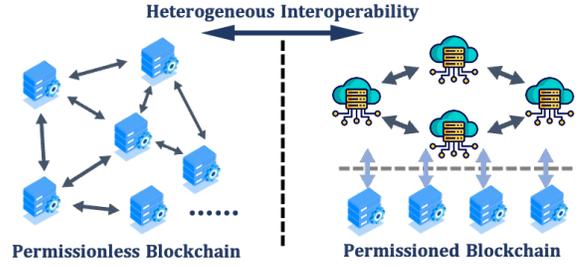


Fig. 8. Network architectures for different types of blockchains.

- No identity authentication is required;
- Any node can join, send transactions, participate in consensus, or leave at any time;
- At any given moment, the number of participating nodes is subject to variation and cannot be reliably predicted.

Definition 3 (Permissioned Blockchain). A permissioned blockchain system is jointly managed and maintained by multiple organizations or institutions, where only authenticated nodes are permitted to join the network, read data, and execute transactions.

Different from permissionless blockchain, to maintain consistency among replicated data on different nodes, the permissioned blockchain should employ a State Machine Replication (SMR) algorithm [81], ensuring nodes agree on the order of incoming transactions to maintain identical copies of the distributed ledger.

Distributed Ledger Model. In the following context, the terms *blockchain* and *distributed ledger* are used interchangeably. Regarding interoperability, we consider the interaction between the source chain \mathcal{S} and the target chain \mathcal{T} , which may involve distinct consensus participants and different consensus protocols. Let \mathcal{L} represent a ledger, with $\mathcal{L}_{\mathcal{S}}$ and $\mathcal{L}_{\mathcal{T}}$ corresponding to the ledgers of \mathcal{S} and \mathcal{T} , respectively. The state of a ledger is defined as a dynamically evolving sequence of transactions, denoted by $\langle \text{Tx}_1, \dots, \text{Tx}_n \rangle$. We assume the ledger state evolves in discrete rounds, indexed by natural numbers $r \in \mathbb{N}$. Thus, $\mathcal{L}^P[r]$ represents the state of ledger \mathcal{L} at round r , which is defined as the state after applying all transactions recorded in \mathcal{L} since round $r-1$, according to the perspective of some party P . Hence, $\text{Tx} \in \mathcal{L}^P[r]$ can be denoted as a transaction Tx has been included in \mathcal{L} as position r .

To maintain cross-chain protocol security, as a premise, either a singular \mathcal{S} or \mathcal{T} must exhibit the following properties [82]:

Definition 4 (Robust Distributed Ledger). We say that a robust distributed ledger must meet the following properties:

- **Persistence.** For any two honest parties P_1 and P_2 , if they adopt respective ledgers $\mathcal{L}^{P_1}[r_1]$ and $\mathcal{L}^{P_2}[r_2]$ at round r_1 and r_2 respectively, where $r_1 \leq r_2$. It holds that $\mathcal{L}^{P_1}[r_1] \preceq \mathcal{L}^{P_2}[r_2]$.
- **Liveness.** After the environment submits a valid Tx , any honest parties P will report $\text{Tx} \in \mathcal{L}^P[r']$ at round r' after t round.

TABLE IV
COMPARATIVE DEFINITIONS OF INTEROPERABILITY IN DIFFERENT LITERATURE

Year	Proposer	Core Definition
1996	Wegner et al. [38]	It refers to the capability of multiple software components to work together, even when there are variations in programming language, interface, and execution environment.
2006	Vernadat et al. [84]	It denotes the capability of two or more systems to either offer services to one another or receive services, while efficiently leveraging a shared exchange for mutual benefit.
2016	Buterin et al. [85]	It involves three main operations: ① transferring assets between platforms; ② implementing payment-versus-payment and payment-versus-delivery models; ③ retrieving information from one blockchain within another.
2019	Pillai et al. [86]	It is designed not to directly alter the state of other blockchains. Instead, its purpose is to initiate specific functionalities on the other system, which are expected to carry out operations within their own network.
2019	Yaga et al. [87]	Its atomic transaction execution extends across multiple blockchains, enabling data recorded on one chain to be accessible, verifiable, and referenced by potentially external transactions in a semantically consistent manner.
2021	Belchior et al. [27]	The capability of \mathcal{S} to modify the state of \mathcal{T} , facilitated by inter- or intra-cross-chain transactions, spanning both homogeneous and heterogeneous blockchain systems.
2023	Wang et al. [28]	It refers to the capability to accurately execute asset transfers across a mix of homogeneous and heterogeneous blockchain systems while preserving the foundational design principles of each system.
2023	Ren et al. [29]	It refers to the flexibility to transfer assets, share data, and execute smart contracts across public, private, and permissioned blockchains without altering their underlying systems.

Persistence guarantees that confirmed the cross-chain transaction Tx_CC is irreversible, and *liveness* ensures the eventual inclusion of all valid Tx_CC . These properties are ensured when the in-chain consensus adheres to the specified requirements [82]: *Common Prefix, Chain Quality, and Chain Growth*.

Transaction Model. When a transaction Tx is included in a ledger \mathcal{L} , it modifies the ledger’s state by specifying a set of operations that must be executed and agreed upon by consensus participants P_1, \dots, P_n . The nature of these operations is system-dependent and can vary from simple transfers to the execution of complex programs [83]. For the sake of generality, we do not distinguish between different transaction models, i.e. *UTXO* [1] and the *account-based* model [83].

B. Blockchain Interoperability Definition

In the early development of computer science, numerous descriptions of interoperability were introduced [38], [84], [88]. Interoperability is defined by the Institute of Electrical and Electronics Engineers (IEEE) as follows: “The ability of two or more systems or components to exchange information and to use the information that has been exchanged” [88]. Vernadat et al. [84] expanded upon this definition from a systems perspective, and these conceptual frameworks have been effectively integrated into the discourse on blockchain interoperability. Although the technologies facilitating blockchain interoperability remain nascent and lack standardization, several representative definitions have emerged [27]–[29], [85]–[87]. As illustrated in Tab. IV, these definitions underscore various dimensions of blockchain interoperability. We assert that blockchain interoperability, also referred to as cross-chain interoperability, which refers to the ability of blockchain networks to facilitate mutual interaction with one another by exchanging assets, data, or both, primarily manifests through *Data Interoperability, Functional Interoperability, and Value Interoperability*. Data interoperability

emphasizes cross-chain data access and transmission among disparate blockchains. Value interoperability pertains to asset exchanges and transfers across different blockchains. Functional interoperability seeks to integrate functionalities between various blockchains, such as enabling cross-chain calls to smart contracts. However, it is essential to recognize that each blockchain system operates as an isolated entity, and interoperability is an ancillary feature of the system. Consequently, when introducing new functionalities to a blockchain, it is imperative not to undermine its foundational role as a decentralized ledger system.

C. A Generic Interoperability Paradigm

Let us define a more generic interoperability paradigm that can signify the transfer of goods, assets, or objects between \mathcal{S} and \mathcal{T} . We assume that an operation $\mathcal{O}_\mathcal{S}$ runs on \mathcal{S} , and an operation $\mathcal{O}_\mathcal{T}$ runs on \mathcal{T} . Operations can influence the blockchain state in two distinctive ways: ① by writing transactions to the blockchain; ② by halting interaction with the blockchain. These assumptions align with the CCC protocol model proposed in [30].

Definition 5 (A Generic Interoperability Paradigm). The generic paradigm is constructed by the following phases:

- **a) Setup.** The primary task during the setup phase is to establish the relevant information for both the parameterized \mathcal{S} and \mathcal{T} , and to define the application-level specifications for interoperability to facilitate the initialization of cross-chain communication. For instance, in the case of digital asset exchanges, this involves specifying the asset types to be exchanged (e.g., Tokens or NFTs), the valuation standards (e.g., based on ERC-20 [89] or ERC-721 [90]), time constraints, and any additional conditions;
- **b) Commit on Source Chain \mathcal{S} .** Upon successful setup, a publicly verifiable commitment to execute a Tx_CC is submitted on \mathcal{S} . Specifically, $\mathcal{O}_\mathcal{S}$ writes the transaction

to \mathcal{L}_S . Based on the persistence and liveness of \mathcal{L}_S (as described in Def. 4), all honest participants in S will determine that the transaction has ultimately reached a stable state;

- **c) Verify.** The commitment made by \mathcal{O}_S on S is verified by \mathcal{O}_T (or \mathcal{O}_T receives the proof from \mathcal{O}_S). Based on the persistence and liveness of \mathcal{L}_S , the verification will succeed once the transaction stabilizes on \mathcal{L}_S ;
- **d.1) Commit on Target Chain \mathcal{T} .** Following successful verification, a commitment that is publicly verifiable to execute a Tx_CC is submitted on \mathcal{T} . \mathcal{O}_T writes the transaction to \mathcal{L}_T . Based on the persistence and liveness of \mathcal{L}_T , all honest participants in \mathcal{T} will ascertain that the transaction has ultimately reached a stable state;
- **d.2) Abort.** If the verification fails, or if \mathcal{O}_T is unable to fulfill the commitment execution on \mathcal{T} , the protocol will execute an abort operation on S to revert the modifications to their original state, ensuring atomicity.

It is noteworthy that some asset exchange interoperability protocols follow a Two-Phase Commit (2PC) [89] design, allowing phase *b*) and *d.1*) to be executed concurrently. Phase *d.2*) is not preemptory, indicating that once *commit* has been executed, *abort* is no longer an option [30].

D. Security Definition of Blockchain Interoperability

First of all, let's describe an example of an interoperability atomicity transmission failure. Let Tx_CC denote a cross-chain transaction, where Tx_CC.In represents the input impacting the ledger state of the transaction originator, and Tx_CC.Out represents the output affecting the ledger state of the transaction recipient. The atomicity failure of Tx_CC can be categorized into two scenarios, as illustrated in Fig. 9. In the first scenario (Fig. 9(a)), due to intentional or unintentional forks on Chain #1, Tx_CC.In fails to be executed, while Tx_CC.Out successfully takes effect on the longest chain of Chain #2. This situation introduces a potential double-spending risk for Tx_CC , necessitating measures to prevent such occurrences. In the second scenario (Fig. 9(b)), although Tx_CC.Out is forked and fails to take effect, this does not pose a double-spending risk. Instead, Tx_CC.Out can be rewritten on the longest chain of Chain #2, thereby mitigating the atomicity failure of Tx_CC in this case. Therefore, the challenge of blockchain interoperability stems from the need for atomic synchronization of transactions across two or multiple chains, e.g., in an atomic swap, a transaction Tx_CC.In on Chain #1 succeeds if and only if Tx_CC.Out was previously posted on Chain #2.

A necessary guarantee for a secure *CCI* protocol is **atomicity**. Referring to [30], [91], we articulate in a weak and a strong variant. For S and T , each with respective underlying ledgers \mathcal{L}_S and \mathcal{L}_T , the goal of *CCI* can be described as the synchronization of processes #In and #Out such that #Out writes Tx_CC.Out to \mathcal{L}_T if and only if #In has written Tx_CC.In to \mathcal{L}_S . From *persistence* and *liveness* of \mathcal{L} (Def. 4), it follows that eventually #In writes

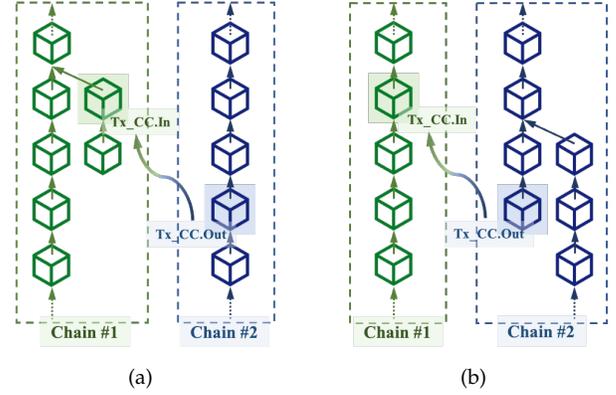


Fig. 9. Cases studies on cross-chain atomicity transfer failure. (a) Tx_CC.In is not on the longest chain of Chain #1; (b) Tx_CC.Out is not on the longest chain of Chain #2.

Tx_CC.In in \mathcal{L}_S and #Out becomes aware of and verifies Tx_CC.Out in \mathcal{L}_T . Hence, a secure *CCI* protocol must exhibit the following properties:

Definition 6 (The Security of *CCI*). For both blockchain S and T with ledgers \mathcal{L}_S and \mathcal{L}_T , each of which satisfies persistence and liveness required for a robust distributed ledger in Def. 4. Consider two processes, #In on S and #Out on T , with to-be-synchronized transactions Tx_CC.In and Tx_CC.Out . A *CCI* protocol is secure if the following properties can be satisfied:

- **Weak Atomicity.** A valid Tx_CC.In is reported stable on \mathcal{L}_T only if Tx_CC.Out has been reported stable on \mathcal{L}_S , i.e.: $\text{Tx_CC.In} \in \mathcal{L}_T \implies \text{Tx_CC.Out} \in \mathcal{L}_S$.
- **Strong Atomicity.** There are no outcomes in which Tx_CC.In is reported stable on \mathcal{L}_T but Tx_CC.Out is not stable on \mathcal{L}_S , or Tx_CC.Out is reported stable on \mathcal{L}_S but Tx_CC.In is not stable on \mathcal{L}_T , i.e.:

$$\neg((\text{Tx_CC.In} \in \mathcal{L}_T \wedge \text{Tx_CC.Out} \notin \mathcal{L}_S) \vee (\text{Tx_CC.Out} \in \mathcal{L}_S \wedge \text{Tx_CC.In} \notin \mathcal{L}_T)).$$

The former ensures that Tx_CC.Out appears on \mathcal{L}_T only if Tx_CC.In has been already written into \mathcal{L}_S . The latter ensures that Tx_CC.Out appears on \mathcal{L}_T if and only if Tx_CC.In has been already written into \mathcal{L}_S .

E. Interoperability Modes

We propose three interoperability modes based on the existing works of literature [12], [28], [92]. The choice of interoperability mode determines the required protocol architecture, with each configuration delivering its own specific security guarantees.

Asset Swap. Asset swap refers to the exchange of different assets between two separate blockchains through an agreed-upon protocol. This typically occurs when users want to exchange one asset for another, such as swapping Bitcoin for tokens on Ethereum. Without migrating the assets to another blockchain, this exchange happens via decentralized cross-chain protocols (e.g., atomic swaps [59] with HTLC [31] and adaptor signatures [93]). In this process, each party retains its assets

on its respective blockchains, but they achieve an equal-value swap.

Asset Migration. Asset migration refers to moving the asset from one blockchain to another, which encompasses locking or burning the asset in \mathcal{L}_S and creating or minting a representation of that asset in \mathcal{L}_T . Once the asset is locked in \mathcal{L}_S , the verification process is carried out in \mathcal{L}_T . This verification can be achieved by replicating the consensus mechanism of \mathcal{S} on \mathcal{T} [94], [95] or by employing proof-based mechanisms such as zero-knowledge proofs [15], [96], [97].

Data Transfer. Data transfer focuses on the transfer of information, such as transaction histories or the state of smart contracts, and extends the concept of interoperability. Information written in one chain can be transferred or replicated to another chain, typically accompanied by proofs, such as the payload of a blockchain view [98]. Blockchain gateways are frequently employed to support this process, functioning via gateway-to-gateway protocols. [99]. Examples include coordinating and managing decentralized autonomous organizations (DAOs) governance and actions across chains.

F. Trust Model of Interoperability

Zamyatin et al. [30] have demonstrated that in an asynchronous setting, *CCI* is fundamentally impossible without a TTP. Therefore, the trust model is a crucial element that must be addressed when discussing interoperability solutions, and it is typically categorized into the following three types.

TTP. The simplest method of cross-chain verification relies on a TTP to verify state changes across chains during interoperability execution. TTP-based solutions are typically realized through external validators or consensus committees. External validators outsource the cross-chain verification process to a trusted custodian that is independent of both \mathcal{S} and \mathcal{T} , bypassing the need for on-chain validation. These external validators may be static or dynamic and are often incentivized to act honestly by staking assets on relevant blockchains. Alternatively, consensus committees, composed of members from either \mathcal{S} or \mathcal{T} , can handle verification. The committee members reach a consensus on the ledger's state through mechanisms such as *BFT* [100] or *the longest chain rule* [101]. Misbehaviour by committee members can be viewed as a failure of the chain itself. In practice, external validators can be implemented via multi-signature contracts, requiring a set of signatures from the validators. The vote of the consensus committee is implemented through smart contracts, ensuring that committee members agree upon the execution outcome.

Synchrony. This model does not rely on TTP but assumes synchronized communication between participants and derives security from cryptographic hardness assumptions by using locking mechanisms. Such protocols are often referred to as non-custodial protocols, as they avoid transferring asset custody to a TTP.

In the worst-case scenario, a failure would result in permanently locking funds rather than providing any financial gain to a third party. In practice, this model is realized through technologies such as HTLC, adaptors, time-lock puzzles [102], and verifiable delay functions (VDFs) [103], often in combination with smart contracts.

Hybrid. In cases where a party crashes or the synchrony assumption fails. i.e., when a predefined timeout is exceeded, the watchtower is employed to enforce commitments [104]. This structure was first introduced and applied to off-chain payment channels [105], which can help channel users monitor the blockchain online in real-time and perform specific actions on behalf of users when needed. It is particularly useful in atomic swaps utilizing HTLC, where one party crashes after the secret in the hash lock has been revealed. Additionally, we refer to the model that incorporates both TTP and synchrony as the Hybrid model.

G. Interoperability Layers

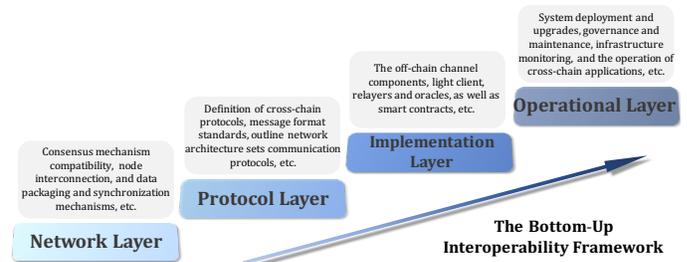


Fig. 10. Interoperability layers.

From a security perspective, interoperability solutions can be categorized into multiple layers, as shown in Fig. 10. This layered classification is supported by existing literature [12], [106].

Network Layer serves as the foundation, focusing on the underlying logic of interoperability solutions, such as the validity and compatibility of consensus rules, methods of node interconnection, local data packaging, and synchronization mechanisms. This layer is critical in distinguishing between homogeneous and heterogeneous solutions. *Protocol Layer* addresses the architectural decisions required for constructing interoperability protocols. This includes defining various types of participants, their roles and responsibilities, as well as ensuring security, performance, standardizing message formats, etc. *Implementation Layer* involves the development of complex on-chain and off-chain components, while accounting for diverse programming languages, smart contract standards, oracles, etc. Finally, *Operational Layer* covers system deployment, updates, maintenance, regulatory oversight, governance, the operation of external validators, and the management of dApps in cross-chain contexts, etc. Most solutions span at least one or two layers. The following sections concentrate on the key layers targeted by each solution.

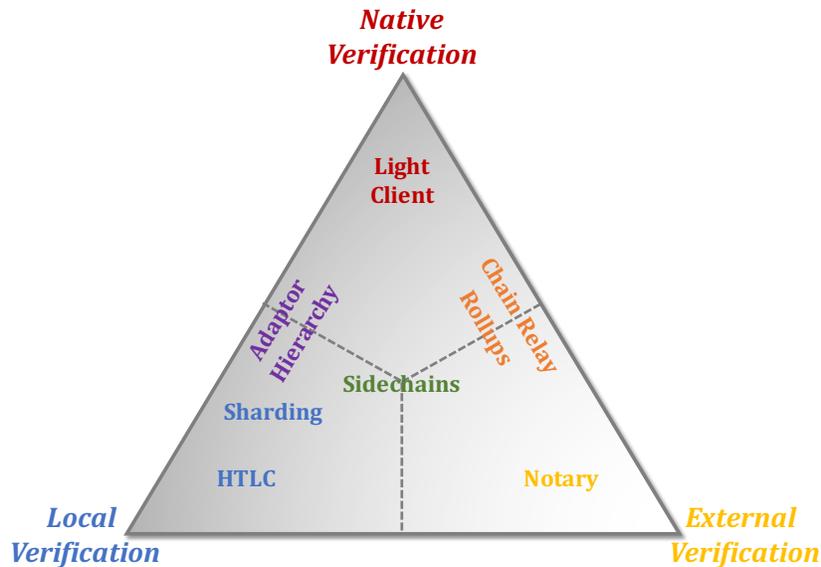


Fig. 11. Technology classification triangle (The darker the gray color, the stronger the trustlessness).

IV. EXISTING SOLUTIONS

This section presents concrete solutions. Categorizing blockchain interoperability has been a persistent challenge. In reality, each classification may overlap, indicating there is no universally fixed categorization [28]. Our approach focuses on interoperability verification, dividing it into native verification, local verification, and external verification. The specific technologies are outlined in Fig. 11.

- *Native verification* refers to cross-chain transactions or states verified directly through the blockchain’s consensus mechanism and rules, without reliance on third parties. Here, the verification is entirely performed on-chain by the nodes of either \mathcal{S} or \mathcal{T} , with security ensured by the blockchain’s inherent model. For example, one blockchain might synchronize the state or block headers of another using a light client and verify based on the consensus of the counterpart chain. This method, relying on internal rules and consensus algorithms, is considered decentralized and trust-minimized.
- *External verification* involves cross-chain transaction or state verification by an external third party (often witnesses or validators) that does not directly belong to \mathcal{S} or \mathcal{T} . This process relies on independent intermediaries or validator networks (e.g., MPC network, TEE network, Multi-signature group, or Oracles [107]), which can be centralized or decentralized, ensuring transaction integrity.
- *Local verification* pertains to operations or transactions on a specific chain, verified directly by the chain’s local nodes, without requiring external chain data. For example, in state channels, participants verify each other’s transactions during execution and settlement. This method applies to intra-chain transactions and is generally used to secure smart

contracts, state transitions, or transaction execution on-chain. Given the opposing economic interests of the transacting parties, the potential for collusion is effectively eliminated.

Consider three trustless verification mechanisms with respective security metrics: source chain security, M_1 ; target chain security, M_2 ; and external verifier security, M_3 , where external verification introduces an additional security assumption. Thus, the security metric for *CCI* is approximated as $M = \text{Min}(M_1, M_2, M_3)$ under external verification, $M = M_1 \oplus M_2$ under local verification (assuming fully opposing transacting parties), and $M = \text{Max}(M_1, M_2)$ under native verification. Generally, M_3 represents the weakest link, often criticized in external verification despite its higher efficiency.

Chain relay integrates both native and external verification mechanisms. Typically, chain relay achieves native verification through its consensus, while occasionally utilizing external validators, such as intermediary networks, specific nodes, or Oracles to assist in verifying cross-chain transactions. In contrast, rollups process and compress large volumes of transactions on Layer-2, subsequently submitting the aggregated results to the Layer-1 main chain to ensure data integrity and state consistency. Rollups mandate that Layer-2 inherit the security properties of Layer-1, such that only the state finalized on Layer-1 is accepted as authoritative. As a result, rollups effectively combine native and external verification mechanisms. Sidechains, on the other hand, can be designed with centralized, consortium-based, or SPV-based anchoring methods, positioning them centrally within Fig. 11. The following sections delve into each technology’s unique characteristics, providing a detailed analysis of their respective technology’s unique characteristics.

TABLE V
COMPARATIVE ANALYSIS OF INTEROPERABILITY SOLUTIONS BASED ON HTLC

Reference	Technique	Trust Model	Privacy ^①	Generic	Summary of Advantages
LN [13]	HTLC	Synchrony	✓	●	It Creates a network of micropayment channels that enables bitcoin scalability, micropayments down to the satoshi, and near-instant transactions.
CheaPay [120]	CHTLC	Synchrony	✗	▶	It examines the issue of payment routing in PCNs through an optimization lens, intending to minimize the transaction fee associated with a payment path.
AMHLs [121]	Multi-hop lock	Synchrony	✓	▶	It serves as a versatile primitive, applicable beyond multi-hop payments in PCNs, and illustrates how this primitive can be leveraged to achieve <i>CCZ</i> within PCNs.
Deshpande et al. [122]	HTLC and Schnorr signatures	Hybrid	✓	▶	It introduces the primitive of atomic release of secrets (ARS), which facilitates the atomic exchange of pre-agreed secrets in transactions, and illustrates how ARS can be applied to build privacy-protecting atomic swaps.
MAD-HTLC [123]	HTLC-Spec	Synchrony	✗	▶	A new approach is proposed that harnesses miner rationality to secure smart contracts, and it is employed to design MAD-HTLC, which implements the HTLC-Spec.
Cross Channel [124]	HTLC, zk-SNARK	Hybrid	✓	▶	It is the first off-chain channel that supports cross-chain services, effectively reducing the high latency inherent in asynchronous networks, and delivering both strong security and practical utility.
zkCross [125]	HTLC and zk-Rollup	Hybrid	✓	●	It overcome three important challenges in cross-chain privacy-preserving auditing, namely Cross-chain Linkability Exposure, Incompatibility of Privacy and Auditing, and Full Auditing Inefficiency.

^① Privacy involves safeguarding the confidentiality of the identities of the sender and receiver, payment amount, and payment path within *CCZ*.

A. Atomic Swaps

Atomic swaps is a type of contract that facilitates decentralized cryptocurrency exchanges [59]. In this context, the term “atomic” implies that the transfer of ownership of one asset inherently triggers the transfer of ownership of another, satisfying the *atomicity* property defined in Def. 6. This concept was first introduced by TierNolan on the Bitcointalk forum in 2013 [108]. For four years, atomic swaps remained largely theoretical. Until 2017, when Charlie Lee, the founder of Litecoin [109], tweeted about successfully performing a cross-chain atomic swap between LTC and BTC, exchanging 10 LTC for 0.1167 BTC. Since that event, numerous decentralized exchange platforms and independent traders have adopted the technology for cryptocurrency trading [110]. Additionally, specialized cryptocurrency wallets, such as Atomic Wallet [111] and Liquidity, have been developed to facilitate cross-chain atomic swaps.

Atomic swaps must maintain *fungibility*, meaning that observers of the ledger (aside from the transacting parties) should not be able to distinguish between transfers executed as part of an atomic swap and standard asset transfers on the same ledger. Currently, cross-chain atomic swaps require a minimum of four transactions, although some solutions attempt to reduce the number of transactions to two [112], but it will increase the real-time online requirements for the exchanging parties. The most commonly used atomic swap technologies include hash time-lock contracts (HTLC) [13], and adaptor signatures [113]. While some methods [114]–[116] propose deferring atomic swap functionality to *Trusted Execution Environments* (TEEs) [117], such solutions require all users to possess a TEE, which is impractical. Furthermore, recent research has revealed significant vulnerabilities in TEEs

[118], [119]. We next describe HTLC and adaptor signature techniques in detail.

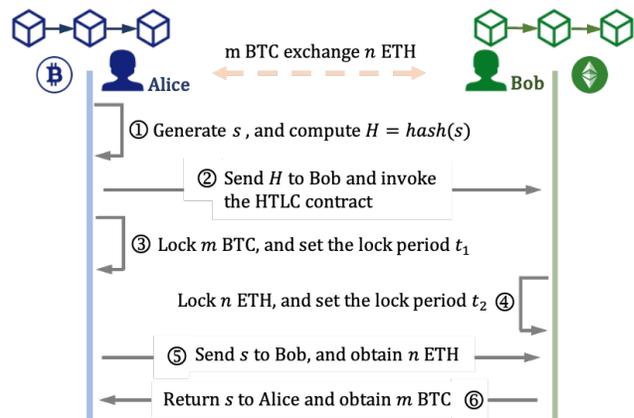


Fig. 12. HTLC interaction between two different blockchains.

1) **HTLC-Based Atomic Swaps:** HTLC was originally proposed to enable cross-chain transactions in DEXs [31] and serves as a core technology for atomic swaps [59]. It facilitates conditional payments across different blockchains through programmable logic and asset collateralization, with a notable application being *payment channel networks* (PCNs) [126]. The concept of HTLC is derived from sequential game theory [127], where users on the same or different blockchains make decisions in sequence, based on the order of time. These decisions form the basis of a game-theoretic approach to achieving cross-chain asset swaps via collateralized transactions. The core components of HTLC are time-lock and hash-lock. A time-lock ensures that both parties to a transaction must submit their respective actions within a predefined time frame for the transaction to be valid. The commitment for this transaction is void if the time

expires, and each party retains their assets. Conversely, a hash-lock involves setting a hash function, where a party can prove their commitment by revealing the pre-image s that generates the hash value $\mathcal{H} = \text{hash}(s)$. If the corresponding hash value \mathcal{H} is verified, the commitment remains valid; otherwise, it expires. HTLC allows for asset exchanges between distinct blockchain systems, ensuring that while the total quantity of assets on each blockchain remains unchanged, the ownership of these assets can be swapped, facilitating cross-chain asset exchange but not actual asset migration. Tab. V summarizes some of the HTLC solutions that we identified in the literature.

Technological Process of HTLC. For example, as shown in Fig. 12, consider the scenario where Alice, operating within the Bitcoin network, wishes to exchange m BTC for n ETH held by Bob in the Ethereum network: ① Alice generates a random secret s and computes its hash value $\mathcal{H} = \text{hash}(s)$; ② Alice sends \mathcal{H} to Bob and invokes the HTLC contract in the Ethereum network; ③ Alice then locks m BTC in the Bitcoin network through a locking contract, setting a time limit t_1 . This contract promises Bob that he can obtain the m BTC if he provides the pre-image s of \mathcal{H} within the time limit t_1 ; ④ Upon learning that Alice has locked m BTC, Bob locks n ETH in the Ethereum network under a similar locking contract with a time limit t_2 (where $t_2 < t_1$), promising Alice that she can claim the n ETH if she provides the pre-image s within time t_2 ; ⑤ Alice then sends s to Bob and unlocks the contract on Ethereum to receive n ETH. If she fails to unlock within t_2 , the system returns the n ETH to Bob; ⑥ Bob, upon receiving s , submits it to the Bitcoin network to unlock the m BTC. If the contract is not unlocked within t_1 , the system returns the m BTC to Alice.

Limitations of HTLC. HTLC-based atomic swaps are deployed in practice [31], [123] and have a wide range of applications [19], [57], [121]. Despite their advantages, these methods exhibit intrinsic limitations that undermine their utility, which we summarize below:

- *Compatibility of the Hash Function.* Both \mathcal{S} and \mathcal{T} must support compatible hash functions within their scripting languages, and each ledger must represent the hash function using the same number of bits. Otherwise, atomicity may be compromised, as one ledger might not allow sufficiently large pre-images [93]. Beyond atomicity, using the same hash value across both ledgers also raises privacy concerns, as observers could link two HTLCs as part of the same swap. Finally, a fundamental issue arises in that many cryptocurrencies, such as Monero [128], Ripple [129], or Zcash [130] (with shielded addresses), do not support HTLC contract computation in their scripting languages.
- *Limitations of Time-Lock.* To facilitate this feature, both ledgers must include support for time-lock functionality in their respective scripting languages.

However, adding time-lock conflicts with privacy protection for several reasons: ① It makes time-locked transactions easier to distinguish from transactions without time restrictions [131]; ② It may interfere with other privacy-enhancing operations already in place on the ledger [132]; ③ Even if it is possible to implement time locks in a privacy-preserving manner, it significantly increases computational and storage costs for the ledger [131], [133]; ④ Both parties involved in the transaction may be exposed to price speculation during the waiting period, such as front-running attacks [134]. Therefore, in such cases, designing privacy-focused cryptocurrencies requires avoiding time-locked assets as a design principle [93].

- *Single-Asset Swap.* The swap is limited to two parties and does not support multiparty exchanges. In addition, given the significant value differences among cryptocurrencies, current atomic swaps are typically restricted to small values of m (or n) to match swap offers (e.g. m BTC by n ETH). In practice, there are users, such as market makers or exchanges, who hold diversified portfolios across multiple ledgers. If multi-asset swaps were possible, they could leverage several of their assets to match swap offers more efficiently.

2) *Adaptor Signature-Based Atomic Swaps:* Adaptor signature [113] allows users to create a pre-signature for a message \mathcal{M} , which, on its own, is not valid. However, it can be transformed into a valid signature once the user reveals a specific secret value. Fig. 13 provides the formal definition of adaptor signatures. As a promising cryptographic primitive, it not only addresses several limitations of HTLCs, but have also found applications in areas such as DeFi, payment channel networks, multiparty signature protocols, and privacy-enhancing transactions. Recent research has investigated its use in multiparty atomic swap scenarios.

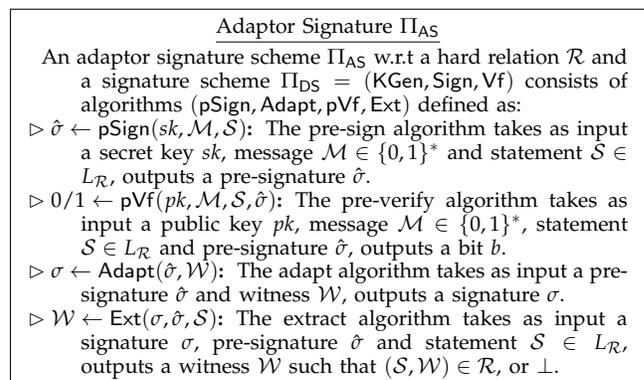


Fig. 13. A generic adaptor signature scheme.

Atomic swap protocol based on adaptor signature involves the interaction between an initiator on the source chain and a recipient on the target chain to exchange assets Tx_1 and Tx_2 , as illustrated in Fig. 14. To ensure

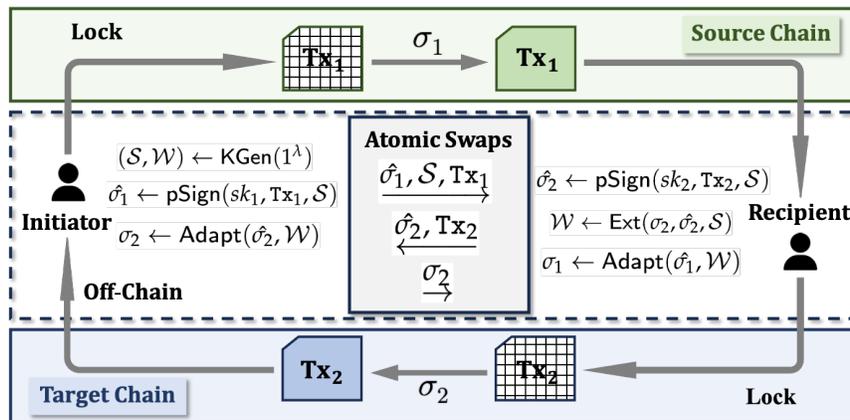


Fig. 14. Atomic Swaps based on adapter signature.

fairness, both parties apply time locks to the assets involved, primarily to provide the recipient with sufficient time to complete the transaction and prevent the initiator from claiming both assets. The protocol begins with the initiator generating a hard relation $(S, \mathcal{W}) \leftarrow \text{KGen}(1^\lambda)$, and using the statement S to produce a pre-signature $\hat{\sigma}_1$ for the transaction Tx_1 (i.e., transferring Tx_1 to the recipient). The pre-signature is then sent to the recipient, who verifies its correctness. Upon successful verification, the recipient uses the same statement S to generate a pre-signature $\hat{\sigma}_2$ for the transaction Tx_2 (i.e., transferring Tx_2 to the initiator), and returns it to the initiator. The initiator verifies $\hat{\sigma}_2$ and then adapts it into a full signature σ_2 using the witness \mathcal{W} . The initiator then broadcasts σ_2 on-chain to claim Tx_2 . Observing this, the recipient extracts \mathcal{W} from $\hat{\sigma}_1$ and σ_1 , adapts $\hat{\sigma}_1$ into a full signature σ_1 , and broadcasts σ_1 on-chain to claim Tx_1 . This completes the atomic and fair exchange process.

In Tab. VI, we provide a detailed analysis of the strengths, weaknesses, and suitability of various protocols.

Compared with HTLC. Atomic swaps utilizing adaptor signatures offer the following key advantages:

- *Reduced Lock Time and On-Chain State.* It eliminates the reliance on on-chain scripts like time-lock and hash-lock used in “secret-hash” swaps, thereby reducing the time assets remain locked.
- *Higher Off-Chain Efficiency.* The primary interactions in adaptor signature schemes occur off-chain, with only the final state requiring on-chain confirmation. This makes cross-chain transactions more lightweight and reduces complexity and transaction fees, especially in Multi-path Payment [135] and frequent cross-chain operations scenarios.
- *Enhanced Privacy.* While HTLC necessitates using the same hash value across chains, adaptor signatures decouple transactions, thereby minimizing the exposure of publicly visible information on-chain.
- *Support for Multi-Party and Multi-Chain Scenarios.* By incorporating multi-signatures or other cryptographic primitives, adaptor signatures provide

greater flexibility for multi-party, multi-chain, and multi-asset atomic swaps [93], [136], making them more scalable for complex cross-chain transaction environments.

Open Issues of Adaptor Signature. Despite the growing applicability of adaptor signatures, several unresolved issues or challenges remain. In multi-party atomic swap scenarios, mitigating collusion attacks continues to be a significant open problem. Possible solutions include employing reputation systems, mandating participants to furnish deposits or collateral, or utilizing advanced cryptographic methods like threshold signatures or MPC. Nevertheless, these approaches may add significant complexity and overhead to the protocols. While some multi-party atomic swap protocols [93], [136] have made substantial progress in cross-chain asset exchanges, it is crucial to acknowledge the limitations and assumptions of these protocols. In PipeSwap [137], it was pointed out that the scheme in [93] is vulnerable to *double-claiming* attacks, which are relatively easy to execute and can naturally extend to other scriptless cross-chain swap protocols and PCNs. Future research should address these challenges and enhance the protocols’ robustness in real-world scenarios.

B. Notary-based Token Swap Bridges

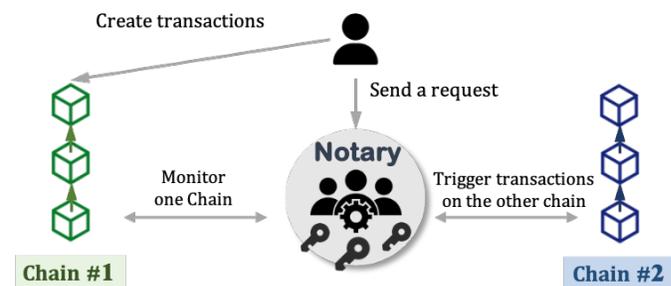


Fig. 15. Workflow of a notary-based scheme via a TTP.

Due to the independence of different blockchains in cross-chain transactions, they cannot directly understand

TABLE VI
COMPARATIVE ANALYSIS OF INTEROPERABILITY SOLUTIONS BASED ON ADAPTOR SIGNATURE

Reference	Object	Generic	Strong Points	Weak Points
[122]	Two-Party	○	It represents an atomic secret release scheme that is built upon the combination of adaptor signatures and the Schnorr signature algorithm.	They are limited to two-party and do not consider the challenges of multi-party atomic swaps scenario.
[14]			It is an enhanced two-party adaptor signature scheme grounded in quantum-secure coding theory problems.	
[138]	Multi-Party	●	It proposes a generalized adaptor signature scheme for N parties, enabling secure multi-party transactions.	They often focus on specific scenarios or address a limited set of potential attack vectors. Potential vulnerabilities linked to time-lock puzzle mechanisms and the computational burden of managing multiple blockchains still require resolution.
[139]			It proposes a privacy-preserving multi-party cross-chain transaction protocol based on a novel pre-adaptor signature scheme.	
[140]			It proposes the concept of threshold adaptor signatures for enhancing the security and fault tolerance of multi-party swaps.	
[93]	Multi-Party Non-custodial Multi-Asset Universal	●	It establishes a complete framework for general atomic swaps, incorporating adaptor signatures and time-lock puzzle techniques to optimize practicality.	
[136]			It represents the first fully scalable off-chain atomic swap protocol, supporting multiple participants (of any number), while ensuring zero overhead for the local blockchain, without the dependency on smart contracts or trusted third parties.	

or verify the state changes on each other's chain. Therefore, a trusted intermediary, known as a "Notary", is introduced to act as a bridge between the two chains. Notaries are widely used for their efficiency and ease of implementation [49], [141], [142]. A typical notary workflow can be described as follows (Fig. 15):

- *Initiating Transactions.* The user initiates a transaction or event on \mathcal{L}_S (e.g., locking a certain amount of tokens).
- *Notary Verification on \mathcal{S} .* The notary monitors the transaction on the \mathcal{S} and verifies whether the transaction has been successfully executed. Verification usually involves checking whether the transaction has been confirmed by the consensus mechanism of \mathcal{S} .
- *State Notification to \mathcal{T} .* Once the notary confirms the event or transaction on \mathcal{L}_S , it notifies \mathcal{T} , indicating that the event has occurred. For example, the notary can issue proof on \mathcal{T} to indicate that assets on \mathcal{S} have been locked.
- *Execution of Cross-Chain Operation.* Based on the notary's proof, \mathcal{T} executes the corresponding operation on-chain, such as releasing an equivalent amount of assets or triggering a cross-chain smart contract call.

Notary Evolution. Variants of this mechanism include centralized notary schemes and decentralized notary schemes. Tian et al. [143] designed a decentralized notary scheme for executing atomic swaps in cryptocurrency exchange protocols. This protocol involves a verification committee (a group of notaries) responsible for inspecting and verifying transactions, with a notary election mechanism mitigating the risk of a single point of failure. Similarly, RenVM [136] employs a Byzantine Fault-Tolerant network combined with Secure Multi-Party Computation (SMPC) to facilitate cross-chain asset transfers, replacing centralized custodianship with a decentralized, trustless custodian model.

While distributed collective signatures enhance the

decentralization of notary groups, this method does not eliminate the issues of trust and incentives for notaries. As a result, some researchers have turned to reputation metrics to address trust issues associated with notaries. Xiong et al. [144] improved the reliability of notaries by refining the internal selection process of the notary group and integrating collateral pools with a reputation-driven incentive system. Niu et al. [145] introduced an enhanced reputation value model that ensures notary reliability while reducing the risk of over-centralization. Zhao et al. [146] developed a reputation-based notary election mechanism using an advanced PageRank algorithm, effectively preventing malicious nodes from becoming notaries. Similarly, Sun et al. [147] adopted a reputation-based election method, randomly selecting notaries from high-reputation candidates to handle cross-chain transactions, while updating reputation values to restrict malicious behavior by notaries. Hu et al. [148] introduced reputation decay and dynamic window mechanisms to prevent inactive malicious notaries from regaining reputation over time. In contrast to these approaches, Bool Network [141] is a secure notary platform that uses Ring VRF and TEEs to hide the notary group, reducing trust conflicts.

Limitations of Notary. Notary-based cross-chain technology, valued for its simplicity and flexibility, is theoretically compatible with most heterogeneous blockchain interoperability needs. However, its reliance on external notary entities introduces a trust assumption that undermines the core principles of decentralization and trustlessness in blockchain systems. This has become a major obstacle to its broader adoption. In practice, the approach is mainly used in low-frequency cross-chain scenarios, such as asset transfers or cross-chain smart contract calls, where accuracy is critical but real-time performance is not. The system's security and correctness depend entirely on the notary's proper behavior. Moreover, its dependence on off-chain entities

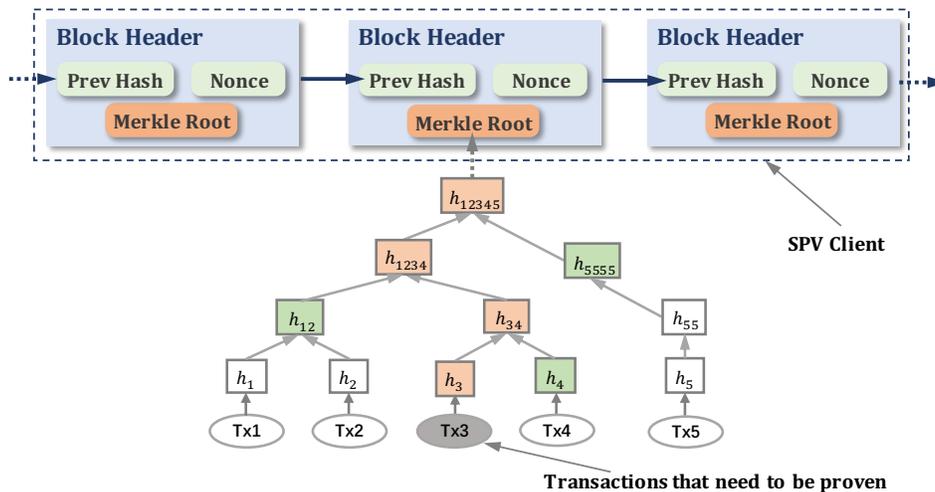


Fig. 16. Simplified Payment Verification. The orange items in the Merkle Tree constitute the proof of Tx3. The green item can be computed and validated against the Merkle Root.

introduces regulatory and compliance risks. If notaries are influenced by legal or policy constraints, the system may lose its neutrality and global accessibility. These limitations make notary-based solutions more suitable for short-term, domain-specific applications rather than fully autonomous and secure cross-chain ecosystems. As a result, researchers are increasingly exploring alternative cross-chain mechanisms to balance decentralization with performance better.

C. Light Client

Interoperability verification is typically achieved by running full nodes or employing **light clients** with linear storage overhead, which scales with the length of \mathcal{S} . The core concept of the light client was first introduced by Satoshi Nakamoto in his original whitepaper [1] as an SPV solution.

A Light Client [149] is a type of node in blockchain networks that, compared to full nodes, aims to provide fundamental verification and interaction capabilities with significantly lower resource and storage requirements. As a result, this technology serves as a low-cost alternative for node implementation and can act as a bridge for data verification and communication in blockchain interoperability mechanisms. Specifically, a light client leverages the consensus mechanism of the source chain to ensure the authenticity of data, while functioning as a verification module on the target chain to validate the legitimacy of transactions from the source chain. In scenarios requiring cross-chain synchronization of account states (e.g., balances or assets), the light client enables efficient state synchronization by verifying block headers and associated state proofs. As a result, the security of light clients often depends on the robustness of $\mathcal{L}_{\mathcal{S}}$ (see Def. 4 for details).

Simplified Payment Verification (SPV). SPV operates by utilizing Merkle proofs, a critical component that allows light nodes to verify whether a transaction is included in a block without downloading the entire

block (see Fig. 16). Specifically, a transaction’s Merkle proof consists of its Merkle path and the root of the Merkle tree. The Merkle path is a collection of sibling nodes along the path from the transaction to the root of the tree. By verifying the Merkle path, a light node can confirm that the transaction indeed exists within a specific block, thus participating in the blockchain network without maintaining the entire chain’s data.

Light Client Evolution. While SPV light clients save storage space (Bitcoin’s block headers are around 80 bytes compared to the full block size of about 1MB), they still require processing a large amount of data proportional to the chain’s length. For Bitcoin, this amounts to approximately 60MB of storage, while for Ethereum, it requires around 4GB. To reduce this storage burden, various optimizations have emerged. The first succinct construction was the interactive *Proofs of Proof-of-Work* (PoPoW) protocol [150], which achieves polylogarithmic communication costs. INPoPoW [151] removed the need for interactivity and provided security and succinctness for $1/2$ adversaries under optimistic conditions. This was later optimized [158] and further improved to more practical solutions [159], with backward compatibility ensured through redesigns [160]. In later work, the optimistic environment constraint was addressed, enabling succinctness for all adversaries, with security guarantees for up to $1/3$ threshold adversaries [161]. Another alternative, FlyClient [152], was proposed to provide security and succinctness for $1/2$ adversaries, adding support for variable difficulty adjustments.

More recently, universal (recursive) zero-knowledge (ZK) technologies have been employed to construct light clients with constant communication overhead [15], [153], [154]. For example, DendrETH [154] is a decentralized and efficient ZK proof-based light client, which mitigates security problems by lowering the attack surface by relying on the properties of ZK proofs. However, these methods incur high computational costs and require a trusted setup for key generation and verifica-

TABLE VII
COMPARISON OF LIGHT CLIENT SOLUTIONS.

Concrete ^① Type	References	Information Relayed	Backward Compatibility ^②	Storage Overhead	No Trusted Setup	Upfront Mining Secure ^③	Communication ^④ Complexity
LC	[55] [96] [94]	Linear	✓	Linear	✓	✓	$\mathcal{O}(C)$
SLC	[150] [151] [152]	Logarithmic	✗	Logarithmic	✓	✓	$\mathcal{O}(k \cdot \text{polylog}(C))$
ZK	[153] [15] [154]	Linear	✓	Constant	✗	✓	$\mathcal{O}(1)$
SSPV ^⑤	[155] [156]	Constant	✓	Constant	✓	✗	$\mathcal{O}(k)$
	[91]					✓	
PSLC	[157]	Constant	✓	Constant	✓	✓	

^① *Abbreviation:* Light Client (LC), Super-Light Client (SLC), Zero-Knowledge Based (ZK), Stateless SPV (SSPV), Provably Secure Light Client (PSLC).

^② Super-light Clients with logarithmic complexity were proposed [150]–[152], but they either require constant PoW difficulty [151] or an hard fork in Bitcoin [152], and are thus not backward compatible.

^③ By knowing the transaction to be verified in advance, a malicious prover can exploit the fact that users on S cannot ensure that the proof corresponds to the correct suffix of the chain. The prover can pre-construct a forged subchain. Since there is no backward time constraint on executing an upfront mining attack, the attacker will eventually succeed in finding a sufficient number of forged blocks, regardless of their mining power or the need to bribe any miners [91].

^④ Let C denote the lifetime of the system (informally, the length of S or \mathcal{T}) and k denote the security parameter. According to Def. 4 with the Bitcoin Backbone model [82], k is the *common prefix* parameter, which is constant for a protocol execution, albeit with the trade-off of logarithmically increasing the probability of failure in the lifetime of the system.

^⑤ In SSPV, users provide proof π to the smart contract with quasi-Turing completeness hosted on \mathcal{T} , convincing it that a transaction has appeared on PoW-based S . This proof consists of the block header containing the transaction, the Merkle inclusion proof of the transaction within the block, and n subsequent confirmation block headers. The smart contract subsequently validates the Merkle proof and ensures that each of the $n + 1$ block headers constitutes a legitimate subchain of its parent chain, and ensures that all headers contain sufficient PoW, meaning their hash values are less than the predetermined target.

tion. To develop a constant communication light client without the need for a trusted setup, the concept of *stateless SPV* (SSPV) was proposed by Prestwich [162] and implemented by Summa [163]. Recently, Barb ara et al. [164] implemented, and for the first time formalized, stateless SPV within the BxTB cross-chain exchange. However, Scaffino et al. revealed that this construction is vulnerable to upfront mining attacks, rendering it insecure [91]. They proposed a new protocol named Glimpse [91], which builds on the stateless SPV idea by introducing high-entropy transactions to prove that the provided chain segment is “fresh” and not pre-mined. Aumayr et al. [157] refined the problem of PoPoW and proved that Blink has optimal communication cost, constructing the first provably secure Optimal Proof of Proof-of-Work without a trusted initialization Setting. A comparative summary of various light clients for *CC* verification is presented in Tab. VII.

Open Issues of Light Client. Research focus has shifted from SLC and SSPV to PSLC (see Tab. VII), with an emphasis on reducing cross-chain verification size and communication complexity without compromising security. However, no solution has been developed that fully satisfies functional, security, and efficiency properties while remaining practical for clients and minimizing overhead for consensus participants or full nodes [149]. Existing studies have not sufficiently addressed the inefficiencies associated with frequent offline phases of light clients. Even for light clients with efficient bootstrapping protocols, frequent offline periods may still be inefficient due to the time lag in synchronizing with the blockchain state. Future research may explore the delegation of certain computational tasks of light clients to participants on the source chain, such as consensus nodes or full nodes. By introducing appropriate incen-

tive mechanisms, this approach can ensure the feasibility and reliability of such delegation. Not only does this strategy significantly reduce the storage and computational burden on light clients, but it also improves overall system efficiency, offering a more optimized solution for cross-chain verification and state synchronization.

D. Sidechains with Wrapped Assets

Sidechains, also known as pegged sidechains, is a cross-chain technique that facilitates blockchain interoperability by supporting bidirectional transfers between blockchains [16]. In addition to enhancing interoperability, sidechains contribute to the scalability and upgradability of blockchains [165]. They enable blockchains to offload transactions, executing them on sidechains, thus promoting scalability. Furthermore, new functionalities can be explored by bootstrapping sidechains from the mainchain.

Two-way peg mechanisms can be categorized as centralized or federated. In a centralized two-way peg, a TTP performs token locking, which offers speed and simplicity but introduces a single point of failure and centralization [74]. In contrast, the federated two-way peg distributes control among a group of notaries, thereby mitigating issues of centralization and single points of failure [16], [166]. Depending on the mode of implementation, two-way Pegs can be implemented as following five modes: Single Custodian, Consortium, SPV, Driving Chain and Hybrid, with specific descriptions and comparison referenced in Tab. VIII.

Fig. 17(a) illustrates the bidirectional transfers facilitated by a two-way peg. To transfer assets from the mainchain to the sidechain, users send assets to an external address associated with a consortium [16], which

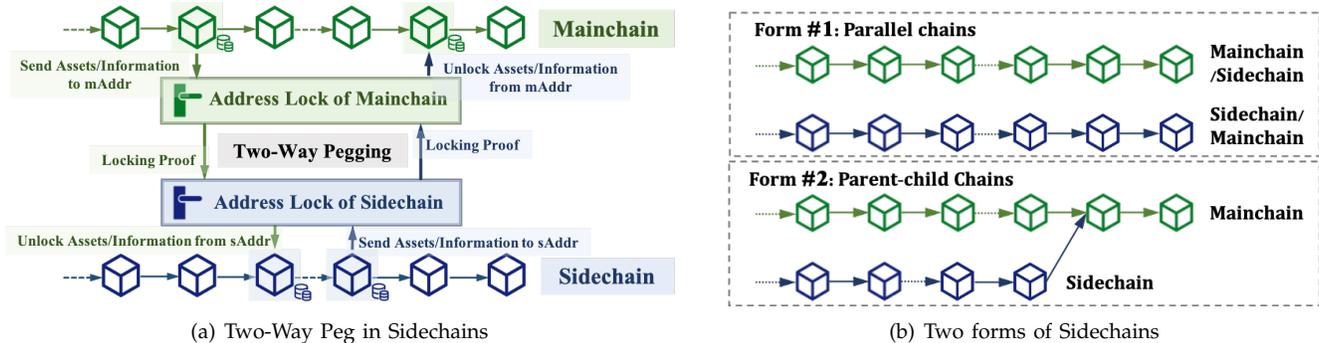


Fig. 17. Sidechains construction and types.

TABLE VIII
PERFORMANCE COMPARISON OF DIFFERENT TWO-WAY PEGS MODE FOR SIDECHAINS IMPLEMENTATIONS.

Benchmark	Single Custodian	Consortium	SPV	Driving Chain	Hybrid
Realization Approach ^①	Central Exchange	Multi-Party Signature	Soft Fork	Soft Fork	Soft Fork
Implementation Difficulty ^②	○	○	►	►	●
Security Strength ^③	○	►	►	►	●
Degree of Centralization	●	►	○	►	►
Interoperability Efficiency	●	●	○	►	►
Trust Model	TTP	TTP	Synchrony	TTP	Hybrid
Typical Case	Liquid [168]	Cumulus [169]	Pegged Sidechains [53]	Drivechain [170]	IBC [23]

^① Driving Chain allows miners from the mainchain to control the sidechain. By involving mainchain miners in the consensus process of the sidechain, this mechanism ensures the security of the sidechain. Hybrid model combines characteristics from the aforementioned models to achieve higher security, decentralization, and flexibility. Typically, Hybrid model selects different mechanisms based on specific needs, such as a combination of Consortium with SPV. The security of these three models—Consortium, SPV, and Driving chain—relies on the longest-chain rule [101], so their implementation often requires a soft fork [171].

^② Sort order (from low to high): Single-Custodian>Consortium>SPV>Driving Chain>Hybrid. The first two are relatively straightforward, as they do not require complex cross-chain protocols or smart contract mechanisms. SPV relies on light client verification. The latter two demand deep modifications to blockchain infrastructure, making them more challenging to implement.

^③ Sort order (from low to high): Single-Custodian>Consortium>Driving Chain>SPV>Hybrid. The security of TTP-based models is relatively weak, and in SPV, if the light client is maliciously compromised (e.g., eclipse attack) [172], it could result in faulty cross-chain verification. In Driving Chain, insufficient economic incentives for miners may still pose security risks. Hybrid model, which combines the strengths of other approaches, offers the highest level of security.

acts as an intermediary for locking and unlocking assets or information. After a specified transaction time commitment, the consortium releases equivalent assets on the sidechain. As depicted in Fig. 17(b), sidechains are generally divided into two types: parallel chains and parent-child chains, where the mainchain serves as the parent in the latter.

Wrapped Assets in sidechains are digital representations of underlying assets on other chains. They are deposited (wrapped) on \mathcal{S} when the corresponding original tokens have been locked on \mathcal{T} , and then they are destroyed or withdrawn (unwrapped) to redeem the original ones. This category encompasses assets issued on sidechains and collateralized on parent chains, such as Liquid [166] tokens L-BTC wrapped by BTC. It also includes wrapped tokens, such as WBTC on Ethereum [167] wrapped by BTC.

Sidechains Evolution. The current researches on sidechains primarily focus on three key technical dimensions: universality, performance, and security. We provide a detailed comparison of these research works across key metrics such as universality, proof size, and computational cost, as summarized in Tab. IX.

Universality. To enhance the universality of sidechain

constructions, several researchers have proposed innovative approaches. Kiayias et al. [176] introduced a PoW sidechain architecture applicable to blockchain systems using PoW consensus. Similarly, Gaži et al. [165] presented a construction designed for PoS blockchains. Westerkamp et al. [96] developed zkRelay, another sidechain framework compatible with PoW systems. Additionally, Yin et al. [177] proposed two distinct sidechain architectures: one optimized for speed within PoS blockchains and another for efficiency in PoW systems. Compared to earlier studies [55], [170], [173], these approaches expanded the applicability of sidechain solutions, extending beyond specific blockchain systems to support a broader range of blockchain consensus mechanisms. However, these solutions still necessitate forking of the mainchain, introducing potential security vulnerabilities, and face limitations when enabling interoperability between heterogeneous blockchains. To further improve universality, Zedoo [97] employs zk-SNARKs [181] to enable secure communication between a mainchain and multiple sidechains without relying on trusted intermediaries, making it compatible with various blockchain consensus models. The protocol remains susceptible to security risks despite these advancements

TABLE IX
COMPARISON AMONG DIFFERENT SIDECHAINS CONSTRUCTIONS.

Schemes	Universality			PS ^③	CC ^④	SM
	AR ^①	VD ^②	H ^③			
BTCRelay [55]	PoW Chains	No	✗	$\mathcal{O}(C)$	$\mathcal{O}(C)$	SPV
zkRelay [96]	PoW Chains	No	✗	$\mathcal{O}(C)$	$\mathcal{O}(C)$	SPV
ETHRelay [94]	PoS Chains	No	✗	$\mathcal{O}(C)$	$\mathcal{O}(C)$	SPV
Drivechains [173]	PoW Chains	No	✗	$\mathcal{O}(C)$	$\mathcal{O}(C)$	Driving Chain
SEPoW [174]	PoW Chains	No	✗	$\mathcal{O}(\log(C))$	$\mathcal{O}(\log(C))$	Driving Chain
FlyClient [152]	PoW Chains	Yes	✗	$\mathcal{O}(k \cdot \text{polylog}(C))$	$\mathcal{O}(k \cdot \text{polylog}(C))$	SPV
Txchain [175]	PoW Chains	Yes	✗	$\mathcal{O}(k \cdot \text{polylog}(C))$	$\mathcal{O}(k \cdot \text{polylog}(C))$	SPV
PoW Sidechains [176]	PoW Chains	No	✗	$\mathcal{O}(\log(C))$	$\mathcal{O}(\log(C))$	Consortium
PoS Sidechains [165]	Pos Chains	No	✗	$\mathcal{O}(S)$	$\mathcal{O}(S)$	Consortium
Yin et al. [177]	PoW or PoS Chains	Yes	✗	$\mathcal{O}(S)$	$\mathcal{O}(S)$	Consortium
PSSC [178]	Chains with SNARK	N/A	✓	$\mathcal{O}(1)$	N/A	Hybrid
Zendoo [97]	Chains with zk-SNARK	N/A	✓	$\mathcal{O}(1)$	N/A	Hybrid
Cumulus [169]	Chains with customized SC	N/A	✓	$\mathcal{O}(1)$	N/A	Consortium
USSC [179]	PoW or PoS Chains	Yes	✓	$\mathcal{O}(S)$	$\mathcal{O}(S)$	Consortium
Ge-Go [180]	PoW or PoS Chains	Yes	✗	$\mathcal{O}(1)$	$\mathcal{O}(1)$	Consortium
Glimpse [91]	PoW Chains	Yes	✓	$\mathcal{O}(k)$	$\mathcal{O}(k)$	Hybrid

★ *Abbreviation.* AR: Applicability Range; VD: Variable Difficulties; H: Heterogeneous; PS: Proof Size; CC: Computation Cost; SM: Sidechains Mode.

^① In the parent-child chains form, only the mainchain serves as the study object of applicability range. This is because the sidechain is bootstrapped from the mainchain and has customizability. Additionally, we consider the mainchain with basic payment functionality. Here SC means smart contract.

^② This refers to whether the sidechains construction can be applied to various sidechains with variable difficulties.

^③ Which means whether a sidechains construction supports the interoperability between heterogeneous systems; for instance, PoW-based chains communicate with PoS-based chains.

^④ Let C denote the lifetime of the system (informally, the length of the mainchain or sidechain) and k denote the *common prefix* parameter. S is the validation set (or committee) size.

due to potential forks. PSSC [178] leverages SNARK technology to construct a general sidechain architecture tailored for IoT environments, which supports heterogeneous chains while maintaining constant storage size. However, the complex script language design poses challenges for practical application.

Efficiency. Some researchers have focused on improving the efficiency of sidechains. In systems like BTCRelay [55], zkRelay [96], and ETHRelay [94], cross-chain proofs consist of block headers that increase linearly with the length of the chain, resulting in substantial storage and communication overhead for the nodes in sidechains. To reduce the size of these proofs, Kiayias et al. [150] introduced PoPoW, a cryptographic primitive that generates succinct proofs of transactions occurring in PoW blockchains. In this approach, the complexity of the proof is sublinear to the length of the PoW blockchain. To further minimize proof sizes, Kiayias et al. [151] proposed NIPoPoW, which scales logarithmically with the length of the blockchain. However, NIPoPoW is limited to blockchains with fixed block difficulty. FlyClient [152], and Txchain [175] improved upon NIPoPoW, achieving smaller proof sizes with logarithmic complexity, but these protocols require continuous PoW difficulty or Bitcoin hard forks, making them not backward-compatible. Additionally, other works [15], [182] leverage zk-SNARKs to reduce the size of the

proofs, ensuring that the proof size remains constant, regardless of the length of the blockchain.

Security. The security of sidechain constructions largely depends on the level of decentralization and the fulfillment of three key security properties: *persistence*, *liveness* (Def. 4), and *atomicity* (Def. 6). Dilley et al. [166] introduced a federated model that facilitates cross-chain asset transfers among various blockchains. This model employs trusted federated boards to manage assets, allowing transfers only when most board members approve, thereby mitigating centralization risks. Kiayias et al. [176] proposed the first decentralized sidechain framework specifically for PoW blockchains. Similarly, Gaži et al. [165] developed the first formal framework for PoS sidechain constructions, offering rigorous security processing and validation. Other works, like Cosmos [23], Polkadot [57], and Liquid [168], have also made improvements to cross-chain verification. Their validation relies on trusted committees or federations or is left unspecified, lacking formal security definitions.

Compared with Light Client. The primary technical distinction between sidechains and light clients lies in their respective verification targets. Sidechains verify the nodes on either the main or sidechain, while light clients verify transactions for lightweight nodes. A sidechain is an independent chain capable of supporting high-frequency transactions, providing a smart contract ex-

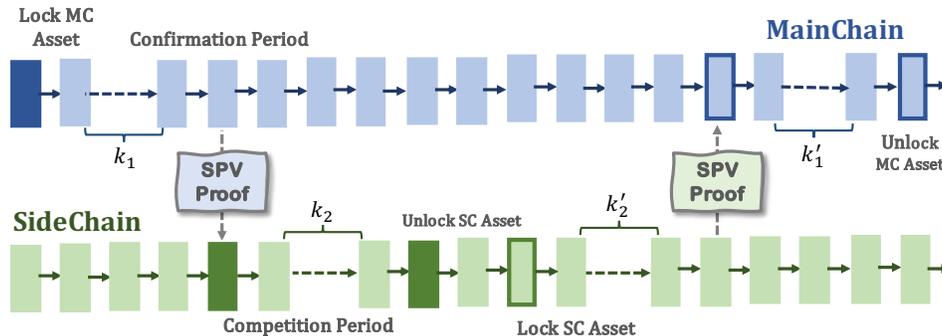


Fig. 18. Conventional wrapped assets transfer for SPV sidechains from \mathcal{S} to \mathcal{T} and back again.

ecution environment [80], and performing consensus mechanisms [72]. In contrast, a light client serves as a lightweight verification system that does not participate in consensus but merely validates the correctness of transactions.

However, both technologies share common ground in that they can utilize the lightweight verification mechanism derived from SPV. As illustrated in Fig. 18, we present a simplified wrapped asset transfer process based on SPV sidechains as an example, which can be simplified as following steps: ① Lock the assets of \mathcal{S} ; ② Wait for a confirmation period on $\mathcal{L}_{\mathcal{S}}$ (k_1 blocks) to ensure sufficient proof of work, which helps resist DoS attacks; ③ After the confirmation period, the user creates a minting transaction on $\mathcal{L}_{\mathcal{T}}$ with SPV proof of lock transaction in \mathcal{S} . The assets of \mathcal{T} remain locked during a competition period; ④ During the competition period, which prevents double-spending, other users can provide an updated SPV proof to invalidate the minting transaction of \mathcal{T} if the mainchain assets are moved. This is called a reorganization proof; ⑤ After the competition period (k_2 blocks¹), the tokens of \mathcal{T} are minted and can circulate; ⑥ To withdraw assets to $\mathcal{L}_{\mathcal{S}}$, and repeat the above steps.

Thus, it becomes evident that all verification mechanisms supporting light clients can be directly or indirectly applied to sidechains, a concept further explained in the Glimpse [91] protocol.

Open Issues of Sidechains. Sidechains enables the sharing of states between mainchain and sidechain, allowing users to securely lock tokens on one and utilize them on the other chain. This facilitates higher transaction frequency and faster instant transactions on the sidechain [183]. However, frequent token transfers between the mainchain and sidechain introduce additional security risks, particularly with regard to fraudulent transfers. This increases the complexity of interface design and may further lead to resource centralization among miners. In certain scenarios, cross-chain asset interoperability is typically achieved through the use of wrapped assets, wherein a trusted entity locks the original tokens and issues equivalent wrapped tokens for

use on the sidechain. However, this approach poses centralized trust risks, as the operation of wrapped tokens relies on a centralized authority. Moreover, wrapped tokens may face economic challenges due to the following reasons:

- *Value Parity.* The system must ensure that the value of the wrapped tokens remains consistent with the original tokens, as any deviation could lead to market instability.
- *Secure Custody.* The locked original assets must be securely held by the trusted entity. If the custodian fails, there is a risk of theft or loss of the assets.
- *Exchange Rate Stability.* The exchange rate between the wrapped tokens and the original tokens must remain stable over time; otherwise, users' trust in the wrapped tokens could be eroded.
- *Liquidity Pressure.* Users can redeem wrapped tokens at any time, which may create liquidity stress on the custodied asset pool. This risk is heightened during periods of market volatility or mass redemptions [184].

Moreover, ensuring the persistence and liveness of interactions between mainchains and sidechains in asynchronous network environments presents a significant challenge. In other words, it is essential to guarantee that valid asynchronous cross-chain transactions are executed correctly, eventually recorded on-chain, and confirmed by a sufficient number of subsequent blocks to achieve stability. This introduces new technical difficulties for sidechain construction [185]. For instance, key open challenges include designing cross-chain interaction models that remain robust under asynchronous conditions—especially for resource-constrained nodes with intermittent connectivity—and ensuring the ordering consistency of cross-chain transactions to prevent conflicts and state inconsistencies arising from out-of-order execution.

E. Chain Relay-based Swap Bridges

To overcome the limitations of the mainchain, some sidechain solutions have evolved into **chain relay** mechanism. Chain relay combines the strengths of notary schemes and sidechain solutions: on one hand, chain relay adopts the intermediary approach from notary

¹It is possible that $k_1 \neq k_2$ due to differing blockchain parameters, such as variations in block generation time or network synchrony.

mechanisms, allowing compatibility with diverse heterogeneous chains without modifying \mathcal{S} ; on the other, by using a third-party chain as an intermediary, chain relay can act as “sidechains” for multiple chains, thereby ensuring decentralization and trust in cross-chain processes.

Fundamentally, chain relay operates through a light client within a smart contract. Off-chain untrusted relayers continuously transfer block headers from \mathcal{S} to \mathcal{T} . To prevent malicious relayers from submitting invalid block headers, smart contracts ensure correct relay operations via two safeguards: ① internal verification of block headers through a partially replicated consensus mechanism of \mathcal{S} , and ② enhanced system stability through fork management.

The concept of relay chains originated with BTC Relay [55] and has been widely implemented in interoperability protocols. XCLAIM [186] leverages BTC Relay to achieve trustless atomic swaps between Bitcoin and Ethereum, introducing a cryptocurrency collateral mechanism to enable multi-party asset exchange and redemption requests. Westerkamp et al. [96] proposed zkRelay, which supports batch block header processing and uses zkSNARKs for on-chain and off-chain verification, ensuring fixed verification costs. Verilay [187], the first relay solution for PoS blockchains, deployed on Ethereum 2.0, validates the PoS protocol by generating final blocks and provides methods to retrieve validator public keys. Tesseract [114] employs a TEE as a relay to enable secure real-time cryptocurrency exchanges and support cross-chain transactions and asset tokenization.

Compared with sidechains. Some researchers [27], [28], [33] classify chain relay and sidechains together as the coordinating interoperable technologies due to their reliance on light client validation mechanisms. However, we assert that they have fundamental differences: *sidechains are homogeneous extensions of primary chains, while chain relay connects distinct chains (either homogeneous or heterogeneous) to facilitate asset transfer and message exchange.* See Tab. X for further differences.

TABLE X
PRIMARY DIFFERENCES BETWEEN SIDECHAINS AND CHAIN RELAY.

Benchmark	Sidechains	Chain Relay
Core Functionality	Extending Mainchain	Cross-Chain Transfer
Subordination Relationship	Sidechain Subordinate to the Mainchain	Chains Operate Independently
Processing Method	Synchronize Header	Block No Need to Synchronize Block Header
Transaction Speed	Relatively Fast	Relatively Slow
Security	Reliant on Mainchain	Based on Each Chain

Traditional classifications [33] also include distributed private key control, which enhances chain relay security by redundantly distributing private keys to verifiers. Although not an independent cross-chain approach, dis-

tributed private key control improves the security of notary and relay chain solutions.

Limitations. Chain relay enables validation of any transaction on \mathcal{S} , achieving partial decentralization and atomicity and defending against double-spending attacks, yet they remain vulnerable to MEV attacks and do not provide transaction privacy protection. Additionally, chain relay protocols are costly to operate, with limited cross-chain efficiency, particularly in terms of time. Overall, chain relay solutions have advantages in heterogeneity; however, only a few relay chains are currently operational, and significant node subsidies through incentive mechanisms are required.

F. Miscellaneous Interoperability Solutions

1) **Rollups:** Rollups [188] is a sidechains solution that batches processes transactions from a source chain and executes them on an external chain. It can be categorized into Optimistic Rollups (e.g., Arbitrum [189] and Optimism [190]) and Zero-Knowledge Rollups (e.g., ZkSync [191] and Loopring [192]), with each differing in trust model and proof mechanism.

- *Optimistic Rollups* [193] operate under the assumption that all transactions are valid, submitting results directly to the main chain. A “challenge period” mechanism is only triggered when a dispute arises, requiring fraud-proof submission. This model improves processing speed but may introduce delays in cross-chain environments due to the challenge period.
- *ZK-Rollups* [194] generate a ZK proof for each batch of transactions, ensuring data correctness and consistency when submitted to the main chain. ZK-Rollups hold a significant advantage in cross-chain operations, as their instant verification enhances the security and efficiency of cross-chain transfers.

Rollups can batch multiple transactions across chains into a single cross-chain operation, reducing fees and increasing data transmission efficiency. Additionally, Rollups’ proof generation inherently provides data consistency, minimizing the trust cost for asset migration across chains and reducing potential security risks during cross-chain interactions. Typically, Rollups are funded through native bridges (e.g., Polygon’s PoS bridge and zkEVM bridge) [195], which serve as Layer-2 onboarding pathways for technologies like Starkware [196] and ZkSync [191]. The latter enhances Layer-1 scalability by parallelizing instances of EVM circuit execution.

2) **Burn-and-Mint Style Protocol:** In the field of blockchain interoperability, the burn-to-claim protocol proposed by Pillai et al. [197], [198] is a notable burn-and-mint mechanism. This protocol facilitates cross-chain asset transfers through a two-step process: locking and burning the asset on \mathcal{S} , followed by minting an equivalent asset on \mathcal{T} .

The protocol effectively mitigates the risk of double-spending attacks, as assets are irreversibly burned before they are claimed on \mathcal{T} . Additionally, it preserves trustlessness, as no TTP is required to manage the transaction. However, the author does not provide proof of the protocol's inherent resistance to Maximal Extractable Value (MEV) attacks [197]. Malicious miners may exploit their control over transaction execution order within a block to gain an unfair advantage, which could undermine the fairness of asset exchange rates.

Limitations. While the Burn-to-Claim protocol facilitates cross-chain asset transfers, it exposes transaction details and involves a complex recovery process in the event of a failed transfer, meaning the atomicity of the protocol is not always guaranteed [199]. Moreover, current burn-and-mint designs often rely on APIs or centralized gateways, compromising the principles of decentralized trust and security.

3) **Hierarchical Blockchain:** A hierarchical architecture is a design approach that separates blockchain consensus tasks into multiple layers, aimed at enhancing the performance, scalability, and security of blockchain systems. However, this naturally creates interoperability requirements between the underlying and upper-layer blockchains.

Some protocols [11], [200]–[202] employ the underlying blockchain using consensus mechanisms like PoW or PoS to prevent double-spending attacks. After selecting a set number of nodes, these nodes undergo identity verification, followed by a chain consensus algorithm to generate an upper-layer blockchain. Other protocols [17], [203]–[205] select optimal leaders to serve as committee members for the upper-layer chain based on the underlying committee and reputation mechanisms, making these committees responsible for *CCI* tasks (e.g. based on 2PC [89], [206]).

Through coordination of high-level consensus, *CCI* between upper-layer and lower-layer blockchains can be more efficient, ensuring global consistency by sharing the underlying consensus. Additionally, state synchronization and information transmission between lower-layers are simplified and secured, preventing incompatibilities between different consensus protocols.

4) **Sharding:** Sharding [18] is a scalability technique designed to enable blockchain networks to process more transactions concurrently. The core idea of sharding is to partition nodes into smaller committees (shards, each maintaining a separate chain). Each shard manages a disjoint subset of the overall blockchain state, performing intra-shard consensus independently and processing different transactions in parallel. However, each shard still stores the entire state ledger. To optimize storage efficiency, the authors of OmniLedger [207] proposed *state sharding*, where each shard is responsible for storing and managing only a subset of the ledger data. Several other state-of-the-art state sharding protocols have since been introduced, including Monoxide [10], BrokerChain [208], and Pyramid [209].

State sharding is one of the most challenging aspects of implementing sharding. In the context of state sharding, verifying cross-shard transactions becomes particularly complex, as nodes in different shards store distinct portions of the ledger. Thus, mechanisms must be developed to facilitate the transfer of transactions or ledger state exchanges across shards [210]. Cross-shard transactions involve two or more shards, requiring coordination between them, which introduces the need for interoperability between different chains or ledgers. To handle cross-shard transactions, protocols such as OmniLedger [207], RapidChain [211], and ChainSpace [212] use 2PC protocol. Additionally, Monoxide [10] introduces a relay transaction mechanism to ensure the atomic finality of cross-shard transactions. In these mechanisms, the makespan of cross-shard transactions tends to be higher than that of intra-shard transactions. Furthermore, a high proportion of cross-shard transactions increases the complexity of the sharded blockchain system, potentially degrading system performance. Some of the latest research [213], [214] focuses on addressing these challenges.

V. REPRESENTATIVE PLATFORMS IN INDUSTRY

Interoperability platforms are technological frameworks designed to enable seamless collaboration among diverse applications, devices, and systems. In the industry, a primary function of interoperability platforms is their ability to support communication across different blockchain protocols and accommodate various data formats. Another key function is standardization. by adhering to industry standards and protocols, these platforms ensure reliability and trust in system interactions. Standards like SWIFT in banking [215], OPC UA in industrial big data, and HL7 standards in health IT [216] illustrate how interoperability platforms facilitate standardized communication across sectors.

Given that blockchain interoperability is a crucial practical aspect of the modern decentralized economy, numerous industry platforms provide such services. We present several notable platforms and categorize them broadly into two types: interoperability based on permissionless blockchains and based on permissioned blockchains. As described in Def. 2 and Def. 3, permissionless and permissioned blockchains serve different purposes and exhibit distinct characteristics, which in turn influence their interoperability requirements.

A. Interoperability for Permissionless Blockchains

Interoperability among permissionless blockchains typically focuses on the transfer of assets across networks. Mechanisms such as atomic swaps, relays, and sidechains enable the direct exchange of cryptocurrencies between different permissionless blockchains without the need for intermediaries. Below, we present an in-depth overview of several leading platforms, with a focus on their comparative analysis as shown in Tab. XI.

TABLE XI
ANALYSIS AND COMPARISON OF DIFFERENT PERMISSIONLESS BLOCKCHAIN INTEROPERABILITY PLATFORMS

Benchmark	Interledger	Polkadot	LayerZero	RSK	HyperService	Cosmos
Design Goal	Cross-ledger payment protocol	Multi-chain interoperability platform	Cross-chain messaging protocol	Bitcoin-based smart contract platform	Cross-chain programmability	Decentralized blockchain interoperability
Core Mechanism	Hash lock, escrow	Parachain, relay chain	Light client, oracle	Sidechain	HSL, cross-chain gateway	IBC, Hub-Zone architecture
Consensus Model	Depends on native ledger consensus	NPoS (Nominated PoS)	Native blockchain consensus	PoW (merged mining)	NSB-based coordination	Tendermint-BFT
Interoperation Method	Connector	XCMP protocol	Cross-chain messaging	Two-way peg lock	Gateway routing	Zone, IBC protocol
Main Use Cases	Cross-ledger payment, distributed payment gateway	Multi-chain dApps, DeFi interoperability	Cross-chain asset/NFT transfer	DeFi, cross-border payment, smart contracts	dApps, NFT transfer	Multi-chain DApps, DeFi, NFT cross-chain
Data Transfer Mechanism	ILP packet transfer	Parachain XCMP messaging	Packet-based payment transfer	Two-way peg escrow account	HyperBridge middleware	IBC cross-chain messaging
Cross-chain Capability	Strong (multi-ledger compatible)	Strong (multi-chain support)	Strong (supports major chains)	Weak (Bitcoin-focused)	Medium	Strong (Zone extensible)
Security Mechanism	Escrow + hash lock	Relay chain shared security	Relay + oracle dual validation	Merged with mining Bitcoin security	NSB-based	Tendermint + IBC verification
Execution Speed	Fast	Efficient	Efficient (packet optimized)	Slow	Fast	Fast
Native Token	None	DOT	None	R-BTC	HSP	ATOM
High-level Protocols	Supported (sharded payment, price query)	Extended via parachains	Supports multi-protocol interaction	EVM-compatible, supports Solidity	EVM/WASM-compatible	Supports IBC and smart contract calls

1) *Interledger*: Interledger protocol (ILP) [49] is one of the most classical notary-based interoperability platforms [50] based on Hash-locking. Its primary function is to facilitate the transfer of bundled payments across different payment networks or ledgers. ILP² creates a system that connects transacting parties, enabling two distinct systems to exchange currencies via third-party connectors³ without requiring mutual trust.

ILPv4, the simplified version⁴ of ILP, is optimized for routing numerous low-value data packets, commonly referred to as "penny swaps". This version can be integrated with any type of ledger, including those not originally designed for interoperability. Moreover, it is designed to function in conjunction with various higher-level protocols, which implement features ranging from quoting prices to sending larger sums using chunked payments. The precondition for implementing ILP is the concept of escrow. Escrow refers to a process where the sender creates an escrowed transaction, putting assets under conditional hold without transferring ownership. Custodial transactions are governed by preimage conditions, which permit any party with knowledge of the condition to confirm or revoke the transaction.

²<https://github.com/interledger>

³Connectors, which act as intermediaries forwarding ILP data packets between the sender and receiver, can generate revenue through currency conversion fees, subscription charges, or other mechanisms.

⁴<https://github.com/interledger/interledger.org-v4>

The sender may also impose a time lock, preventing any modification or deletion of the transaction during the lock period. Upon expiration of the time lock, the custodial transaction is automatically invalidated.



Fig. 19. Interledger Multi-Hop transaction schematic.

Let us use Fig. 19, along with a simple example, to illustrate the entire process [217] of an atomic transaction via ILP for detail (Scenario assuming one sender S , one receiver R and two connectors C_1, C_2): ① S and R agree on the hashlock H . The preimage P is only known to R ; ② Sender prepares the transfer to C_1 by creating and funding an HTLC on S with H ; ③ C_1 prepares a transfer to C_2 via their shared payment channel, also using H ; ④ C_2 prepares a transfer to R on their shared trustline using H ; ⑤ If R produces the preimage P before the transfer timeout, C_2 will "pay" R by increasing his balance on their trustline; ⑥ If C_2 sends P to C_1 before their transfer times out, C_1 will send a signed claim to pay C_2 ; ⑦ If C_1 submits P to S before the timeout, the transfer will be executed and S will receive the proof P that R was paid.

The protocol fundamentally relies on the formulation

of address rules for each account and the definition of a standardized cross-chain messaging format. Transactions are completed exclusively when consensus is reached among all participants. Connectors, functioning as trustless intermediaries, can be operated by any party with access to two or more ledgers, ensuring secure transaction execution.

2) *Cosmos*: The concept of Cosmos⁵ was first introduced by Jae Kwon in 2017 [23], [218], who is also the founder of Tendermint [9]. Kwon proposed two novel concepts in Cosmos: the Hub and the Zone. The Hub functions as a relay chain that handles cross-chain interactions, managing and coordinating communication between blockchains, while the Zones are parallel chains within the Cosmos ecosystem. Together, these Zones form a network of independent blockchains. The architecture of Cosmos is illustrated in Fig. 20.

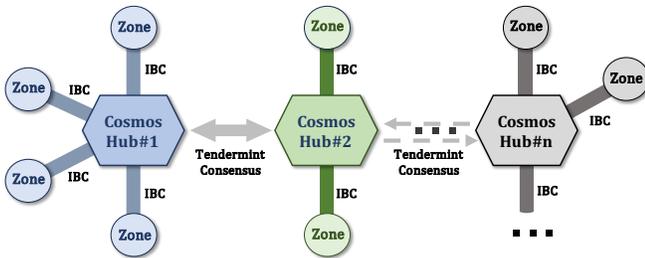


Fig. 20. Cosmos architecture.

To facilitate interoperability among parallel chains, Cosmos introduced the Inter-Blockchain Communication (IBC)⁶ protocol. This protocol supports the transfer of various digital assets, ranging from cryptocurrencies to non-fungible tokens (NFTs), as well as cross-chain smart contracts. The Cosmos SDK⁷, by default, utilizes the Tendermint consensus engine [85], a proof-of-stake consensus algorithm, to secure the network. Tendermint’s instant finality enables the transmission of state and data across multiple heterogeneous chains. The Cosmos Hub adopts a decentralized governance mechanism, where network participants can stake ATOM (the native token of the Cosmos Hub) to become consensus validators and earn rewards. The more ATOM staked, the greater the validator’s voting power.

Currently, Cosmos has several application cases, such as serving as a Layer-2 scaling solution for Ethereum. Previously, Ethereum employed the Casper consensus protocol [219] as a Layer-1 scaling solution, aiming to transition Ethereum to a proof-of-stake (PoS) consensus mechanism. Cosmos, in its design, also made Ethereum-compatible with the Ethereum Virtual Machine (EVM), and its underlying blockchain, which uses a PoS protocol called Tendermint, is referred to as Ethermint.

As the IBC protocol matures and more blockchains join the Cosmos ecosystem, Cosmos gradually realizes its vision of becoming the “Internet of Blockchains”. In

the future, Cosmos will further advance applications in DeFi, NFTs, DAOs, and other use cases, promoting the prosperity of the cross-chain ecosystem.

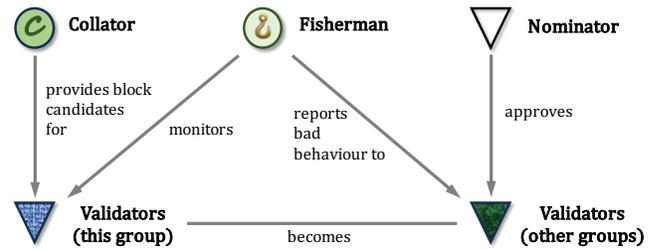


Fig. 21. Participating roles of Polkadot.

3) *Polkadot*: Polkadot [57], [220] is a relay-chain network platform⁸ based on interchain protocols, allowing multiple independent chains to run in parallel or connect to other chains, such as Ethereum, through bridging. Polkadot categorizes the nodes in its network into four roles: Collator, Fisherman, Nominator, and Validator on the relay chain. The relationships among these roles are illustrated in Fig. 21 and the functions of each role can be expressed as:

- *Collator* maintains a “full node” of a parallel chain, storing all essential information of the parallel chain and enabling transactions with other nodes on the chain. The primary task of the collator is to organize and execute on-chain transactions and submit them, along with ZK proofs, to the responsible Validators.
- *Validators* deploy the relay chain client, validating blocks submitted by collators, approving blocks produced by parallel chains, and executing the relay chain’s consensus before packaging blocks onto the chain.
- *Nominators* represent a group with staking interests. Their main responsibility is to select trustworthy validators and stake their assets with these validators. Validators are elected by nominators. By staking their assets, nominators trust the elected validators to maintain the network, and they receive rewards or penalties proportionate to those of the validators.
- *Fishermen* do not participate in block production on the relay or parallel chains. Their role is to monitor and report any malicious behavior by the other participants, earning a one-time reward for successful detection.

In the Polkadot network, cross-chain transactions are facilitated by a queuing mechanism, where the Merkle tree structure plays a critical role in ensuring data integrity. Transactions are routed from the exit queue of \mathcal{S} , through the relay chain, and into the entry queue of \mathcal{T} , with the relay chain maintaining records of the relayed transactions. The relay chain manages the queues and guarantees the atomicity of transactions. If any issues

⁵<https://github.com/cosmos/cosmos>

⁶<https://github.com/cosmos/ibc-go>

⁷<https://github.com/cosmos/cosmos-sdk>

⁸<https://polkadot.com/>; <https://wiki.polkadot.network/docs/build-guide>; <https://wiki.polkadot.network/docs/learn-bridges>

arise at any point in the process, the entire transaction is invalidated, and the relay chain assumes responsibility for validating and executing the transaction. When a cross-chain transaction is needed, \mathcal{S} places the cross-chain transaction in its output queue alongside other transactions. The collator of \mathcal{S} identifies the cross-chain transaction, packages it, and sends it to the validators, with Fishermen monitoring its legitimacy. Once validated, the cross-chain transaction is placed into the input queue of \mathcal{T} and referenced in the relay chain. Finally, \mathcal{T} executes the transactions in its input queue.

A key distinction between Cosmos and Polkadot pertains to the sovereignty of parallel chains, which varies significantly between the two network architectures. In Cosmos, parallel chains maintain autonomy in consensus, whereas Polkadot requires parallel chains to achieve global consensus through the relay chain to ensure shared security.

4) **HyperService**: HyperService⁹ [221] is the first platform designed to build and execute programmable dApps on heterogeneous blockchains. From a macro perspective, HyperService is built upon two key innovations: a programming framework for developers to write cross-chain dApps and a cryptographic protocol for securely implementing these dApps on blockchain networks. The programming framework introduces the Unified State Model (USM), a blockchain-agnostic and scalable model designed to describe cross-chain dApps. Additionally, HyperService introduces HSL, a high-level programming language tailored to the USM model for writing cross-chain dApps. These dApps, written in HSL, are then compiled into HyperService executable files and executed by the underlying cryptographic protocol.

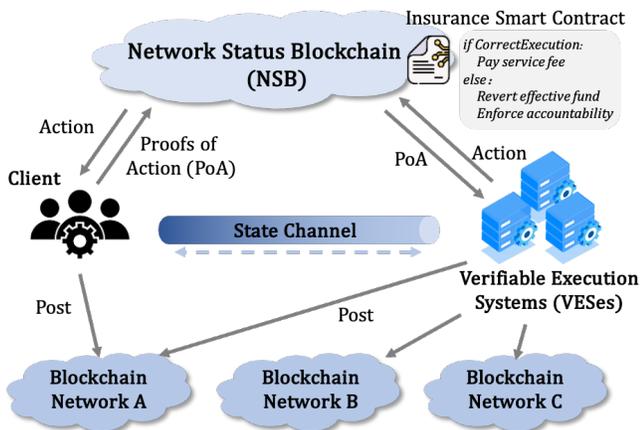


Fig. 22. The architecture of HyperService.

As shown in Fig. 22, the HyperService architecture comprises three main components:

- **Verifiable Execution Systems (VESes)**: Conceptually acting as a blockchain driver, the VESes compile

⁹<https://github.com/HyperService-Consortium>

high-level dApp programs provided by the client into executable blockchain transactions, which are runtime executables on HyperService.

- **Network State Blockchain (NSB)**: Designed as a “blockchain of blockchain”, the NSB offers an objective and unified view of the dApp’s execution state.
- **Insurance Smart Contract (ISC)**: ISC arbitrates the correctness or violations of dApp executions, based on information provided by the NSB, without relying on trust. In cases of anomalies, the ISC rolls back all executed transactions, ensuring financial atomicity and holding malicious actors accountable.

HyperService introduces a groundbreaking paradigm for interoperability, streamlining the complexities of dApp development while ensuring atomicity and consistency in cross-chain operations within a secure, trustless environment. This platform holds profound significance for the future of blockchain applications, particularly in DeFi and cross-chain smart contract execution, where it paves the way for more seamless and secure interactions across diverse blockchain ecosystems.

5) **LayerZero**: LayerZero¹⁰ [63], [222] is a decentralized cross-chain communication protocol that facilitates data transfer through endpoints on the source and target chains, along with an off-chain infrastructure consisting of oracles and relayers, as illustrated in Fig. 23. This architecture allows LayerZero to transmit messages and state information, making it an efficient cross-chain bridging solution.

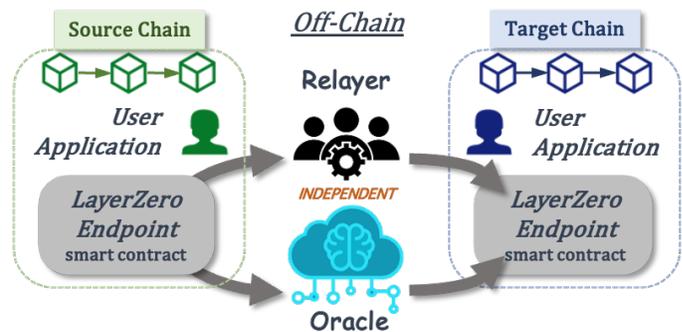


Fig. 23. LayerZero upholds the integrity of *CCI* by mandating the corroboration of each transaction by two distinct entities *Oracle* and *Relayer*, ensuring its validity.

- **Endpoints**: These are the foundational components of LayerZero on the blockchain, responsible for transmitting messages between different chains. They manage the reception and dispatch of on-chain data, ensuring that on-chain activities can seamlessly interact with the off-chain transmission mechanisms.
- **Oracle and Relayer**: The distinctive aspect of LayerZero lies in its use of two independent off-chain roles to achieve state synchronization. The oracle is tasked with retrieving data from \mathcal{S} and transmitting it to \mathcal{T} , while the relayer is responsible for verifying

¹⁰<https://github.com/layerzero-Labs>

the data's validity. This design separates data acquisition from verification, enhancing the protocol's security.

Unlike trust-minimized native verification protocols, such as Polkadot's XCMP and Cosmos' IBC, LayerZero adopts a novel trust assumption: the oracle and re-layer are assumed not to collude. This design increases the flexibility and efficiency of cross-chain communication, allowing developers to select a security model that balances trust assumptions with performance costs. However, it also implies a partial reliance on external verification, somewhat undermining the system's trust-minimization properties.

LayerZero's trust model involves a partial reliance on the relayer, as it employs an implicit, on-demand state synchronization mechanism rather than the traditional explicit block header synchronization. While implicit synchronization is less costly, it necessitates a trade-off between trust and performance. By default, Chainlink is chosen as the oracle provider, with LayerZero itself serving as the relayer provider. Although these services can be substituted with user-defined solutions, the system inherently relies to some extent on social trust. Despite the associated trust risks, LayerZero's flexibility and efficiency present significant potential for applications in *CCI*.

6) **RSK**: RSK¹¹ (Rootstock) [223] is a sidechain platform enabling Bitcoin blockchain interoperability through a two-way peg mechanism. Its goal is to expand Bitcoin's functionality to support smart contracts and dApps. RSK achieves these objectives through key technologies such as smart contracts, the two-way peg, and merged mining.

One of RSK's core features is its smart contract capability. RSK is compatible with the Ethereum Virtual Machine (EVM), allowing developers to use Ethereum's development tools (such as the Solidity programming language) to build and deploy smart contracts on the RSK platform. This compatibility enables Ethereum applications and smart contracts to be ported to RSK, thereby expanding Bitcoin's use cases.

A crucial technology behind RSK is merged mining, a concept first referenced in the well-known sharding consensus system Monoxide [10]. Merged mining¹² allows miners to utilize their computational power to secure both the Bitcoin and RSK networks by publishing blocks on RSK and earning additional fees with minimal extra cost. This process aligns RSK with the Bitcoin network, ensuring that RSK inherits the security of Bitcoin's computational power.

When users wish to transfer Bitcoin to RSK, they send BTC to a special multi-signature address, where the BTC is locked on the Bitcoin. In return, an equivalent amount of RBTC is generated on RSK. Users can then use RBTC for transactions or to execute smart contracts

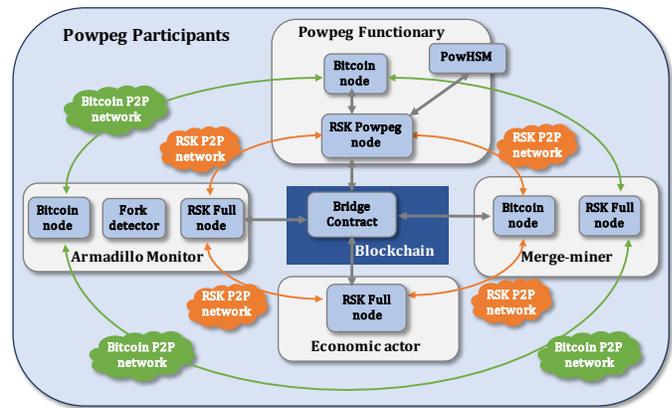


Fig. 24. RSK architecture.

on RSK. When users want to convert RBTC back into Bitcoin, they can destroy the RBTC through the two-way peg mechanism, and the corresponding BTC will be unlocked from the multi-signature address on the Bitcoin mainchain. To ensure the security of this process, RSK employs three key components: the Bridge smart contract, Pegnetories, and the Armadillo monitor. Fig. 24 illustrates the different components of the RSK architecture.

Despite offering smart contract functionality similar to Ethereum, RSK's ecosystem remains relatively small and faces strong competition from platforms such as Ethereum [167], Polkadot [57], and Cosmos [23]. Additionally, the incentive structure for merge mining must be sufficiently attractive to miners, as inadequate participation could compromise the security of the RSK network.

B. Interoperability for Permissioned Blockchain

Permissioned blockchains restrict access to specific participants and are often utilized by enterprises for internal operations. These blockchains are designed to provide enhanced control, privacy, and efficiency. The interoperability of which primarily emphasizes the integration of various enterprise systems and applications. By implementing standardized protocols and data formats, different permissioned blockchains can effectively understand and process data seamlessly.

Cactus¹³ [224] is an open-source *CCI* platform designed to streamline communication between enterprise blockchains. Utilizing a flexible plugin-based architecture, it enables custom connectors for specific blockchain networks. Cactus interacts with different blockchains through "ledger connectors" and "validators", ensuring secure and consistent data transfer. It supports multiple consensus algorithms and multi-signature mechanisms, enhancing cross-chain security. The platform's modular design facilitates seamless integration with diverse permissioned blockchain systems.

¹¹<https://rootstock.io/>

¹²<https://github.com/rsksmart>

¹³<https://github.com/opentaps/cactus>

WeCross¹⁴ [225], developed by WeBank, is an open-source cross-chain platform focused on efficient interoperability between consortium blockchains. It employs a four-component architecture (Zone, Router, Stub, and Resource) to manage flexible cross-chain connections and data exchange. WeCross supports 2PC and HTLC to ensure atomic and irreversible cross-chain transactions. The platform is compatible with major consortium blockchains like Hyperledger Fabric [8] and FISCO BCOS [226], enabling asset swaps and data access control. Using a smart contract-based framework, WeCross ensures transparency and security in cross-chain operations.

FireFly¹⁵ [227] is a blockchain interoperability platform tailored for enterprise use, focusing on the integration of both on-chain and off-chain data. Utilizing a microservices architecture, it creates a modular and scalable ecosystem that simplifies the management of smart contracts, digital assets, and external data sources. Unlike Cactus, FireFly emphasizes application development, offering a comprehensive software development kit for building DApps across multiple blockchains.

Weaver¹⁶ [228], an open-source project under Hyperledger Labs, provides a *CCI* framework without relying on trusted intermediaries. It utilizes a “relay” and “driver” architecture, coordinated through smart contracts to synchronize states across blockchains. Weaver prioritizes compatibility with existing blockchain systems, avoiding modifications to underlying protocols, and employs a decentralized identity platform to protect user privacy and security. The platform supports cross-chain data sharing, asset transfers, and state validation, making it suitable for multi-permissioned blockchain environments.

Cacti¹⁷ [229] is a versatile interoperability platform that leverages the advanced technical capabilities of Cactus [224] and Weaver [228], a project from Hyperledger Labs. It offers a seamless integration path for users of both platforms. Unlike traditional approaches, Cacti does not force separate blockchain networks to merge into a single overarching chain. Nor does it require the creation of a new settlement chain or consensus protocol that other networks must adopt. Instead, Cacti enables independent networks to retain their decision-making autonomy while facilitating cross-network transactions as needed.

VI. PROSPECTIVE AND INTERSECTING FIELD RESEARCH AVENUES

In this section, we analyze several prospective and intersecting field research approaches to offer scholars new perspectives in cross-disciplinary areas.

¹⁴<https://github.com/WeBankBlockchain/WeCross>

¹⁵<https://github.com/hyperledger/firefly>

¹⁶<https://github.com/hyperledger-labs/weaver-dlt-interoperability>

¹⁷<https://github.com/hyperledger-cacti/cacti>

A. Redactable Blockchain with Interoperability

The concept of redactable blockchain was initially proposed by Giuseppe et al. [230], with the aim of enabling controlled modifications to on-chain data, effectively overcoming the limitations of blockchain’s immutability and providing a more flexible data storage paradigm. This includes scenarios such as removing inappropriate content, enhancing storage scalability, and complying with the “right to be forgotten” laws [231]. These solutions target issues like deleting illicit content for digital currency like Bitcoin [232], revising vulnerable smart contracts and on-chain states for Ethereum [233], and editing on-chain data for the permissioned blockchain platform [234].

However, existing redactable blockchain proposals remain underdeveloped, with most efforts focusing on designing redaction policies for individual chains. These approaches face limitations when applied in *multi-chain* environments. In particular, when dealing with rewriting across multiple heterogeneous or homogeneous blockchains, identifying and redacting relevant transactions becomes a critical challenge. If a cross-chain transaction is modified, the on-chain states of different blockchains are interdependent, meaning that rewriting a specific block or transaction in one blockchain may have direct or indirect impacts on the states of others. Consequently, the corresponding on-chain states must be redacted accordingly to maintain data consistency across blockchains. Failure to do so could lead to inconsistencies in dApps that span multiple chains, posing challenges in maintaining redaction consistency.

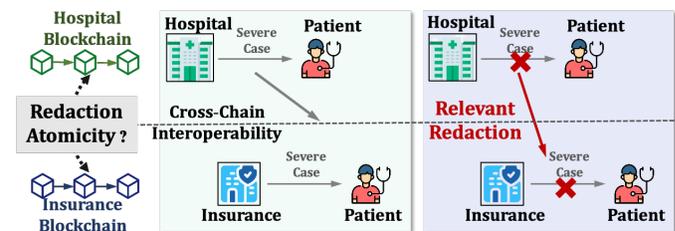


Fig. 25. A linkage scene: Redaction cross two different blockchains.

A Linkage Scene. To illustrate the practical significance of combining redactable blockchain and *CCI*, consider the following scenario involving two independent blockchains, as shown in Fig. 25: one manages medical records, while the other handles health insurance services. The hospital blockchain specializes in managing patient health records and treatment data, while the insurance blockchain deals with policy applications, claims, and related transactions. Suppose a physician in a medical institution incorrectly diagnoses a patient with a severe illness and uploads the erroneous information to the medical records blockchain. However, the physician fails to detect and correct the error in time. Subsequently, the patient submits an application for high-risk insurance coverage and compensation to

the insurance blockchain based on the faulty medical records. Since the insurance system relies on data from the hospital blockchain, the policy and payout are approved. Without the support of redactable blockchain and interoperability technology, both the misdiagnosis record and erroneous insurance application would be permanently stored on both blockchains. This could lead to data bloat, impact the patient’s future medical and insurance records, and potentially cause financial losses for the insurance company. Therefore, an appropriate cross-chain rewriting method is needed to remove the erroneous record from the hospital blockchain, followed by rewriting the related transactions on the insurance blockchain to synchronize the correction.

Another crucial consideration is maintaining atomicity during cross-chain redaction. If a transaction on a specific chain is fully redacted, resulting in a state change, any cross-chain transactions dependent on the previous state must be rewritten accordingly. Alternatively, if rewriting these cross-chain transactions is not possible, the states associated with the redacted transaction must be reverted. Ensuring atomic redaction presents a significant challenge.

Research in this area remains limited [235], [236]. Although Hu et al. [235] proposed the LvyRedaction, which can achieve atomicity and consistency in cross-chain editing, it requires middleware support and is limited to permissioned blockchains. In the future, a unified and robust solution will be essential to support the editing of transactions across different blockchains. This solution must include mechanisms for monitoring editing transactions, generating editing suggestions, and verifying editing proposals to ensure the atomicity, consistency, and auditability of the redaction and interoperability processes.

B. Asynchronous Consensus with Interoperability

Most current cross-chain technologies are based on network time assumptions to achieve *global time*¹⁸ synchronization. Synchronous networks rely on the assumption that all messages are received within a specified time limit, denoted as Δ , whereas partially synchronous networks function without a time constraint until a Global Stabilization Time (GST) event occurs, after which messages must be received within Δ [207]. However, these time-based assumptions lack robustness. As blockchain systems scale up, the workload for consensus increases, potentially preventing nodes from reaching global consistency. In addition, it may also destabilize the entire cross-chain system, ultimately leading to protocol failures.

To address these challenges, there is a need to explore interoperability technologies [237], [238] that adopt asynchronous consensus. Sidechains, relay chains, and sharding depend on their respective consensus mechanisms,

while the advantage of asynchronous consensus is that it does not rely on network performance for its protocol design. In 2001, Cachin et al. [239] introduced the first asynchronous Byzantine atomic broadcast protocol, CKPS01. In 2016, Miller et al. [240] presented the first practically applicable asynchronous consensus protocol for blockchain environments—HoneyBadgerBFT. BEAT [241] employs a modular design to reduce consensus latency and improve throughput. Dumbo [242] is the first fully practical asynchronous BFT consensus protocol, which enhances HoneyBadger using provably reliable broadcast and multi-value Byzantine agreement.

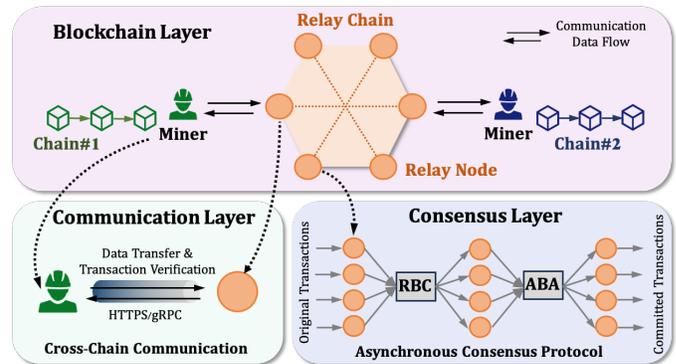


Fig. 26. Potential case: an interoperability framework based on asynchronous consensus.

As illustrated in Fig. 26, we propose a universal cross-chain framework based on asynchronous consensus and relay chain, with asynchronous consensus as the core component. Future research will focus on extending this framework to more protocols, incorporating asynchronous consensus theory and structure into cross-chain technology to further enhance system interoperability and scalability.

C. Growing Web3 & Metaverses Through Interoperability

The underlying data storage of the metaverse and web3 relies on blockchain technology, and its development is intrinsically linked to interoperability [243]. This involves connecting different virtual worlds and allowing users to move seamlessly between them while maintaining ownership and functionality of digital assets. In the metaverse, interoperability means that users can transfer their digital identity, assets, and experiences across various virtual platforms without losing functionality or ownership [244].

To achieve cross-metaverse interoperability, two fundamental components [6] must be seamlessly connected:

- *Identity*. In the metaverse, identity establishes the uniqueness of users and digital assets and is fundamental for linking user behaviors with assets. To enable interoperability, standardized identity markers are needed across different metaverses, encompassing user identities, assets, currencies, items, and their transfers. Although users may create multiple identities across various metaverses, each identity

¹⁸The state evolution of two distinct blockchains may progress at different *time* intervals. So a clock θ maps a given epoch on any ledger to the time on a global [30] synchronized clock $\theta : s \rightarrow t$.

should be managed independently, similar to maintaining separate accounts on different social media platforms to safeguard privacy and retain control.

- *Objects.* Objects in the metaverse include digital assets, avatars, and interactive entities, each characterized by unique attributes such as gender, material, rendering effects, and functionality. These attributes can be generated through technologies like 3D and digital twins (DT) scanning or created directly by users. To support interoperability, objects with the same identity should maintain consistent attributes across metaverses, ensuring a seamless user experience and facilitating functionality and interaction across diverse environments.

Based on this foundation, a set of universal standards needs to be established to regulate cross-platform asset, identity, and data handling. Currently, various platforms use proprietary formats for data storage, leading to assets in one environment often being incompatible with others. Therefore, establishing universal standards will enhance asset compatibility between different virtual spaces.

- *Token Standards.* Standards such as ERC-721 [90] and ERC-1155 [245] lay the groundwork for the transfer and recognition of NFTs across different platforms. These standards allow digital assets to be recognized and utilized across multiple dApps within the same blockchain network, thus enhancing interoperability.
- *Cross-Platform Protocols.* There is a need to develop cross-platform protocols to define the methods of data exchange between different virtual environments. This may include standardized avatar formats, item specifications, and transaction mechanisms to ensure assets maintain consistent appearances and functionalities across various virtual worlds, providing users with a seamless experience.

Enhancing blockchain interoperability is fundamental to achieving interconnectedness in the metaverse, as it provides a decentralized and secure foundation for asset transfers, identity verification, and data exchange between virtual environments. By establishing standardized blockchain protocols, various metaverse platforms can facilitate interoperability, enabling users to freely access and trade digital assets. This capability fosters richer and more coherent experiences, ultimately contributing to a more integrated metaverse ecosystem. Through robust interoperability mechanisms, users can seamlessly navigate different virtual worlds while retaining ownership and functionality of their digital assets.

VII. CURRENT CHALLENGES

The blockchain field faces numerous persistent challenges. Based on a review of interoperability literature from 2023 onward [12], [28], [29], [36], [78], these challenges can be broadly categorized into four main areas: infrastructure, security, privacy, and scalability. We

summarize these categories in Tab. XII and provide a detailed breakdown of specific challenges within each category. Certain challenges, such as privacy protection in asset swaps and the prevention of double-spending, have been relatively well-addressed through existing technologies. However, issues like script compatibility, network interconnectivity, and architectural compatibility remain in the early stages of research and exploration, requiring further technological advancements. Building on this categorization, we analyze current interoperability challenges from three broader perspectives: trustlessness, regulatory compliance, and knowledge frameworks. This broader analysis offers a multi-dimensional perspective on the challenges of interoperability. For a deeper understanding of specific challenges in privacy and security, readers are encouraged to consult [12].

A. Trust Model Discrepancies

Blockchain networks generally function on varying trust models and security protocols. Bridging the differences in trust models across networks while preserving security and decentralization is a challenging task. Achieving this requires a thoughtful approach to consensus mechanisms, cryptographic methods, governance structures, etc. Trustless cross-chain transactions aim to minimize dependence on third-party verifiers or intermediaries, typically employing mechanisms such as state channels [246] and hash-locked transfers [247]. These technologies require precise design and rigorous testing to ensure secure asset transfers across different blockchains without introducing vulnerabilities.

B. Regulatory Concerns

Blockchain interoperability encounters considerable regulatory and legal obstacles, especially in the context of cross-border transactions and data sharing. Issues such as regulatory ambiguity, compliance demands, and jurisdictional challenges can impede the widespread adoption of *CCI* solutions. Collaboration between industry participants, policymakers, and regulatory authorities is essential for creating well-defined frameworks and standards. For instance, data privacy regulations vary by region, such as the EU's General Data Protection Regulation (GDPR) [248] and the California Consumer Privacy Act (CCPA) [249] in the U.S., making compliance in cross-chain data sharing highly complex. Non-compliance with data privacy laws can lead to severe legal and financial repercussions. Another challenge involves jurisdiction: as data and transactions flow across blockchain networks in different countries, determining the applicable legal framework is not straightforward. Blockchain's decentralized nature further complicates this issue, as pinpointing the exact location of data and transactions is difficult. Many regulators are still exploring blockchain regulations, and the lack of clarity makes

TABLE XII
KEY CHALLENGES HIGHLIGHTED IN INTEROPERABILITY REVIEWS SINCE 2023

Category	Challenge	Description	Progress	Reference
Infrastructure	Interoperable Architecture	e.g., Universal Modules, Booting Approaches, etc.	►	[28]
	Scripting Language	Need for Simpler and More Compatible Scripting Languages	►	[29]
	Cryptographic Primitives	e.g. Cryptographic Sources Used in Adapter Signatures	►	[28], [29], [78]
	Network Compatibility	e.g. More Universal API, Heterogeneous Networks in Sidechains	○	[78]
Security	Monitoring	Enhanced Compliance and Legality Standards	►	[12], [78]
	Trustless	Reliability in Synchronous Modes that Do Not Rely on TTP	►	[29], [36]
	Double-Spending Attack	Involve the Reliability of Consensus in \mathcal{S} or \mathcal{T}	●	[29]
	Smart Contract Security	Contract Vulnerability Remediation, Governance, and Upgrades	►	[12], [28], [29], [36]
Privacy	Asset Swaps	Non-Distinguishability and Non-Linkability	●	[12], [78]
	Asset Transfers	Anonymity and Confidentiality	►	[12], [78]
	Data Transfers	Unbreakability of Ciphertext and Security of Key Agreement	○	[12], [78]
	Heterogeneous Systems	Unlinkability and Anonymity Across Different Ledgers	○	[29]
Scalability	Sharding	e.g. Coordinating State Sharding, Reducing Attacks on one Shard	●	[28]
	Layer-2: Rollups	Complex Contracts and Inefficiency of ZK Proofs	►	[36]

★ *Symbol.* ● - mostly addressed; ► - partially addressed; ○ - unresolved or insufficiently addressed.

it challenging for organizations to develop compliant interoperability solutions. Additionally, intellectual property and patent issues may pose regulatory obstacles, as proprietary technologies and protocols on various blockchain platforms are often protected by intellectual property rights. Developing interoperability solutions that respect these rights requires careful consideration and substantial legal expertise.

C. Fragmentation of Interoperability Knowledge Framework

The current study presents a preliminary knowledge framework for blockchain interoperability, highlighting that this field remains relatively fragmented, even within specific applications or technologies (e.g., sidechains). Several studies have noted a lack of systematic information regarding types of interoperability, and the definition of interoperability itself is still debated [27]–[29]. No consensus has yet been reached on models and frameworks for interoperability—both conceptual models and cross-chain asset management models—particularly regarding their specific content and practical applicability. As discussed in Sect. IV, there is currently no optimal categorization that unifies all blockchain interoperability technologies. Future research could aim to systematize knowledge on blockchain interoperability by adopting approaches inspired by frameworks like SEBOK (Systems Engineering Body of Knowledge) [250]. Such frameworks could standardize general definitions of interoperability types, delineate their interrelationships, and specify the essential components of blockchain interoperability models and frameworks.

VIII. CONCLUSION AND FUTURE OUTLOOK

In this paper, we conducted a comprehensive literature review on blockchain interoperability. By analyzing over one hundred relevant documents, we identified and

categorized more than ten types of technologies, aiming to address the gaps in existing research concerning technical classification and interdisciplinary studies. We anticipate that this research will alleviate the burden for newcomers in the field and provide valuable insights for interdisciplinary researchers.

Looking ahead, as more scholars and organizations acknowledge the significance of interoperability, there is a growing trend in increasing research and development investment. Joint efforts from industry alliances and academic institutions will be essential in driving forward the development of *CCI* standards and solutions. Furthermore, the integration of emerging technologies such as IoT, neural networks [251], 6G [252], the metaverse [6], and AI [5] with blockchain interoperability holds promising potential for new application scenarios. For instance, AI algorithms can optimize cross-chain transactions, while IoT devices can securely exchange data and automate processes through interoperable blockchains. Overall, the future of blockchain interoperability is highly promising, with the potential to transform interactions and collaborations within blockchain networks. In spite of all these difficulties, continued innovation and collaboration in the blockchain community are anticipated to propel the development of robust *CCI* solutions. By addressing concerns related to standardization, security, privacy, scalability, and compliance, the blockchain ecosystem can pave the way for new growth and innovation opportunities, ultimately realizing a decentralized future of interconnected devices.

REFERENCES

- [1] S. Nakamoto and A. Bitcoin, “A peer-to-peer electronic cash system,” *Bitcoin*.—URL: <https://bitcoin.org/bitcoin.pdf>, vol. 4, no. 2, p. 15, 2008.
- [2] H. Wu, Q. Yao, Z. Liu, B. Huang, Y. Zhuang, H. Tang, and E. Liu, “Blockchain for finance: A survey,” *IET Blockchain*, 2024.

- [3] X. Wang, H. Zhu, Z. Ning, L. Guo, and Y. Zhang, "Blockchain intelligence for internet of vehicles: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, 2023.
- [4] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," *IEEE communications surveys & tutorials*, vol. 25, no. 1, pp. 386–424, 2022.
- [5] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6g wireless communications," *IEEE Communications Surveys & Tutorials*, 2023.
- [6] T. Li, C. Yang, Q. Yang, S. Lan, S. Zhou, X. Luo, H. Huang, and Z. Zheng, "Metaopera: A cross-metaverse interoperability protocol," *IEEE Wireless Communications*, vol. 30, no. 5, pp. 136–143, 2023.
- [7] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.
- [8] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.
- [9] J. Kwon, "Tendermint: Consensus without mining," *Draft v. 0.6, fall*, vol. 1, no. 11, pp. 1–11, 2014.
- [10] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *16th USENIX symposium on networked systems design and implementation (NSDI 19)*, 2019, pp. 95–112.
- [11] R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," *Cryptology ePrint Archive*, 2016.
- [12] A. Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang, and T. Hardjono, "Sok: Security and privacy of blockchain interoperability [extended version]," *Authorea Preprints*, 2024.
- [13] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.
- [14] J. B. Klamti and M. A. Hasan, "Post-quantum two-party adaptor signature based on coding theory," *Cryptography*, vol. 6, no. 1, p. 6, 2022.
- [15] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, "zkbridge: Trustless cross-chain bridges made practical," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3003–3017.
- [16] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," URL: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>, vol. 72, pp. 201–224, 2014.
- [17] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2020.
- [18] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 17–30.
- [19] A. Adams, "Layer 2 be or layer not 2 be: Scaling on uniswap v3," *arXiv preprint arXiv:2403.09494*, 2024.
- [20] I. K. Nassr, E. Kostika, and A. Melachrinou, "Concentration of defi's liquidity: Evidence from decentralised exchanges (dexs) and automated market makers (amms)," 2024.
- [21] J. A. Berg, R. Fritsch, L. Heimbach, and R. Wattenhofer, "An empirical study of market inefficiencies in uniswap and sushiswap," in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 238–249.
- [22] S. Agrawal, D. Zindros, D. Karakostas, and A. Tzinas, "Grant proposal: An ethereum light client on axelar," 2023.
- [23] J. Kwon and E. Buchman, "Cosmos whitepaper," *A Netw. Distrib. Ledgers*, vol. 27, pp. 1–32, 2019.
- [24] Q. Wei, X. Zhao, X.-Y. Zhu, and W. Zhang, "Formal analysis of ibc protocol," in *2023 IEEE 31st International Conference on Network Protocols (ICNP)*. IEEE, 2023, pp. 1–11.
- [25] "Coinmarketcap." [Online]. Available: <https://coinmarketcap.com/>
- [26] "Research nester for blockchain interoperability market." [Online]. Available: <https://www.researchnester.com/reports/blockchain-interoperability-market/5868>
- [27] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *Acm Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.
- [28] G. Wang, Q. Wang, and S. Chen, "Exploring blockchains interoperability: A systematic survey," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–38, 2023.
- [29] K. Ren, N.-M. Ho, D. Loghin, T.-T. Nguyen, B. C. Ooi, Q.-T. Ta, and F. Zhu, "Interoperability in blockchain: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 12, pp. 12750–12769, 2023.
- [30] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, "Sok: Communication across distributed ledgers," in *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25*. Springer, 2021, pp. 3–36.
- [31] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervasive and Mobile Computing*, vol. 59, p. 101079, 2019.
- [32] R. Bhatia *et al.*, "Interoperability solutions for blockchain," in *2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE)*. IEEE, 2020, pp. 381–385.
- [33] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, and W. Han, "An overview on cross-chain: Mechanism, platforms, challenges and advances," *Computer Networks*, vol. 218, p. 109378, 2022.
- [34] S. D. Kotey, E. T. Tchao, A.-R. Ahmed, A. S. Agbemenu, H. Nunoo-Mensah, A. Sikora, D. Welte, and E. Keelson, "Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication," *IET Communications*, vol. 17, no. 8, pp. 891–914, 2023.
- [35] Y. Zhou, Y. Bai, Z. Liu, H. Gao, C. Liu, and H. Lei, "Exploring cross-chain mechanisms and projects in blockchain: A comprehensive summary," in *International Conference on Computer Engineering and Networks*. Springer, 2023, pp. 421–431.
- [36] N. Li, M. Qi, Z. Xu, X. Zhu, W. Zhou, S. Wen, and Y. Xiang, "Blockchain cross-chain bridge security: Challenges, solutions, and future outlook," *Distributed Ledger Technologies: Research and Practice*, 2024.
- [37] G. LaVeau, "Interoperability in defense communications," *IEEE transactions on communications*, vol. 28, no. 9, pp. 1445–1455, 1980.
- [38] P. Wegner, "Interoperability," *ACM Computing Surveys (CSUR)*, vol. 28, no. 1, pp. 285–287, 1996.
- [39] J. Postel, "Rfc0793: Transmission control protocol," 1981.
- [40] H. Zimmermann, "Osi reference model-the iso model of architecture for open systems interconnection," *IEEE Transactions on communications*, vol. 28, no. 4, pp. 425–432, 1980.
- [41] F. P. Coyle, *XML, Web services, and the data revolution*. Addison-Wesley Professional, 2002.
- [42] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The characteristics of cloud computing," in *2010 39th International Conference on Parallel Processing Workshops*. IEEE, 2010, pp. 275–279.
- [43] T. O'reilly, *What is web 2.0*. O'Reilly Media, Inc., 2009.
- [44] A. Park, M. Wilson, K. Robson, D. Demetis, and J. Kietzmann, "Interoperability: Our exciting and terrifying web3 future," *Business Horizons*, vol. 66, no. 4, pp. 529–541, 2023.
- [45] J. Zhu, F. Li, and J. Chen, "A survey of blockchain, artificial intelligence, and edge computing for web 3.0," *Computer Science Review*, vol. 54, p. 100667, 2024.
- [46] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1020–1047, 2021.
- [47] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE international conference on software quality, reliability and security companion (QRS-C)*. IEEE, 2018, pp. 139–145.
- [48] W. Liu, B. Cao, M. Peng, and B. Li, "Distributed and parallel blockchain: Towards a multi-chain system with enhanced security," *IEEE Transactions on Dependable and Secure Computing*, 2024.
- [49] "Interledger protocol." [Online]. Available: <https://interledger.org/developers/>
- [50] A. Hope-Bailie and S. Thomas, "Interledger: Creating a standard for payments," in *Proceedings of the 25th international conference companion on world wide web*, 2016, pp. 281–282.

- [51] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenger, "Ripple: Overview and outlook," in *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings 8*. Springer, 2015, pp. 163–180.
- [52] T. Nolan, "Alt chains and atomic transfers," in *Bitcoin Forum*, 2013.
- [53] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," URL: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>, vol. 72, pp. 201–224, 2014.
- [54] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Stabilization, Safety, and Security of Distributed Systems: 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings 17*. Springer, 2015, pp. 3–18.
- [55] "Btcrelay reference implementation," 2017. [Online]. Available: <https://www.github.com/ethereum/btcrelay>
- [56] V. Buterin, "Chain interoperability," *R3 research paper*, vol. 9, pp. 1–25, 2016.
- [57] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White paper*, vol. 21, no. 2327, p. 4662, 2016.
- [58] I. A. Qasse, M. Abu Talib, and Q. Nasir, "Inter blockchain communication: A survey," in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, 2019, pp. 1–6.
- [59] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM symposium on principles of distributed computing*, 2018, pp. 245–254.
- [60] M. Burgess, "Bringing bitcoin to defi: A complete beginners deep dive into renvm," 2020.
- [61] D. P. Bauer, "Erc-20: Fungible tokens," in *Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer*. Springer, 2022, pp. 17–48.
- [62] J. Kim, M. Essaid, and H. Ju, "Inter-blockchain communication message relay time measurement and analysis in cosmos," in *2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2022, pp. 1–6.
- [63] R. Zarick, B. Pellegrino, and C. Banister, "Layerzero: Trustless omnichain interoperability protocol," *arXiv preprint arXiv:2110.13871*, 2021.
- [64] "Multichain: Cross-chain router protocol." [Online]. Available: <https://multichain.xyz/>
- [65] T. Lavour, J. Lacan, and C. P. Chanel, "Enabling blockchain services for ioe with zk-rollups," *Sensors*, vol. 22, no. 17, p. 6493, 2022.
- [66] V. Buterin, "Why sharding is great: demystifying the technical properties (2021)," URL <https://vitalik.ca/general/2021/04/07/sharding.html>, 2021.
- [67] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE access*, vol. 8, pp. 125 244–125 262, 2020.
- [68] G. A. F. Rebello, G. F. Camilo, L. A. C. de Souza, M. Potop-Butucaru, M. D. de Amorim, M. E. M. Campista, and L. H. M. Costa, "A survey on blockchain scalability: From hardware to layer-two protocols," *IEEE Communications Surveys & Tutorials*, 2024.
- [69] E. A. Brewer, "Towards robust distributed systems," in *PODC*, vol. 7, no. 10.1145. Portland, OR, 2000, pp. 343–477.
- [70] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *Ict Express*, vol. 7, no. 2, pp. 229–233, 2021.
- [71] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881*, 2021.
- [72] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–35, 2023.
- [73] X. Fan, Q. Chai, and Z. Zhong, "Multav: A multi-chain token backed voting framework for decentralized blockchain governance," in *International Conference on Blockchain*. Springer, 2020, pp. 33–47.
- [74] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *Journal of Network and Computer Applications*, vol. 149, p. 102471, 2020.
- [75] E. N. Tas, R. Han, D. Tse, and M. Yu, "Interchain timestamping for mesh security," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 1585–1599.
- [76] "Connex.t." [Online]. Available: <https://connexscan.io/>
- [77] "Coindesk." [Online]. Available: <https://www.coindesk.com/tag/cross-chain/>
- [78] R. Belchior, J. Süßenguth, Q. Feng, T. Hardjono, A. Vasconcelos, and M. Correia, "A brief history of blockchain interoperability," *Communications of the ACM*, 2023.
- [79] S. Raval, *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.", 2016.
- [80] W. Liang, Y. Liu, C. Yang, S. Xie, K. Li, and W. Susilo, "On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: A comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–35, 2024.
- [81] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 179–196.
- [82] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*. Springer, 2015, pp. 281–310.
- [83] G. Wood, "A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
- [84] F. Vernadat, "Interoperable enterprise systems: architectures and methods," *IFAC Proceedings Volumes*, vol. 39, no. 3, pp. 13–20, 2006.
- [85] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," Ph.D. dissertation, University of Guelph, 2016.
- [86] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Blockchain interoperable digital objects," in *Blockchain-ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 2*. Springer, 2019, pp. 80–94.
- [87] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.
- [88] A. Geraci, *IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries*. IEEE Press, 1991.
- [89] R. Rahimian and J. Clark, "Tokenhook: Secure erc-20 smart contract," *arXiv preprint arXiv:2107.02997*, 2021.
- [90] M. À. Cabot-Nadal, M. M. Payeras-Capellà, M. Mut-Puigserver, and A. Soto-Fernández, "Improving the token erc-721 implementation for selective receipt: rejectable nfts," in *2022 6th International conference on system reliability and safety (ICRSRS)*. IEEE, 2022, pp. 243–250.
- [91] G. Scaffino, L. Aumayr, Z. Avarikioti, and M. Maffei, "Glimpse: {On-Demand}{PoW} light client with {Constant-Size} storage for {DeFi}," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 733–750.
- [92] R. Belchior, L. Riley, T. Hardjono, A. Vasconcelos, and M. Correia, "Do you need a distributed ledger technology interoperability solution?" *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 1, pp. 1–37, 2023.
- [93] S. A. Thyagarajan, G. Malavolta, and P. Moreno-Sanchez, "Universal atomic swaps: Secure exchange of coins across all blockchains," in *2022 IEEE symposium on security and privacy (SP)*. IEEE, 2022, pp. 1299–1316.
- [94] P. Fraunthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, "Eth relay: A cost-efficient relay for ethereum-based blockchains," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 204–213.
- [95] O. Ciobotaru, F. Shirazi, A. Stewart, and S. Vasilyev, "Accountable light client systems for pos blockchains," *Cryptology ePrint Archive*, 2022.
- [96] M. Westerkamp and J. Eberhardt, "zkrelay: Facilitating sidechains using zksnark-based chain-relays," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 378–386.
- [97] A. Garofolo, D. Kaidalov, and R. Oliynykov, "Zendoo: A zk-snark verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2020, pp. 1257–1262.

- [98] R. Belchior, L. Torres, J. Pfannschmid, A. Vasconcelos, and M. Correia, "Can we share the same perspective? blockchain interoperability with views," 2022.
- [99] C. Pedreira, R. Belchior, M. Matos, and A. Vasconcelos, "Trustable blockchain interoperability: Securing asset transfers on permissioned blockchains," *Authorea Preprints*, 2023.
- [100] X. Zhang, W. Zhong, C. Yang, L. Chen, J. Liao, and N. Xiong, "Bft consensus algorithms," in *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2023, pp. 434–439.
- [101] R. Pass and E. Shi, "Fruitchains: A fair blockchain," in *Proceedings of the ACM symposium on principles of distributed computing*, 2017, pp. 315–324.
- [102] S. Agrawal, G. Malavolta, and T. Zhang, "Time-lock puzzles from lattices," in *Annual International Cryptology Conference*. Springer, 2024, pp. 425–456.
- [103] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Annual international cryptology conference*. Springer, 2018, pp. 757–788.
- [104] Z. Avarikioti, O. S. Thyfronitis Litos, and R. Wattenhofer, "Cerberus channels: Incentivizing watchtowers for bitcoin," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 346–366.
- [105] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "Sok: Off the chain transactions." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 360, 2019.
- [106] "Crosschain risk framework." [Online]. Available: <https://crosschainriskframework.github.io/>
- [107] G. Caldarelli, "Overview of blockchain oracle research," *Future Internet*, vol. 14, no. 6, p. 175, 2022.
- [108] "Atomic swap 2013," 2013. [Online]. Available: <https://iq.wiki/wiki/atomic-swap/>
- [109] H. Yu, Y. Sun, Y. Liu, and L. Zhang, "Bitcoin gold, litecoin silver: An introduction to cryptocurrency valuation and trading strategy," in *Future of Information and Communication Conference*. Springer, 2024, pp. 573–586.
- [110] "Atomic swap 2020," 2020. [Online]. Available: <https://corporatefinanceinstitute.com/resources/cryptocurrency/atomic-swaps/>
- [111] S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: A review," in *2020 4th international conference on computer, communication and signal processing (ICCCSP)*. IEEE, 2020, pp. 1–7.
- [112] "Sas: Succinct atomic swap," 2020. [Online]. Available: <https://gist.github.com/RubenSomsen/8853a66a64825716f51b409be528355f>
- [113] L. Aumayr, O. Ersoy, A. Erwig, S. Faust, K. Hostakova, M. Maffei, P. Moreno-Sanchez, and S. Riahi, "Generalized bitcoin-compatible channels," 2020.
- [114] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1521–1538.
- [115] J. Lind, I. Eyal, P. Pietzuch, and E. G. Sirer, "Teechan: Payment channels using trusted execution environments," *arXiv preprint arXiv:1612.07766*, 2016.
- [116] X. Wen, Q. Feng, J. Niu, Y. Zhang, and C. Feng, "Mercury: Practical cross-chain exchange via trusted hardware," *arXiv preprint arXiv:2409.14640*, 2024.
- [117] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.
- [118] G. Chen, S. Chen, Y. Xiao, Y. Zhang, Z. Lin, and T. H. Lai, "Sgxpectre: Stealing intel secrets from sgx enclaves via speculative execution," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2019, pp. 142–157.
- [119] J. Van Bulck, D. Oswald, E. Marin, A. Aldoseri, F. D. Garcia, and F. Piessens, "A tale of two worlds: Assessing the vulnerability of enclave shielding runtimes," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1741–1758.
- [120] Y. Zhang, D. Yang, and G. Xue, "Cheapay: An optimal algorithm for fee minimization in blockchain-based payment channel networks," in *ICC 2019-2019 IEEE international conference on communications (icc)*. IEEE, 2019, pp. 1–6.
- [121] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," *Cryptology ePrint Archive*, 2018.
- [122] A. Deshpande and M. Herlihy, "Privacy-preserving cross-chain atomic swaps," in *International conference on financial cryptography and data security*. Springer, 2020, pp. 540–549.
- [123] I. Tsabary, M. Yechieli, A. Manuskin, and I. Eyal, "Mad-htlc: because htlc is crazy-cheap to attack," in *2021 IEEE symposium on security and privacy (SP)*. IEEE, 2021, pp. 1230–1248.
- [124] Y. Guo, M. Xu, D. Yu, Y. Yu, R. Ranjan, and X. Cheng, "Cross-channel: Scalable off-chain channels supporting fair and atomic cross-chain operations," *IEEE Transactions on Computers*, vol. 72, no. 11, pp. 3231–3244, 2023.
- [125] Y. Guo, M. Xu, X. Cheng, D. Yu, W. Qiu, G. Qu, W. Wang, and M. Song, "zkcross: A novel architecture for cross-chain privacy-preserving auditing," *Cryptology ePrint Archive*, 2024.
- [126] N. Papadis and L. Tassiulas, "Blockchain-based payment channel networks: Challenges and recent advances," *IEEE Access*, vol. 8, pp. 227 596–227 609, 2020.
- [127] M. Escardó and P. Oliva, "Sequential games and optimal strategies," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 467, no. 2130, pp. 1519–1545, 2011.
- [128] R. W. Lai, V. Ronge, T. Ruffing, D. Schröder, S. A. K. Thyagarajan, and J. Wang, "Omniring: Scaling private payments without trusted setup," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 31–48.
- [129] D. Schwartz, N. Youngs, A. Britto et al., "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.
- [130] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE symposium on security and privacy*. IEEE, 2014, pp. 459–474.
- [131] "Monero timelock woes." [Online]. Available: <https://thecharlatan.ch/Monero-Unlock-Time-Privacy/>
- [132] "Time locked transaction outputs." [Online]. Available: <https://github.com/mimblewimble/grin/issues/25>
- [133] "Implement confidentially timelocked funds." [Online]. Available: <https://github.com/zcash/zcash/issues/344>
- [134] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "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.
- [135] Y. Liu, W. Liang, K. Xie, S. Xie, K. Li, and W. Meng, "Lightpay: A lightweight and secure off-chain multi-path payment scheme based on adapter signatures," *IEEE Transactions on Services Computing*, 2023.
- [136] S. You, A. Joshi, A. Kuehlkamp, and J. Nabrzycki, "A multi-party, multi-blockchain atomic swap protocol with universal adaptor secret," *arXiv preprint arXiv:2406.16822*, 2024.
- [137] P. Ni, A. Tian, and J. Xu, "pipeswap: Forcing the early release of a secret for atomic swaps across all blockchains," *Cryptology ePrint Archive*, 2024.
- [138] K. Kajita, G. Ohtake, and T. Takagi, "Generalized adaptor signature scheme: From two-party to n-party settings." *IACR Cryptol. ePrint Arch.*, vol. 2024, p. 241, 2024.
- [139] C. Chen, G. Yang, Z. Li, F. Xiao, Q. Chen, and J. Li, "Privacy-preserving multi-party cross-chain transaction protocols," *Cryptology*, vol. 8, no. 1, p. 6, 2024.
- [140] Y. Ji, Y. Xiao, B. Gao, and R. Zhang, "Threshold/multi adaptor signature and their applications in blockchains," *Electronics*, vol. 13, no. 1, p. 76, 2023.
- [141] Z. Yin, B. Zhang, J. Xu, K. Lu, and K. Ren, "Bool network: An open, distributed, secure cross-chain notary platform," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3465–3478, 2022.
- [142] J. Wang, Y. Wan, Y. Hu, Y. Yuan, and K. Fan, "Cross-chain supervision mechanism of distributed notaries for consortium blockchain," in *2023 6th International Conference on Artificial Intelligence and Big Data (ICAIBD)*. IEEE, 2023, pp. 579–584.
- [143] H. Tian, K. Xue, X. Luo, S. Li, J. Xu, J. Liu, J. Zhao, and D. S. Wei, "Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3928–3941, 2021.

- [144] A. Xiong, G. Liu, Q. Zhu, A. Jing, and S. W. Loke, "A notary group-based cross-chain mechanism," *Digital Communications and Networks*, vol. 8, no. 6, pp. 1059–1067, 2022.
- [145] X. Niu, L. Kong, F. Jin, X. Song, X. Min, and Q. Li, "Nft cross-chain transfer method under the notary group scheme," in *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2023, pp. 996–1001.
- [146] S. Zhao and L. Cao, "Dynamic notary group election algorithm based on reputation value," in *2022 International Conference on Bigdata Blockchain and Economy Management (ICBBEM 2022)*. Atlantis Press, 2022, pp. 903–915.
- [147] Y. Sun, L. Yi, L. Duan, and W. Wang, "A decentralized cross-chain service protocol based on notary schemes and hash-locking," in *2022 IEEE International Conference on Services Computing (SCC)*. IEEE, 2022, pp. 152–157.
- [148] X. Hu, Y. Ling, J. Hua, Z. Dong, Y. Sun, and J. Qi, "A blockchain cross-chain transaction method based on decentralized dynamic reputation value assessment," *IEEE Transactions on Network and Service Management*, 2024.
- [149] P. Chatzigiannis, F. Baldimtsi, and K. Chalkias, "Sok: Blockchain light clients," in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 615–641.
- [150] A. Kiayias, N. Lamprou, and A.-P. Stouka, "Proofs of proofs of work with sublinear complexity," in *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20*. Springer, 2016, pp. 61–78.
- [151] A. Kiayias, A. Miller, and D. Zindros, "Non-interactive proofs of proof-of-work," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 505–522.
- [152] B. Bünz, L. Kiffer, L. Luu, and M. Zamani, "Flyclient: Super-light clients for cryptocurrencies," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 928–946.
- [153] J. Bonneau, I. Meckler, V. Rao, and E. Shapiro, "Coda: Decentralized cryptocurrency at scale," *Cryptology ePrint Archive*, 2020.
- [154] R. Belchior, D. Dimov, Z. Karadjov, J. Pfannschmidt, A. Vasconcelos, and M. Correia, "Harmonia: Securing cross-chain applications using zero-knowledge proofs," *Authorea Preprints*, 2024.
- [155] M. Bartoletti and R. Zunino, "Bitml: a calculus for bitcoin smart contracts," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 83–100.
- [156] "Stateless spv proofs and economic security." [Online]. Available: <https://ethresear.ch/t/stateless-spv-proofs-and-economic-security/5451>
- [157] L. Aumayr, Z. Avarikioti, M. Maffei, G. Scaffino, and D. Zindros, "Blink: An optimal proof of proof-of-work," *Cryptology ePrint Archive*, 2024.
- [158] K. Karantias, A. Kiayias, and D. Zindros, "Compact storage of superblocks for nipopow applications," in *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer, 2020, pp. 77–91.
- [159] S. Daveas, K. Karantias, A. Kiayias, and D. Zindros, "A gas-efficient superlight bitcoin client in solidity," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 132–144.
- [160] A. Kiayias, A. Polydouri, and D. Zindros, "The velvet path to superlight blockchain clients," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 205–218.
- [161] A. Kiayias, N. Leonardos, and D. Zindros, "Mining in logarithmic space," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 3487–3501.
- [162] "How to validate bitcoin payments in ethereum (for only 700k gas!)." [Online]. Available: <https://medium.com/summa-technology/cross-chain-auction-technical-f16710bfe69f>
- [163] "Summa." [Online]. Available: <https://github.com/summa-tx/bitcoin-spv>
- [164] F. Barbàra and C. Schifanella, "Bxtb: cross-chain exchanges of bitcoins for all bitcoin wrapped tokens," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2022, pp. 143–150.
- [165] P. Gaži, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 139–156.
- [166] J. Dille, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, "Strong federations: An interoperable blockchain solution to centralized third-party risks," *arXiv preprint arXiv:1612.05491*, 2016.
- [167] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.
- [168] J. Nick, A. Poelstra, and G. Sanders, "Liquid: A bitcoin sidechain," *Liquid white paper*. URL <https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf>, 2020.
- [169] F. Gai, J. Niu, S. A. Tabatabaee, C. Feng, and M. Jalalzai, "Cumulus: a secure bft-based sidechain for off-chain scaling," in *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*. IEEE, 2021, pp. 1–6.
- [170] P. Sztorc, "Drivechain," 2015.
- [171] Y. Shahsavari, K. Zhang, and C. Talhi, "A theoretical model for fork analysis in the bitcoin network," in *2019 IEEE international conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 237–244.
- [172] B. Alangot, D. Reijbergen, S. Venugopalan, and P. Szalachowski, "Decentralized lightweight detection of eclipse attacks on bitcoin clients," in *2020 IEEE international conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 337–342.
- [173] "Drivechain the simple two way peg," 2017. [Online]. Available: <https://www.truthcoin.info/blog/drivechain/>
- [174] T. Li, M. Wang, Z. Deng, and D. Liu, "Sepow: Secure and efficient proof of work sidechains," in *Algorithms and Architectures for Parallel Processing: 21st International Conference, ICA3PP 2021, Virtual Event, December 3–5, 2021, Proceedings, Part III*. Springer, 2022, pp. 376–396.
- [175] A. Zamyatin, Z. Avarikioti, D. Perez, and W. J. Knottenbelt, "Txchain: Efficient cryptocurrency light clients via contingent transaction aggregation," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2020 International Workshops, DPM 2020 and CBT 2020, Guildford, UK, September 17–18, 2020, Revised Selected Papers 15*. Springer, 2020, pp. 269–286.
- [176] A. Kiayias and D. Zindros, "Proof-of-work sidechains," in *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*. Springer, 2020, pp. 21–34.
- [177] L. Yin, J. Xu, and Q. Tang, "Sidechains with fast cross-chain transfers," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3925–3940, 2021.
- [178] Z. Deng, T. Li, C. Tang, D. He, and Z. Zheng, "Pssc: Practical and secure sidechains construction for heterogeneous blockchains orienting iot," *IEEE Internet of Things Journal*, 2023.
- [179] T. Li, H. Huang, L. Yin, S. Yao, and Z. Zheng, "Ussc: Universal and storage-efficient sidechains," in *2024 IEEE 44th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2024, pp. 379–390.
- [180] L. Yin, J. Xu, K. Liang, and Z. Zhang, "Sidechains with optimally succinct proof," *IEEE Transactions on Dependable and Secure Computing*, 2023.
- [181] T. Chen, H. Lu, T. Kunpittaya, and A. Luo, "A review of zk-snarks," *arXiv preprint arXiv:2202.06877*, 2022.
- [182] J. Teutsch, M. Straka, and D. Boneh, "Retrofitting a two-way peg between blockchains," *arXiv preprint arXiv:1908.03999*, 2019.
- [183] B. Pillai, K. Biswas, Z. Hóu, and V. Muthukumarasamy, "Cross-blockchain technology: integration framework and security assumptions," *IEEE access*, vol. 10, pp. 41 239–41 259, 2022.
- [184] G. Caldarelli, "Wrapping trust for interoperability: A preliminary study of wrapped tokens," *Information*, vol. 13, no. 1, p. 6, 2021.
- [185] L. Yang, X. Dong, Z. Wan, S. Gao, W. Tong, D. Lu, Y. Shen, and X. Du, "Asynsc: An asynchronous sidechain for multi-domain data exchange in internet of things," *arXiv preprint arXiv:2412.12723*, 2024.
- [186] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, "Xclaim: Trustless, interoperable, cryptocurrency-backed assets," in *2019 IEEE symposium on security and privacy (SP)*. IEEE, 2019, pp. 193–210.
- [187] M. Westerkamp and M. Diez, "Verilay: A verifiable proof of stake chain relay," in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–9.
- [188] J. Gorzny and M. Derka, "A rollup comparison framework," *arXiv preprint arXiv:2404.16150*, 2024.
- [189] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *27th*

- USENIX Security Symposium (USENIX Security 18), 2018, pp. 1353–1370.
- [190] “Welcome to the optimism collective.” [Online]. Available: <https://community.optimism.io/>
- [191] A. Jain, Y. Punjabi, and R. Mathur, “Exploring the efficacy of rollups—a comparative study of optimistic and zk-rollups and their popular implementations.”
- [192] D. Wang, J. Zhou, A. Wang, and M. Finestone, “Loopring: A decentralized token exchange protocol,” URL https://github.com/Loopring/whitepaper/blob/master/en_whitepaper.pdf, 2018.
- [193] A. A. Khalil and M. A. Rahman, “Parole: Profitable arbitrage in optimistic rollup with ERC-721 token transactions,” in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2024, pp. 129–141.
- [194] A. Yamamoto and S. Yamashita, “Examination on interoperability of blockchains by using zk-rollups,” in *Proceedings of the 2023 5th Blockchain and Internet of Things Conference*, 2023, pp. 41–49.
- [195] D. Ilisei, “Analyzing the role of bridges in cross-chain mev extraction,” Ph.D. dissertation, Master’s thesis, TU München, 2024.
- [196] “Starkware docs.” [Online]. Available: <https://docs.starkware.co/starkex/>
- [197] B. Pillai, K. Biswas, Z. Hóu, and V. Muthukkumarasamy, “Burn-to-claim: An asset transfer protocol for blockchain interoperability,” *Computer Networks*, vol. 200, p. 108495, 2021.
- [198] —, “The burn-to-claim cross-blockchain asset transfer protocol,” in *2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2020, pp. 119–124.
- [199] B. Pillai, Z. Hóu, K. Biswas, and V. Muthukkumarasamy, “Formal verification of the burn-to-claim blockchain interoperable protocol,” in *International Conference on Formal Engineering Methods*. Springer, 2023, pp. 249–254.
- [200] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, “Enhancing bitcoin security and performance with strong consistency via collective signing,” in *25th usenix security symposium (usenix security 16)*, 2016, pp. 279–296.
- [201] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, “Solida: A blockchain protocol based on reconfigurable byzantine consensus,” *arXiv preprint arXiv:1612.02916*, 2016.
- [202] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling byzantine agreements for cryptocurrencies,” in *Proceedings of the 26th symposium on operating systems principles*, 2017, pp. 51–68.
- [203] X. Wu, Z. Wang, X. Li, and L. Chen, “Dbpbft: A hierarchical pbft consensus algorithm with dual blockchain for iot,” *Future Generation Computer Systems*, vol. 162, p. 107429, 2025.
- [204] R. Guo, Z. Guo, Z. Lin, and W. Jiang, “A hierarchical byzantine fault tolerance consensus protocol for the internet of things,” *High-Confidence Computing*, vol. 4, no. 3, p. 100196, 2024.
- [205] Z. Deng, C. Tang, T. Li, and D. He, “A distributed ledger-assisted robust and trusted service protocol for vanets,” *IEEE Internet of Things Journal*, 2024.
- [206] X. Chen, T. Ma, B. Er-Rahmadi, J. Hillston, and G. Yuan, “Parallel byzantine consensus based on hierarchical architecture and trusted hardware,” *IEEE Transactions on Dependable and Secure Computing*, 2024.
- [207] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “Omniledger: A secure, scale-out, decentralized ledger via sharding,” in *2018 IEEE symposium on security and privacy (SP)*. IEEE, 2018, pp. 583–598.
- [208] H. Huang, X. Peng, J. Zhan, S. Zhang, Y. Lin, Z. Zheng, and S. Guo, “Brokerchain: A cross-shard blockchain protocol for account/balance-based state sharding,” in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 1968–1977.
- [209] Z. Hong, S. Guo, E. Zhou, J. Zhang, W. Chen, J. Liang, J. Zhang, and A. Zomaya, “Prophet: Conflict-free sharding blockchain via byzantine-tolerant deterministic ordering,” in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*. IEEE, 2023, pp. 1–10.
- [210] A. Sonnino, S. Bano, M. Al-Bassam, and G. Danezis, “Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers,” in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2020, pp. 294–308.
- [211] M. Zamani, M. Movahedi, and M. Raykova, “Rapidchain: Scaling blockchain via full sharding,” in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 931–948.
- [212] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, “Chainspace: A sharded smart contracts platform,” *arXiv preprint arXiv:1708.03778*, 2017.
- [213] H. Huang, Y. Lin, and Z. Zheng, “Account migration across blockchain shards using fine-tuned lock mechanism,” in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications*. IEEE, 2024, pp. 271–280.
- [214] Y. Lin, M. Li, and J. Zhang, “Spiralshard: Highly concurrent and secure blockchain sharding via linked cross-shard endorsement,” *arXiv preprint arXiv:2407.08651*, 2024.
- [215] G. Robinson, S. Dörry, and B. Derudder, “Global networks of money and information at the crossroads: Correspondent banking and swift,” *Global Networks*, vol. 23, no. 2, pp. 478–493, 2023.
- [216] M. F. Cruz, C. A. M. T. Cavalcante, and S. T. Sá Barretto, “Using OPC and HL7 standards to incorporate an industrial big data historian in a health IT environment,” *Journal of Medical Systems*, vol. 42, pp. 1–11, 2018.
- [217] “The entire process of an atomic transaction via ILP.” [Online]. Available: <https://interledger.org/developers/rfcs/hashed-timelock-agreements/>
- [218] J. Kwon and E. Buchman, “A network of distributed ledgers,” *Cosmos*, dated, pp. 1–41, 2018.
- [219] G. Pititto, “The gasper protocol: a proof of stake era for ethereum,” Ph.D. dissertation, Politecnico di Torino, 2022.
- [220] J. Burdges, A. Cevallos, P. Czaban, R. Habermeier, S. Hosseini, F. Lama, H. K. Alper, X. Luo, F. Shirazi, A. Stewart et al., “Overview of polkadot and its design considerations,” *arXiv preprint arXiv:2005.13456*, 2020.
- [221] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, “Hyperservice: Interoperability and programmability across heterogeneous blockchains,” in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 549–566.
- [222] “Layerzero network.” [Online]. Available: <https://layerzero.network/>
- [223] S. D. Lerner, J. Á. Cid-Fuentes, J. Len, R. Fernández-València, P. Gallardo, N. Vescovo, R. Laprida, S. Mishra, F. Jinich, and D. Masini, “Rsk: A bitcoin sidechain with stateful smart-contracts,” *Cryptology ePrint Archive*, 2022.
- [224] “Hyperledger cactus whitepaper.” [Online]. Available: <https://github.com/opentaps/cactus/blob/main/whitepaper/whitepaper.md>
- [225] “Wecross whitepaper.” [Online]. Available: <https://wecross.readthedocs.io/zh-cn/latest/>
- [226] H. Li, Y. Chen, X. Shi, X. Bai, N. Mo, W. Li, R. Guo, Z. Wang, and Y. Sun, “Fisco-bcos: An enterprise-grade permissioned blockchain system with high-performance,” in *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, 2023, pp. 1–17.
- [227] “Hyperledger firefly.” [Online]. Available: <https://www.lfdecentralizedtrust.org/projects/firefly>
- [228] “Weaver: Interoperability across dlt networks.” [Online]. Available: <https://github.com/hyperledger-labs/weaver-dlt-interoperability/blob/main/OVERVIEW.md>
- [229] “Introducing hyperledger cacti, a multi-faceted pluggable interoperability framework.” [Online]. Available: <https://hyperledger-cacti.github.io/cacti/vision/>
- [230] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, “Redactable blockchain—or—rewriting history in bitcoin and friends,” in *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 2017, pp. 111–126.
- [231] T. Ye, M. Luo, Y. Yang, K.-K. R. Choo, and D. He, “A survey on redactable blockchain: challenges and opportunities,” *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1669–1683, 2023.
- [232] D. Deuber, B. Magri, and S. A. K. Thyagarajan, “Redactable blockchain in the permissionless setting,” in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 124–138.
- [233] Y. Tian, B. Liu, Y. Li, P. Szalachowski, and J. Zhou, “Accountable fine-grained blockchain rewriting in the permissionless setting,” *IEEE Transactions on Information Forensics and Security*, 2023.
- [234] Y. Manevich, A. Barger, and G. Assa, “Redacting transactions from execute-order-validate blockchains,” in *2021 IEEE Interna-*

- tional Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–9.
- [235] S. Hu, M. Li, J. Weng, J.-N. Liu, J. Weng, and Z. Li, “Ivyredaction: Enabling atomic, consistent and accountable cross-chain rewriting,” *IEEE Transactions on Dependable and Secure Computing*, 2023.
- [236] R. Du, T. Chen, J. Tian, and T. Shang, “Starcross: Redactable blockchain-based secure and lightweight data sharing framework for satellite-based iot,” *Computer Networks*, vol. 253, p. 110718, 2024.
- [237] S. Zhang, T. Xie, K. Gai, and L. Xu, “Arc: an asynchronous consensus and relay chain-based cross-chain solution to consortium blockchain,” in *2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2022, pp. 86–92.
- [238] T. Xie, K. Gai, L. Zhu, S. Wang, and Z. Zhang, “Rac-chain: An asynchronous consensus-based cross-chain approach to scalable blockchain for metaverse,” *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 20, no. 7, pp. 1–24, 2024.
- [239] C. Cachin, K. Kursawe, F. Petzold, and V. Shoup, “Secure and efficient asynchronous broadcast protocols,” in *Annual International Cryptology Conference*. Springer, 2001, pp. 524–541.
- [240] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, “The honey badger of bft protocols,” in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 31–42.
- [241] S. Duan, M. K. Reiter, and H. Zhang, “Beat: Asynchronous bft made practical,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 2028–2041.
- [242] B. Guo, Z. Lu, Q. Tang, J. Xu, and Z. Zhang, “Dumbo: Faster asynchronous bft protocols,” in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 803–818.
- [243] L. Yang, S.-T. Ni, Y. Wang, A. Yu, J.-A. Lee, and P. Hui, “Interoperability of the metaverse: A digital ecosystem perspective review,” *arXiv preprint arXiv:2403.05205*, 2024.
- [244] A. J. Bokolo, “Exploring interoperability of distributed ledger and decentralized technology adoption in virtual enterprises,” *Information Systems and e-Business Management*, vol. 20, no. 4, pp. 685–718, 2022.
- [245] J. Yang, Y. Li, Y. Lai, and M. Liu, “Non-fungible tokens (nfts): tokens of digital assets on the blockchain,” in *Proceedings of the 2023 International Conference on Electronics, Computers and Communication Technology*, 2023, pp. 175–182.
- [246] L. D. Negka and G. P. Spathoulas, “Blockchain state channels: A state of the art,” *IEEE Access*, vol. 9, pp. 160 277–160 298, 2021.
- [247] T. Hardjono, “Blockchain gateways, bridges and delegated hashlocks,” *arXiv preprint arXiv:2102.03933*, 2021.
- [248] P. Voigt and A. Von dem Bussche, “The eu general data protection regulation (gdpr),” *A Practical Guide, 1st Ed.*, Cham: Springer International Publishing, vol. 10, no. 3152676, pp. 10–5555, 2017.
- [249] E. Goldman, “An introduction to the california consumer privacy act (ccpa),” *Santa Clara Univ. Legal Studies Research Paper*, 2020.
- [250] “Guide to the systems engineering body of knowledge (sebok).” [Online]. Available: [https://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_\(SEBoK\)](https://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK))
- [251] A. Aldaej, T. A. Ahanger, and I. Ullah, “Deep neural network-based secure healthcare framework,” *Neural Computing and Applications*, pp. 1–16, 2024.
- [252] M. Dohler, D. R. Lopez, and C. Wang, *Blockchains in 6G: A Standardized Approach to Permissioned Distributed Ledgers*. CRC Press, 2024.

AUTHOR BIOGRAPHIES

Zhihong Deng received the M.S. degree in the School of Mathematics and Computational Science, Hunan University of Science and Technology, Hunan, China, in 2021. He is currently working the Ph.D. degree at the School of Mathematics and Information Science, Guangzhou University, Guangzhou, China. His main research interests include blockchain, applied cryptography, algorithmic game theory and Web3.

Chunming Tang received the Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy

of Sciences, Beijing, China, in 2004. He is currently a professor of the School of Mathematics and Information Science, Guangzhou University, Guangzhou, China. He has authored or co-authored more than 100 research papers in refereed international journals and conferences, such as AsiaCrypt, IEEE TRANSACTIONS ON INFORMATION THEORY, and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His main research interests include code theory, cryptography, and information security.

Taotao Li received the Ph.D. degree in cyber security from Institute of Information Engineering, Chinese Academy of Sciences and University of Chinese Academy of Sciences, China, in 2022. He is currently a postdoc with the School of Software Engineering, Sun Yat-Sen University, Zhuhai, China. His main research interests include blockchain, Web3, applied cryptography.

Parhat Abla received the Ph.D. degree in cyber security from Institute of Information Engineering, Chinese Academy of Sciences and University of Chinese Academy of Sciences, China, in 2022. He is currently an assistant researcher with the School of Software, South China Normal University. His main research interests include blockchain, Data security, cryptography, lattice-based cryptography.

Qi Chen received the B.S. degree from the University of Information Engineering, China, in 2001, the M.S. degree from the National University of Defense Technology, China, in 2006, and the Ph.D. degree from Guangzhou University, China, in 2011, all in mathematics. Since 2017, he has been with Guangzhou University. His research interests include secret sharing, blockchain, cryptography, and coding theory.

Wei Liang received a Ph.D. degree in computer science and technology from Hunan University in 2013, and a Postdoctoral Scholar with Lehigh University during 2014-2016. Dr. Liang is currently a Professor at the School of Computer Science and Engineering, Hunan University of Science and Technology. He has authored or co-authored more than 150 journal/conference papers. His research interests include intelligent transportation, security of IoV, blockchain, embedded systems and hardware IP protection, and security management in wireless sensor networks.

Debiao He received the Ph.D. degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University. His research interests include cryptography and information security, in particular, cryptographic protocols. He has authored or co-authored more than 100 research papers in refereed international journals and conferences, such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and USENIX Security Symposium. His work has been cited more than 15000 times at Google Scholar. He was the recipient of the IEEE SYSTEMS JOURNAL 2018, 2019 Best Paper Award and IET Information Security 2019 Best Paper Award. He is with the Editorial Board of several international journals, such as IEEE TRANSACTIONS ON COMPUTERS, Journal of Information Security and Applications, Frontiers of Computer Science, and Human-centric Computing and Information Sciences.