A Survey on Trustless Cross-chain Interoperability Solutions in On-chain Finance

Hasret Ozan Sevim[1,2]

[1]International School of Advanced Studies (University of Camerino), Via Gentile III Da Varano, 62032, Camerino, Italy

[2]Catholic University of the Sacred Heart, Largo A. Gemelli 1, 20123, Milano, Italy

Abstract

Interoperability between different distributed ledger technologies stands as a key concept by enabling efficient and secure communication for the future of fragmented permissioned and permissionless distributed ledger networks. This paper presents an analysis of the fundamentals, state-of-the-art, and pioneering examples of cross-chain interoperability protocols. The leading trustless interoperability protocols (LayerZero, Wormhole, Chainlink Cross-chain Interoperability Protocol, Circle Cross-chain Transfer Protocol, Polkadot, and Cosmos) are compared in terms of their design, mechanisms, consensus, and limitations. A set of simple metrics is proposed to show a conduit for future empirical research like measuring performance and compatibility of different interoperability solutions.

Keywords

Interoperability, Cross-chain, Distributed Ledger Technologies, Comparison, Financial Technologies

1. Introduction

The landscape of cross-chain interoperability solutions has gained significant attention as the distributed ledger network ecosystem keeps growing and becomes more fragmented. The need for interoperability arises from the idea to benefit from the strengths of multiple blockchains simultaneously, creating more integrated, efficient, and versatile systems. Ideal interoperability solutions aim to overcome the issues like liquidity fragmentation across different ledgers, limited accessibility to diverse assets, operational inefficiencies, increased counter-party risks, lower financial adoption and innovation across the distributed ledger technologies (DLT) ecosystem, and poor user experience. This paper is written to detect the developments in the DLT interoperability solutions and explore the capabilities of these solutions on on-chain finance.

The first part of the paper takes a look at the concepts in the DLT and interoperability literature. The second part questions the necessity and future of cross-chain interoperability (CCI) solutions. The third part scans the existing literature on cross-chain interoperability. The fourth part sorts the promising and popular cross-chain interoperability solutions, and examines their features, designs and mechanisms. These solutions are LayerZero, Wormhole, Circle's Cross-chain Transfer Protocol (CCTP), Chainlink's Cross-chain Interoperability Protocol (CCIP), Wormhole, Polkadot, and Cosmos. The fifth part compares these solutions from many aspects: focus, nature, key features, structure, technical mechanisms, chain

6th Distributed Ledger Technologies Workshop (DLT2024), May, 14-15 2024 – Turin, Italy

*PhD Candidate in Blockchain and Distributed Ledger Technology (Cycle 39)

hasretozan.sevim@unicam.it (H. O. Sevim)

0000-0002-1923-737X (H. O. Sevim)

type, consensus/protocol, cross-chain type, vulnerabilities and limitations. The sixth part includes basic statistical charts of LayerZero and tables of Wormhole to see the rising interest in the usage of cross-chain solutions. The seventh and last part concludes the paper and shows a potential path that is concluded from this paper for future research, especially on the impact of cross-chain interoperability solutions in on-chain finance.

2. Key Concepts

Understanding cross-chain interoperability solutions requires the knowledge of fundamental concepts of distributed ledger technologies, especially blockchain. In this paper, these fundamental concepts are not referred in detail instead shortly.

In a broad sense, blockchain can be roughly explained as an immutable, considerably more decentralized, trusted, and distributed ledger based on peer-to-peer networks. Essentially, blockchain is a data structure that functions to record transactions interdependently generated within a network where the distributed ledger is constantly synchronized between the peers. Blockchain can be categorized into distinct categories according to how blockchain organizes its participants in different application scenarios.

	Public Blockchain	***Private Blockchain***	***Consortium Blockchain***
Participants	All	Single organization	Multiple organizations
Identities	Pseudo-anonymous	Approved participants	Approved participants
Permissionless	Yes	No	No
Accessibility to Public	Public Read/Write	Restricted	Restricted
Transaction Processing Speed	Slow	Fast	Fast
Application Scales	Large	Small	Medium
Major Concern	Accessibility	Privacy	Collaboration

Figure 1: Distinct categories of blockchain. Adapted from Wang, Wang, Chen (2023).

The transactions of exchanges on DLTs require an atomic swapping process, which can guarantee the integrity of different execution processes. Different parties can trade their assets from different blockchains with each other thanks to atomic swaps. Both parties should have an address on the other blockchain, and the trades must happen simultaneously on both blockchains. Both transfers must be guaranteed to happen or neither of them happens. This property is called “atomic”, as the swap process is made as a whole. The atomic swap can be adopted into multiple blockchain scenarios, which is referred to as an atomic cross-chain swap. An atomic cross-chain swapping process is a distributed coordination task that enables the exchange of assets across multiple blockchains atomically.1 The whole swapping process is executed and automated with the help of smart contracts. A smart contract is a self-executing digital contract stored on a blockchain, automatically enforcing predefined terms and conditions without the need for intermediaries. Smart contracts disintermediate traditional intermediaries. Cross-blockchain smart contracts target general blockchain interoperability differently from cross-blockchain token transferring mechanisms. Different methods exist to implement atomic cross-chain transactions. One way is the use of Hash Time-Locked Contracts (HTLC).

HTLCs are a type of time-bound smart contract that can be used in cross-chain transactions, especially for atomic swaps. This type of contract ensures that a transaction between parties will be completed only if all conditions are met within a specific timeframe. Otherwise, the transaction is nullified and assets are returned to their original owners.

Cross-chain communication is one of the most important design considerations in the current DLT based systems. Because each blockchain system operates as an information isolated zone where it is difficult to obtain external data. Each blockchain executes transactions on its own. But cross-chain bridges are specialized protocols to provide a transfer service of assets and information between different blockchain networks. Bridges can be classified differently depending on their features, including trusted bridges and trustless bridges. Trusted bridges rely on trusted entities or consortiums to validate and facilitate transactions between blockchains. It is easier to be implemented as trusted bridges don't require a sensitivity of high decentralization. However decentralized bridges are designed for reduced trust and centralization. They can be more complex and must ensure security across disparate systems.2

State	Description	Success Condition	On Success	On Error
INIT	Transaction initiated by user's application	Hash of transaction returned	DEPOSIT	ERROR
ERROR	Transaction not sent; balance unchanged	-	-	-
DEPOSIT	Token deposit to the source bridge contract	Block mined (Event)	PROOF	RETRY
RETRY	User can retry deposit	Deposit successfully made	PROOF	WITHDRAWAL
WITHDRAWAL	User initiates deposit maturity	Block mined	UNDO	
UNDO	Transaction reversed; deposit returned	Block mined	-	-
PROOF	Awaiting proof of the transaction	No errors and proof relayed	TARGET	RETRY
RETRY	Attempt to post proof until accepted	No errors and proof relayed	TARGET	WITHDRAWAL
TARGET	Checking the transaction and proof on target bridge	Transaction relayed, proof correct, and block valid	MINT	REVERT
REVERT	Transfer is reverted to source	Refund is relayed to the source	WITHDRAWAL	SECONDARY ERROR
SECONDARY ERROR	Manual intervention required. User must use tools to return transaction, possibly with proof and error code	Refund is relayed to the source	WITHDRAWAL	
MINT	Awaiting final transaction	Block mined	Finish	REVERT

Figure 2: State transitions in the cross-chain bridge process. Adapted from Zilnieks, Erins (2023).

Wrapped tokens represent native assets on a different blockchain non-natively. They are created to enable cross-chain compatibility by locking the original asset on its native chain and issuing a corresponding token on another chain.

Layer two scaling solutions are built on top of existing blockchain networks to provide more scalability and efficiency for transactions. They handle transactions off-chain (typically on a secondary layer) while trying to stick with the security of the main layer. Rollups are prevalent examples with two main categories: optimistic rollups and zero-knowledge rollups (zkRollups). Optimistic rollups publish the state of the secondary chain to the mainchain periodically after a series of cryptographic proof and fraud detection processes. Zkrollups rely on a proof creation process with less processed data without the need of revealing all of the transaction data. They provide faster finality for transactions and they are generally more efficient in terms of on-chain gas usage.

A sidechain is an independent blockchain that is compatible with a parent blockchain (mainchain), allowing assets and data to be transferred between these two chains. The sidechain operates under its own rules and consensus mechanism but is linked to the mainchain with different mechanisms like two-way peg. Relay chains act as central hubs that facilitate communication and transactions between different blockchains (parachains) connected to the network. Polkadot is the pioneering example of relay chains.

Trustless systems minimize the need for trust among participants by relying on technology and mathematics to secure transactions, whereas trusted systems depend on the credibility and reliability of central authorities. In a trustless system, transactions and interactions are conducted with a considerably low level of trust

between participants. This feature typically can be achieved by the technique of deterministic execution. Instead of relying on a central authority or intermediary to validate transactions, trustless systems can rely on cryptographic algorithms and consensus mechanisms as much as possible to ensure the integrity and security of transactions. Consensus mechanisms allow a distributed network of participants (nodes) to agree on the validity of transactions and the state of the ledger without needing to trust each other. Trustless systems may also promote transparency and inclusivity, as anyone with the necessary resources can participate in the network as long as the network activity doesn't require a certain level of trust and confidentiality. But participants in a trusted system must have confidence in these central entities to act honestly and competently. In trusted DLT systems, such as permissioned blockchains or certain types of distributed databases, a predefined set of validators (which could be financial institutions, corporations, or consortia) are responsible for validating transactions and maintaining the ledger. Trusted systems can offer greater scalability and efficiency compared to trustless systems, as the consensus process doesn't require complex consensus mechanisms typically. Trusted systems provide more control over the network, especially for compliance concerns like regulation and privacy.

Innovations in blockchain technology, such as atomic swaps, relay chains, and rollup solutions, have provided new mechanisms to facilitate cross-chain interactions, contributing to the rise of interoperability solutions. Despite the significant progress, cross-chain interoperability solutions face challenges that could hinder their widespread adoption and impact. Interoperability increases the vulnerability of blockchain systems that can be exploited across chains with more catastrophic results. Ensuring the security of cross-chain transactions remains a significant challenge. Developing protocols that try to enable seamless interaction between different blockchains is technically complex. These solutions must be scalable to handle growing transaction volumes without compromising performance or security. The lack of standards and governance models for cross-chain interoperability complicates integration efforts.

3. Fundamental Points

For on-chain finance or so-called decentralized finance (DeFi) applications, interoperability could enhance liquidity significantly by pooling resources across multiple blockchains. It could also provide users and businesses with access to a broader range of assets and services, potentially increasing participation in the digital economy. Permissioned blockchains like Hyperledger can be used by enterprises for their internal operations due to their privacy controls and scalability. These could interoperate with public blockchains to provide transparency and traceability to end users for certain aspects of the provided services and operations, such as the origin of funds/raw materials, leveraging the controlled environment of permissioned DLTs and the transparency of public blockchains.

Interoperability could lead to a more inclusive and collaborative blockchain space with communication and transactions across diverse blockchain ecosystems by breaking down silos and leveraging the unique strengths of different DLTs. Consider a scenario where a blockchain, that is known for its high security but slower transaction speeds like Ethereum, interoperates with a more efficient but less secure blockchain. Assets could be seamlessly transferred between blockchains, leveraging the strengths of each. For example, a digital asset or token created on Ethereum could be transferred to a blockchain with lower transaction fees for everyday transactions, and then moved back to Ethereum when needed for specific smart contract functionalities.

The notion of a multi-chain future, including permissioned blockchains potentially operated by banks, is not just speculative but seems an almost inevitable reality. However the notion of a cross-chain and/or multi-chain future will be possible when the chronic issues inherent in the concept of permissionless

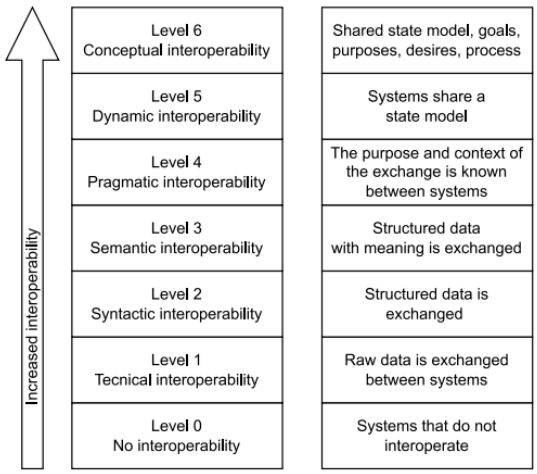

Figure 3: Levels of interoperability. Adapted from Llambias, Bradach, Nogueira, González, Ruggia (2023).

cross-chain interoperability solutions are solved. A hybrid approach, that utilizes both permissioned and permissionless elements where they are most beneficial, might be the most effective solution. But still operating in a less trusted environment can be particularly pertinent for parties from completely different jurisdictions, due to several factors inherent in cross-jurisdictional interactions. Here's why a less trusted or trustless environment, often facilitated by permissionless blockchain platforms, might be required or beneficial in such cases:

1) Reduced Counter-party Risk: In international dealings, the risk of fraud, default, or non-compliance with agreements can be higher due to the difficulty of legal enforcement across borders. Trustless distributed ledger systems reduce counterparty risk by ensuring that transactions are transparent, immutable, and automatically executed in many cases through smart contracts by reducing the need for trust in any single party's actions.

2) Lack of Common Regulatory Framework: Different jurisdictions often have varying regulatory standards, legal systems, and enforcement mechanisms. This diversity can lead to uncertainty and a lack of trust among parties. A considerably more decentralized and trustless system can provide a neutral ground where transactions and agreements are enforced by code, reducing the reliance on any single jurisdiction's legal framework.

3) Cost and Efficiency: Cross-jurisdictional transactions often involve intermediaries such as banks, legal representatives, and regulatory bodies, that can add cost and time delays. A trustless interoperability protocol and a considerably more decentralized blockchain can streamline these processes, enabling direct peer-to-peer interactions without the need for trusted intermediaries, automating transactions, recording them in an immutable and unaltered ledger, leading to more efficient and cost-effective transactions.

4) Anonymity and Privacy: Parties from different jurisdictions may require or prefer anonymity, or at least a degree of privacy in their transaction. Permissionless blockchains can offer mechanisms to protect user identities and transaction details while still ensuring the integrity and verifiability of transactions.

5) Interoperability and Global Access: The global accessibility based on the mentioned technologies ensures that parties from different jurisdictions can interact seamlessly without needing to navigate multiple disparate systems. By leveraging such trustless environments, parties from different jurisdictions can engage more confidently irrespective of the regulatory, cultural, and operational differences that might

exist between them.

However, each distributed ledger system adds layers of complexity to cross-chain interactions with its unique consensus mechanism, governance model, and technical infrastructure. This complexity could lead to bottlenecks, increased transaction costs, and potential points of failure, undermining the very efficiencies blockchain technology seeks to offer. Interoperability solutions require some level of trust in bridging protocols or intermediary chains, which could become prime targets for attacks. The more complex and interconnected the ecosystem, the larger the attack surface becomes. The potential for exploits, hacks, and fraud increases exponentially with each added layer of interoperability, especially when dealing with permissioned blockchains that may have differing security standards or vulnerabilities.

4. Existing Studies

In the literature, many studies exist regarding the theoretical and technical framework of interoperability issues and solutions of DLTs. Especially architectures like sidechain, notary scheme, relay chain, parachain, rollups and critical technical features like atomic swap, hash-time locked smart contracts are well-studied and developed. Financial utilities like asset transfer are analyzed. But the implications other than Cosmos and Polkadot are not analyzed yet. More comparative and empirical approaches are required as the interoperability developments have been accelerated exponentially for the last two years and the new solutions are evolving into hybrid architectures and applications.

Zilnieks and Erins (2023) investigate the role of cross-chain bridges in standardizing DLT within payment systems, which could be crucial in creating a more efficient financial landscape. Yin, Xu, and Zhang (2023) focus on an efficient cross-chain trading protocol named Interopera, aiming to enhance the trading processes across different blockchain systems. Zamyatin et al. (2021) present a systematic approach to cross-chain communication (CCC) by laying out foundational work for future CCC protocols which is critical for interoperable financial smart contracts. Sober et al. (2023) examine protocols for decentralized cross-blockchain asset transfers, emphasizing transfer confirmation to maintain asset integrity. Robinson and Ramesh (2021) discuss General Purpose Atomic Cross-chain Transactions (GPACT) that facilitate synchronous operations across Ethereum blockchains, the concept is becoming vital for complex financial transactions. Ren et al. (2023) provide a comprehensive survey on blockchain interoperability by categorizing current solutions and addressing the performance of some approaches. Pourpouneh et al. (2023) propose an Automated Market Maker framework for cross-chain on-chain finance, using a lock-swap mechanism to enhance AMM functionality in a sharded blockchain context. Pillai et al. (2023) explore the trade-offs between security and performance in blockchain interoperability, which impacts the decentralization and integrity of blockchain systems. Pfister, Kannengießer, and Sunyaev (2022) discuss the balance between technical and political decentralization in token economies and the role of cross-ledger interoperability. Monika and Bhatia (2024)) suggest a decentralized asset transfer protocol for blockchains, emphasizing transaction finality and preventing asset loss during transfers. Miyaji and Yamamoto (2024) propose an efficient cross-chain communication protocol to reduce data storage and transmission requirements. Ming et al. (2024) explore the fusion protocol's cross-chain and interoperation methods, focusing on relay-chain technology and universal digital wallet concepts. McCorry et al. (2021) review validating bridges as a scaling solution for blockchains, discussing operational costs and security implications. Mazor and Rottenstreich (2023), an empirical study of cross-chain arbitrage in on-chain finance platforms, analyses the profitability and challenges in blockchain ecosystems. Mars et al. (2023) look into securing cross-blockchain smart contracts, proposing an extension of the Bifröst architecture using a Trusted Execution Environment (TEE). Mafike and Mawela (2023) conduct a literature review on requirements for interoperable blockchain systems, focusing on technical, semantic, legal, and organizational aspects. Madhuri and Nagalakshmi

(2023) introduce a novel blockchain strategy for secure cross-chain transactions, focusing on third-party interference avoidance. Lu et al. (2023) present the CCIO approach for cross-chain interoperability in consortium blockchains, aiming to improve efficiency and security in data exchanges. Llambias et al. (2023) propose a gateway-based interoperability solution for DLT, providing a detailed design and implementation for platform-to-platform interactions. Li, Wu, and Cui (2023) review cross-chain technology, discussing principles, security implications, and innovative solutions for interoperability among blockchains. Lee et al. (2021) propose an atomic cross-chain settlement model for central bank digital currencies (CBDCs), adding an administrator ledger to the system for efficient market management. Lee, Murashkin, Derka, and Gorzny (2022) provide a review of cross-chain bridge hacks, identifying risks and security improvements for these systems. Kotey et al. (2023) offer a systematic review on heterogeneous blockchain-to-blockchain communication, discussing the current state and future research directions. Jnr. et al. (2023) propose a framework for the standardization of DLTs for interoperable data integration in sustainable smart cities. Jiang, Cao, and Wu (2023) address cross-chain asset exchange for metaverse interoperability, proposing a framework considering cyber worlds, interaction mechanisms, and infrastructures. Hei et al. (2022) build the Practical AgentChain system for cross-chain exchanges, highlighting its performance and the role of trading operators and agent contracts. Harris (2023) examines challenges and opportunities for blockchain interoperability, exploring various cross-chain technologies and projects. Han et al. (2023) conduct a survey on cross-chain technologies, proposing a blockchain interoperability architecture to address security and effectiveness issues. Guo et al. (2024) propose a framework for efficient cross-chain token transfers, optimizing performance and validator engagement in blockchain networks. Darshan et al. (2023) introduce an architecture for cross-chain interoperability, emphasizing the integration of private and public blockchains in smart cities. Chen et al. (2024) discuss privacy-preserving multi-party cross-chain transaction protocols, presenting a new signature algorithm for secure and private transactions.

5. Promising Solutions

5.1. LayerZero v2

LayerZero provides an omnichain interoperability protocol designed to enable cross-chain communication and transfers. It aims to be non-custodial and trust-minimized, which aligns with permissionless principles. However, the degree to which it is permissionless can depend on the specific implementation and use case. Developers can send arbitrary data, external function calls, and tokens across chains via LayerZero omnichain while preserving their control over their applications.

5.2. Wormhole

Wormhole is a cross-chain messaging protocol that allows for the transfer of value and information between different blockchains. It is designed to be considerably more decentralized and permissionless. The following potential applications are possible with Wormhole:

1- Cross Chain Exchange: Developers can build an exchange that allows deposits from any Wormhole connected chain and withdrawals from another Wormhole connected chains. This type of use cases increases the accessible liquidity and reduces liquidity fragmentation across different distributed ledger networks.

2- Cross Chain Governance: A group of different consortiums on different networks are able to vote on a combined proposal if they would like to communicate votes cast on a common chain.

3- Cross Chain Game: A game could be built and played on a performant network, and its rewards can be issued on a different network.

5.3. Chainlink Cross-chain Interoperability Protocol (CCIP)

The CCIP is designed to enable secure messaging and token movements across different blockchains. Chainlink's oracle network is permissionless. Any blockchain can connect and use its services. Chainlink CCIP supports three main capabilities:

1- Arbitrary messaging is the ability to send arbitrary data (encoded as bytes) to a smart contract on a different blockchain. The developer can modify and encode any data. Usually, developers use arbitrary messaging to trigger an action on the receiving smart contract, including rebalancing an index, minting a specific non-fungible token, or calling an arbitrary function with the sent data as custom parameters. Developers can encode multiple instructions in a single message, enabling them to orchestrate complex, multi-step, multi-chain tasks.

2- Token Transfer: You can transfer tokens to a smart contract or directly to an externally owned account on a different blockchain.

3- Programmable token transfer is the ability to simultaneously transfer tokens and arbitrary data within a single transaction. This mechanism allows users to transfer tokens and send instructions on what to do with those tokens. For example, a user could transfer tokens to a lending protocol with instructions to leverage those tokens as collateral for a loan, borrowing another asset to be sent back to the user.

Chainlink CCIP enables a variety of financial use cases:

1- Cross-chain lending: Chainlink CCIP enables users to lend and borrow a wide range of crypto assets across multiple on-chain finance platforms running on independent chains.

2- Low-cost transaction computation: Chainlink CCIP can help offload the computation of transaction data on cost-optimized chains.

3- Optimizing cross-chain yield: Users can leverage Chainlink CCIP to move collateral to new on-chain finance protocols to maximize yield across chains.

4- Creating new kinds of dApps: Chainlink CCIP enables users to take advantage of network effects on certain chains while harnessing the compute and storage capabilities of other chains.

5.4. Circle's Cross-Chain Transfer Protocol (CCTP)

USDC is an electronic money token issued by Circle and CCTP is introduced to facilitate the secure and efficient transfer of USDC across various blockchain networks. It employs a burn-and-mint mechanism, ensuring the seamless movement and conservation of USDC's value between supported chains. This protocol aims to enhance the interoperability and capital efficiency of USDC within the on-chain finance ecosystem. While some networks have built-in protocols to transmit data across their constituent blockchains (e.g. Cosmos uses the Inter-Blockchain Communication (IBC) protocol to send information between its appchains), it is not possible for isolated networks, such as Ethereum and Avalanche, to communicate directly. Typical third-party bridges use lock-and-mint bridging and liquidity pool bridging as common methods that require tying up USDC liquidity in third-party smart contracts, resulting in limited capital efficiency and introducing additional trust assumptions. CCTP can be embedded within any app or wallet—even existing bridges—to enhance and simplify the user experience for cross-chain use cases, as a low-level primitive.

How it works:

1- USDC is burned on the source chain: A user initiates a transfer of USDC from one blockchain to another, by using an application. The user specifies the recipient wallet address on the destination chain. The application facilitates a burn of the specified amount of USDC on the source chain.

2- Circle observes and attests to the burn event on the source chain. The application requests the attestation from Circle, which provides authorization to mint the specified amount of USDC on the destination chain.

3- The application uses the attestation to trigger the minting of USDC. The specified amount of USDC is minted on the destination chain and sent to the recipient wallet address.

Developers can build cross-chain applications that stack together the various functionalities of trading, lending, payments, NFTs, and gaming. Users can perform cross-chain swaps with digital assets that live on disparate chains in an automated way. Users never need to switch wallets or even pay attention to which chain the USDC is held. Thus the user is shielded from complexity.

5.5. Polkadot

Polkadot facilitates cross-chain interoperability through its relay chain and parachain architecture. Parachains can be either permissioned or permissionless, depending on their governance structure. The Polkadot network as a whole is designed to be permissionless, allowing for decentralized participation in the network's security and governance. It is allowed to transfer arbitrary data across blockchains. It is possible to build applications that get permissioned data from a private blockchain and use it on a public blockchain. For instance, a school's private academic records chain could send proof to a degree-verification smart contract on a public chain.

5.6. Cosmos

Cosmos is built around the concept of an "internet of blockchains" where each independent blockchain (called zones) can communicate with others via the Cosmos Hub that uses the Inter-Blockchain Communication (IBC) protocol. The Cosmos ecosystem is designed to support permissionless blockchains with the IBC protocol that enables interoperability in a considerably more decentralized manner. Cosmos uses the IBC protocol to send information between its appchains. The IBC is an end-to-end, connection-oriented, stateful protocol for ordered and authenticated communication between heterogeneous blockchains arranged in an unknown and dynamic topology. IBC can be used to build a wide range of cross-chain applications that include token transfers, atomic swaps, multi-chain smart contracts (with or without mutually comprehensible virtual machines), cross-chain account control, and data or code sharding.

6. Comparison

Comparing the interoperability solutions provided by LayerZero, Wormhole, Chainlink CCIP, Circle CCTP, Polkadot, and Cosmos involves examining their approaches to facilitating communication and asset transfer between diverse blockchain ecosystems. The choice among them would depend on the specific needs of the application, including factors like the desired level of decentralization, security, ease of integration, and the types of assets or data being transferred. Here's a summarized comparison:

Feature	Chainlink CCIP	LayerZero	Wormhole	Circle CCTP	Polkadot	Cosmos
Overview	Secure messaging and token movements, leveraging Chainlink's oracle network.	Omnichain protocol for non-custodial, trust-minimized communication.	Decentralized protocol for cross-chain value and information transfer.	Facilitates secure USDC transfer across blockchains using burn-and-mint.	Cross-chain interoperability via relay chain and parachains.	"internet of blockchains" via the IBC protocol for independent blockchains.
Focus	Secure messaging and token transfers.	Omnichain interoperability with an emphasis on non-custodial operations.	Cross-chain messaging for value and data transfer.	Secure and efficient transfer of USDC.	Interoperability through connecting multiple parachains.	Enabling independent blockchains to interoperate.
Nature	Partially permissionless; dependent on oracle and node operators.	Varies by implementation.	Considerably decentralized and permissionless.	Permissionless, promoting broad USDC usability in DeFi.	Parachains can be permissioned or permissionless; decentralized governance.	Supports permissionless blockchains; emphasizes sovereign operations.
Key Features	Established oracle network for cross-chain communication.	Unique endpoints facilitating chain communication, emphasizing user control.	Decentralized attestation model for transaction verification.	Simplifies USDC transfers, enhancing liquidity.	Shared security model across parachains.	Hub-and-spoke model with IBC for blockchain communication.
Financial Benefits	Expands DApps utility and market reach.	Reduces transaction costs and time.	Increases liquidity and market efficiency.	Improves capital efficiency and liquidity for USDC.	Unique financial services on parachains enhancing on-chain financial products.	Promotes on-chain finance innovation and scalability.
Structure	Decentralized network of oracles.	Omnichain connectivity layer.	Decentralized bridge network.	Protocol layer for USDC transactions.	Relay chain with connected parachains.	Hub-and-spoke model with interconnected zones.

Technical Mechanism	Utilizes decentralized oracles.	Ultra-light nodes and off-chain oracles, adjustable security.	Network of validators with multi-signature schemes.	Burn-and-mint mechanism ensuring token supply integrity.	Central relay chain with diverse parachain functions.	Sovereign blockchains exchange data and tokens through IBC.
Feature	**Chainlink CCIP**	**LayerZero**	**Wormhole**	**CCTP by Circle**	**Polkadot**	**Cosmos**
Chain-type	Overlay network on multiple blockchains.	Cross-chain interoperability layer.	Bridge protocol connecting blockchains.	Cross-chain token transfer protocol.	Heterogeneous multi-chain architecture.	Network of independent blockchains.
Consensus or Protocol	Depends on underlying blockchains; uses Chainlink's oracle network.	Utilizes ultra-light nodes and off-chain oracles; varies with implementation.	Utilizes guardian nodes and multi-signature schemes.	Burn-and-mint mechanism; depends on participating blockchains.	Nominated Proof of Stake (NPoS) on the relay chain.	Tendermint consensus algorithm in the Cosmos Hub.
Cross-chain Type	Messaging and token transfer protocol.	Generalized message passing with trustless delivery.	Token and data bridge.	Token transfer focusing on USDC.	Shared security and interoperability between parachains.	Arbitrary message passing between zones.
Limitation	Reliant on oracle integrity; potential node centralization.	Requires specific dApp integration; security dependent on oracles/relayers.	Security risks associated with guardian nodes.	Focused on USDC transfers; reliant on burn-and-mint security.	Scalability limited by relay chain capacity; parachain development complexity.	Initially limited to fast finality chains; expanding to include others.
Vulnerabilities	Reliance on oracle integrity and potential centralization of node operators.	Dependence on off-chain data reliability and endpoint security.	Security of guardian nodes and risk of collusion or compromise.	Security reliant on the burn-and-mint mechanism and integrity of supported chains.	Potential for parachain centralization and relay chain scalability issues.	Risks associated with sovereign chain security and IBC data integrity.

7. Metrics

To show the interest in cross-chain interoperability solutions, some simple statistics are visualized here from the websites of Layerzero and Wormhole.

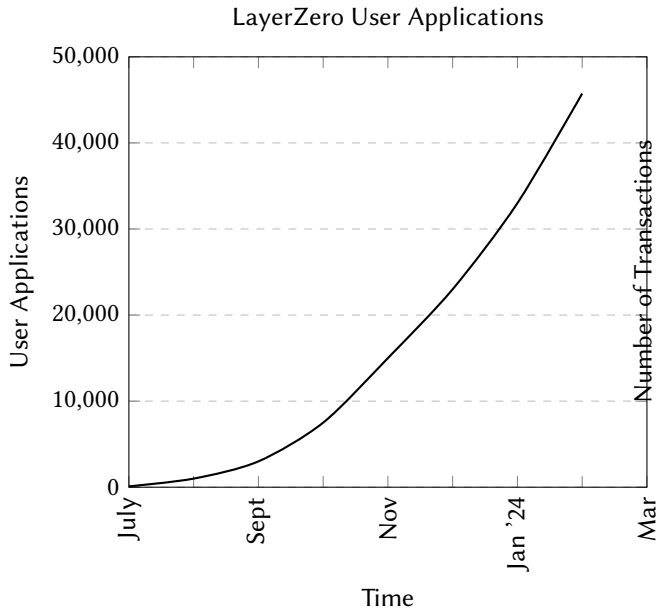

Figure 4: The growth in LayerZero user applications from July 2023 to March 2024.

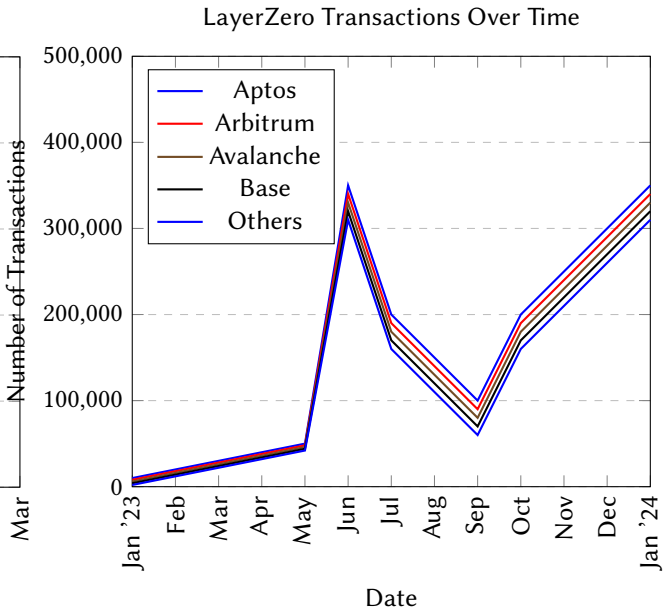

Figure 5: The transaction volume over LayerZero from January 2023 to January 2024.

January 2023 was a pivotal date for LayerZero as the most required omnichain integrations of LayerZero were presented to the users. It is clearly seen in the charts that the interoperability protocol between Ethereum rollups and other pioneering public blockchains has been used with a rising interest. LayerZero has not presented an official product for zk-rollups yet and zero-knowledge-proof technologies have serious impact on scalability recently. So if the upcoming integrations and increasing adoption of this omnichain solution in the industry are taken into account together with the rising trend on the charts, LayerZero and related technologies will have exponential growth statistics hypothetically.

It should be stated that these charts are based on data sourced from LayerZero's website. For a more robust analysis and a deep empirical analysis, detailed transaction data, user engagement metrics, and external market data would be required.

Table 2
Wormhole Cross-chain Total Outflow Transaction Activity from 20 July 2023 to 8 March 2024

Source	% of Total Transactions	Transactions Count
Solana	21.76%	522,416
Polygon	12.68%	304,495
BSC	10.45%	250,794
Arbitrum	8.86%	212,798
Celo	7.11%	170,757
Aptos	5.65%	135,712
Ethereum	5.29%	126,939
Avalanche	5.28%	126,856
Sui	4.58%	109,955
Fantom	4.49%	107,862

Table 3
Wormhole Cross-chain Transactions (Inflow from other chains to Ethereum) from 20 July 2023 to 8 March 2024

Target	% of Total Transactions	Transactions
Solana	65.85%	83,592
Sui	6.99%	8,877
Arbitrum	5.23%	6,643
BSC	4.75%	6,034
Sei	4.19%	5,315
Polygon	2.34%	2,973
Moonbeam	2.04%	2,589
Base	1.86%	2,355
Optimism	1.41%	1,794
Avalanche	0.96%	1,215

Table 4
Wormhole Cross-chain Inflow Volume Activity (From Ethereum to other chains) from 20 July 2023 to 8 March 2024

Target	% of Total Volume	Volume ($)
Sui	52.05%	$1,160,771,342
Solana	29.89%	$666,691,355
Arbitrum	4.32%	$96,415,666
Moonbeam	3.56%	$79,097,428
BSC	1.96%	$43,632,772
Celo	1.95%	$43,464,801
Aptos	1.73%	$38,571,272
Sei	0.82%	$18,295,081
Base	0.62%	$13,777,613
Polygon	0.60%	$13,324,085

Table 5
Wormhole Cross-chain Total Outflow Volume Activity from 20 July 2023 to 8 March 2024

Source	% of Total Volume	Volume ($)
Ethereum	37.20%	$2,230,700,701
Solana	17.90%	$1,072,000,777
Sui	17.15%	$1,026,463,015
Arbitrum	5.44%	$326,304,908
BSC	3.92%	$234,989,757
Moonbeam	2.86%	$171,224,870
Avalanche	2.48%	$148,896,924
Polygon	2.12%	$127,236,585
Aptos	2.02%	$121,036,864
Optimism	1.91%	$114,604,457

These tables show the high volume and usage of another pioneering interoperability solution Wormhole. These visualizations and tables can be a starting point to give an idea for more research like how to structure and analyze the context of DLT interoperability, how to model different scenarios or educational purposes.

8. Conclusion and Future Research

In this paper, we have explored the fundamentals of cross-chain interoperability, the existing literature, pioneering trustless DLT interoperability solutions, their potential role in enhancing financial efficiency, and the comparison or their technical features. Through a comprehensive analysis, we have demonstrated the mechanisms of these solutions to facilitate communication and transaction execution across disparate blockchain networks, eliminating the need for intermediaries and reducing counterparty risks. The adoption of trustless and permissionless interoperability mechanisms has shown promising potential in creating a more inclusive, efficient, and resilient financial ecosystem. By leveraging cryptographic proofs and smart contracts, these solutions ensure security, transparency, and integrity in cross-chain transactions, thus fostering trust among participants in a trustless environment.

For future research on the financial impact of cross-chain interoperability solutions, the following areas are

recommended to both quantitatively and qualitatively analyze based on the insights from the document:

1. Analyzing and measuring the impact of cross-chain communication protocols on any operational costs, financial efficiencies, transaction volumes and operational speed.

2. Contributing to the existing analyses and measures on the hack of cross-chain bridges and interoperability protocols.

3. Examining the challenges and financial implications of executing smart contracts that span multiple blockchain environments, including the issues related to differing virtual machines and programming languages.

4. Contributing to the governance models and audit mechanisms that can support secure and transparent cross-chain interactions, including the role of decentralized autonomous organizations (DAOs) and other forms of governance in managing cross-chain protocols.

5. Studying the design of incentive schemes that encourage participation and maintain the security and efficiency of cross-chain networks, including the implications for transaction fees, staking rewards.

By addressing these areas, future research can contribute to the development of a mature, stable, and efficient cross-chain system, leading to greater value circulation, and innovative FinTech models.

9. References

[1] Anthony Jnr. Bokolo, "Exploring interoperability of distributed Ledger and Decentralized Technology adoption in virtual enterprises," Inf Syst E-Bus Manage, vol. 20, no. 4, pp. 685–718, Dec. 2022, doi: 10.1007/s10257-022-00561-8.

[2] Anthony Jnr. Bokolo, W. Sylva, J. K. Watat, and S. Misra, "A Framework for Standardization of Distributed Ledger Technologies for Interoperable Data Integration and Alignment in Sustainable Smart Cities," J Knowl Econ, Oct. 2023, doi: 10.1007/s13132-023-01554-9.

[3] Michelle Pfister, N. Kannengießer, and A. Sunyaev, "Finding the Right Balance: Technical and Political Decentralization in the Token Economy," in Blockchains and the Token Economy, M. C. Lacity and H. Treiblmaier, Eds. Cham: Springer International Publishing, 2022, pp. 53–86. doi: 10.1007/978-3-030-95108-5_3.

[4] Seth D. Kotey et al., "Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication," IET Communications, vol. 17, no. 8, pp. 891–914, May 2023, doi: 10.1049/cmu2.12594.

[5] Suha Bayraktar and S. Gören, "Design Principles for Interoperability of Private Blockchains," in The International Conference on Deep Learning, Big Data and Blockchain (DBB 2022), vol. 541, I. Awan, M. Younas, J. Bentahar, and S. Benbernou, Eds. Cham: Springer International Publishing, 2023, pp. 15–26. doi: 10.1007/978-3-031-16035-6_2.

[6] Manar A. Talib et al., "Interoperability Among Heterogeneous Blockchains: A Systematic Literature Review," in Trust Models for Next-Generation Blockchain Ecosystems, M. H. U. Rehman, D. Svetinovic, K. Salah, and E. Damiani, Eds. Cham: Springer International Publishing, 2021, pp. 135–166. doi: 10.1007/978-3-030-75107-4_6.

[7] Guzman Llambias, B. Bradach, J. Nogueira, L. González, and R. Ruggia, "Gateway-based Interoperability for DLT," preprint, Feb. 2023. doi: 10.36227/techrxiv.22120520.v1.

[8] Swathi Punathumkandi, V. M. Sundaram, and P. Panneer, "Interoperable permissioned-blockchain with sustainable performance," Sustainability, vol. 13, no. 20, p. 11132, 2021, Accessed: Dec. 24, 2023. [Online]. Available: https://www.mdpi.com/2071-1050/13/20/11132

[9] Senate S. Mafike and T. Mawela, "Requirements for Interoperable Blockchain Systems: A Systematic Literature Review," in The 4th Joint International Conference on Deep Learning, Big Data and Blockchain (DBB 2023), vol. 768, M. Younas, I. Awan, S. Benbernou, and D. Petcu, Eds. Cham: Springer Nature Switzerland, 2023, pp. 41–55. doi: 10.1007/978-3-031-42317-8_4.

[10] Rawya Mars, S. Cheikhrouhou, S. Kallel, M. Sellami, and A. H. Kacem, "Towards a Secure Cross-Blockchain Smart Contract Architecture," in Risks and Security of Internet and Systems, vol. 13857, S. Kallel, M. Jmaiel, M. Zulkernine, A. Hadj Kacem, F. Cuppens, and N. Cuppens, Eds. Cham: Springer Nature Switzerland, 2023, pp. 127–132. doi: 10.1007/978-3-031-31108-6_10.

[11] Babu Pillai, Z. Hóu, K. Biswas, V. Bui, and V. Muthukkumarasamy, "Blockchain Interoperability: Performance and Security Trade-Offs," in Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems, Nov. 2022, pp. 1196–1201. doi: 10.1145/3560905.3568176.

[12] Bo Meng, W. Yibing, Z. Can, W. Dejun, and M. A. Binhao, "Survey on cross-chain protocols of blockchain," Journal of Frontiers of Computer Science Technology, vol. 16, no. 10, p. 2177, 2022, Accessed: Dec. 24, 2023. [Online]. Available: http://fcst.ceaj.org/EN/Y2022/V16/I10/2177

[13] Rita Tsepeleva and V. Korkhov, "Building DeFi Applications Using Cross-Blockchain Interaction on the Wish Swap Platform," Computers (Basel), vol. 11, no. 6, pp. 99-, 2022, doi: 10.3390/computers11060099.

[14] Peter Robinson, Survey of Crosschain Communications Protocols. arXiv, 2021. doi: 10.48550/arXiv.2004.09494.

[15] M. Darshan, M. Amet, G. Srivastava, and J. Crichigno, "An Architecture That Enables Cross-Chain Interoperability for Next-Gen Blockchain Systems," IEEE Internet of Things Journal, vol. 10, no. 20, pp. 18282–18291, Oct. 2023, doi: 10.1109/JIOT.2023.3279693.

[16] Vadims Zilnieks and I. Erins, "Cross-Chain Bridges: A Potential Solution to Standardising Distributed Ledger Technology in Payment Systems," Information Technology and Management Science, vol. 26, no. 1, pp. 27–34, Nov. 2023, doi: 10.7250/itms-2023-0004.

[17] Surisetty Madhuri and V. Nagalakshmi, "A Novel Blockchain Strategy for Third Party Aware Cross-chain Transaction Framework," Wireless Pers Commun, vol. 131, no. 4, pp. 2897–2917, Aug. 2023, doi: 10.1007/s11277-023-10588-w.

[18] Shaofei Lu et al., "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle," Sensors, vol. 23, p. 1864, Feb. 2023, doi: 10.3390/s23041864.

[19] Ryan Zarick, B. Pellegrino, and C. Banister, LayerZero: Trustless Omnichain Interoperability Protocol. arXiv, 2021. doi: 10.48550/arXiv.2110.13871.

[20] Mohsen Pourpouneh, K. Nielsen, and J. B. Gravgaard, Automated Market Makers for Cross-chain DeFi and Sharded Blockchains. arXiv, 2023. doi: 10.48550/arXiv.2309.14290.

[21] Alexei Zamyatin et al., "SoK: Communication Across Distributed Ledgers," in Financial Cryptography and Data Security, 2021, pp. 3–36. doi: 10.1007/978-3-662-64331-0_1.

[22] Patrick McCorry, C. Buckland, B. Yee, and D. Song, SoK: Validating Bridges as a Scaling Solution for Blockchains. 2021. Accessed: Mar. 04, 2024. [Online]. Available: https://eprint.iacr.org/2021/1589

[23] Panpan Han, Z. Yan, W. Ding, S. Fei, and Z. Wan, "A Survey on Cross-chain Technologies," Distrib. Ledger Technol., vol. 2, no. 2, p. 15:1-15:30, Jun. 2023, doi: 10.1145/3573896.

[24] Wenqi Wang, Z. Zhang, G. Wang, and Y. Yuan, "Efficient Cross-Chain Transaction Processing on Blockchains," Applied Sciences, vol. 12, no. 9, p. 4434, Jan. 2022, doi: 10.3390/app12094434.

[25] Michael Sober, M. Sigwart, P. Frauenthaler, C. Spanring, M. Kobelt, and S. Schulte, "Decentralized cross-blockchain asset transfers with transfer confirmation," Cluster Comput, vol. 26, no. 4, pp. 2129–2146, Aug. 2023, doi: 10.1007/s10586-022-03737-6.

[26] Tiancheng Xie et al., "zkBridge: Trustless Cross-chain Bridges Made Practical," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Nov. 2022, pp. 3003–3017. doi: 10.1145/3548606.3560652.

[27] Lokendra Vishwakarma, A. Kumar, and D. Das, "CrossLedger: A Pioneer Cross-chain Asset Transfer Protocol," in 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid), May 2023, pp. 568–578. doi: 10.1109/CCGrid57682.2023.00059.

[28] Ghareeb Falazi, U. Breitenbücher, F. Leymann, and S. Schulte, "Cross-Chain Smart Contract Invocations: A Systematic Multi-Vocal Literature Review," ACM Comput. Surv., vol. 56, no. 6, p. 142:1-142:38, Jan. 2024, doi: 10.1145/3638045.

[29] Hideaki Miyaji and H. Yamamoto, “Efficient cross-chain communication protocol across the blockchain ledgers,” in 2024 IEEE International Conference on Consumer Electronics (ICCE), Jan. 2024, pp. 1–4. doi: 10.1109/ICCE59016.2024.10444248.

[30] Christopher G. Harris, “Cross-Chain Technologies: Challenges and Opportunties for Blockchain Interoperability,” in 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Jul. 2023, pp. 1–6. doi: 10.1109/COINS57856.2023.10189298.

[31] Ori Mazor and O. Rottenstreich, An Empirical Study of Cross-chain Arbitrage in Decentralized Exchanges. 2023. Accessed: Mar. 04, 2024. [Online]. Available: https://eprint.iacr.org/2023/1898

[32] Lingyuan Yin, J. Xu, and Z. Zhang, “Interopera: An Efficient Cross-Chain Trading Protocol,” The Computer Journal, vol. 66, no. 7, pp. 1609–1621, Jul. 2023, doi: 10.1093/comjnl/bxac030.

[33] Gang Wang and M. Nixon, “InterTrust: Towards an Efficient Blockchain Interoperability Architecture with Trusted Services,” in 2021 IEEE International Conference on Blockchain (Blockchain), Dec. 2021, pp. 150–159. doi: 10.1109/Blockchain53845.2021.00029.

[34] Hongyu Guo et al., “A framework for efficient cross-chain token transfers in blockchain networks,” Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, p. 101968, Feb. 2024, doi: 10.1016/j.jksuci.2024.101968.

[35] Peter Robinson and R. Ramesh, “General Purpose Atomic Crosschain Transactions,” in 2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), Sep. 2021, pp. 61–68. doi: 10.1109/BRAINS52497.2021.9569837.

[36] Martin Westerkamp and J. Eberhardt, “zkRelay: Facilitating Sidechains using zkSNARK-based Chain-Relays,” in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), Sep. 2020, pp. 378–386. doi: 10.1109/EuroSPW51379.2020.00058.

[37] Chang Chen, G. Yang, Z. Li, F. Xiao, Q. Chen, and J. Li, “Privacy-Preserving Multi-Party Cross-Chain Transaction Protocols,” Cryptography, vol. 8, no. 1, p. 6, Mar. 2024, doi: 10.3390/cryptography8010006.

[38] Yiming Hei, D. Li, C. Zhang, J. Liu, Y. Liu, and Q. Wu, “Practical AgentChain: A compatible cross-chain exchange system,” Future Generation Computer Systems, vol. 130, pp. 207–218, May 2022, doi: 10.1016/j.future.2021.11.029.

[39] Li Li, J. Wu, and W. Cui, “A review of blockchain cross-chain technology,” IET Blockchain, vol. 3, no. 3, pp. 149–158, 2023, doi: 10.1049/blc2.12032.

[40] Yunyoung Lee, B. Son, H. Jang, J. Byun, T. Yoon, and J. Lee, “Atomic cross-chain settlement model for central banks digital currency,” Information Sciences, vol. 580, pp. 838–856, Nov. 2021, doi: 10.1016/j.ins.2021.09.040.

[41] Babu Pillai, K. Biswas, and V. Muthukkumarasamy, “Cross-chain interoperability among blockchain-based systems using transactions,” The Knowledge Engineering Review, vol. 35, p. e23, Jan. 2020, doi: 10.1017/S0269888920000314.

[42] Idongesit Williams, “Cross-Chain Blockchain Networks, Compatibility Standards, and Interoperability Standards: The Case of European Blockchain Services Infrastructure,” 2020, pp. 150–165. doi: 10.4018/978-1-7998-3632-2.ch010.

[43] Li Ming, S. Wenpeng, L. Ankai, Z. Ziming, and L. Mianchen, “A research on cross-chain and interoperation methods of fusion protocol,” IET Blockchain, vol. 4, no. 1, pp. 18–29, 2024, doi: 10.1049/blc2.12040.

[44] Monika and Rajesh Bhatia, “Cross-blockchain decentralized asset transfer protocol for public blockchains,” International Journal of Communication Systems, vol. n/a, no. n/a, doi: 10.1002/dac.5709.

[45] Gang Wang, Q. Wang, and S. Chen, “Exploring Blockchains Interoperability: A Systematic Survey,” ACM Comput. Surv., vol. 55, no. 13, p. 290:1-290:38, Jul. 2023, doi: 10.1145/3582882.

[46] Kunpeng Ren et al., “Interoperability in Blockchain: A Survey,” IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 12, pp. 12750–12769, Dec. 2023, doi: 10.1109/TKDE.2023.3275220.

[47] Sung-Shine Lee, A. Murashkin, M. Derka, and J. Gorzny, SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks. arXiv, 2022. doi: 10.48550/arXiv.2210.16209.

[48] Fadi Barbàra and C. Schifanella, “MP-HTLC: Enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract,” Concurrency and Computation: Practice and Experience, vol. 35, no. 9, p. e7656, 2023, doi: 10.1002/cpe.7656.