MANTECH Publications

Journal of Blockchain Systems and Smart Contracts
Volume 1, Issue 3, September-December 2025

Interoperability & Cross-Chain Frameworks

Rohan S Kishore[1], Mitali Sharma[2], Anuj Verma[3], Rupesh Dubey[4]

Assistant professor[1], Associate Professor[2, 3, 4]

Department of Crypto Systems and Security

Madurai Kamaraj University – College of Arts & Science

Email ID: *Rohanskishore7@rediffmail.com[1], mitalisharma511@yahoo.com[2], anujverma24@gmail.com[3]*

Abstract

Blockchain technologies have grown rapidly in the last decade, creating many independent chains with unique features and ecosystems. This growth brought a challenge: lack of interoperability between blockchain networks. Without interoperability, blockchains remain isolated siloes that limit data sharing, asset transfer, and coordinated computation. Cross-chain frameworks are emerging solutions to solve the isolation problem. This paper reviews existing interoperability approaches, examines the architectural designs of cross-chain frameworks, compares different techniques, highlights ongoing challenges, and suggests future directions. We also include simple models and tables for clarity. The goal of this paper is to provide a broad understanding for researchers, developers, and industry leaders who want to grasp the core concepts of chain interoperability and evaluate cross-chain frameworks.

Keywords: *Blockchain, Interoperability, Cross-Chain Communication, Smart Contracts, Relays, Bridges, Layer 0, Consensus, Distributed Ledger Technology*

INTRODUCTION

Interoperability in blockchain refers to the ability of different chains to exchange information, transfer value, or communicate state changes without central intermediaries. As blockchain ecosystems expanded — from early single-chain networks like Bitcoin to hundreds of networks such as Ethereum, Polkadot, Cosmos, Solana, and others — the problem of interconnection

became more visible. Without interoperability, users and developers suffer from fragmentation and limited usability.

Cross-chain frameworks provide a structured way to connect these networks and enable secure interaction. They attempt to solve technical challenges including consensus differences, trust assumptions, finality time, and data formats.

This paper reviews the current state of interoperability and compares major cross-chain frameworks. We start by defining interoperability and categorizing its levels, then describe framework designs, and finally provide discussion and outlook.

WHAT IS INTEROPERABILITY? (ELABORATED)

Interoperability in general refers to the ability of different systems, networks, or components to **work together seamlessly**, share information, and perform coordinated functions without friction. In blockchain technology, interoperability is the capability of **distinct blockchain networks to communicate, exchange data, or transfer assets** while maintaining security, consensus, and autonomy.

Blockchain interoperability is essential because most networks were originally designed as **isolated ecosystems**, optimized for their own consensus mechanisms, data structures, and native assets. Without interoperability, users and developers face **fragmentation**, where assets and information are trapped in single chains, limiting innovation and scalability in decentralized applications.

In the blockchain ecosystem, interoperability can be classified into three main types:

Data Interoperability

Definition:

The ability to share and validate data across blockchain networks. This includes sending information such as transaction history, state changes, or off-chain data in a secure and verifiable manner.

Examples:

- **Cross-chain oracles:** Chainlink oracles providing Ethereum price feeds to other blockchains.

- **Supply chain networks:** Data about goods movement on one blockchain being accessible to another for auditing and verification.

Significance:

Data interoperability enables **transparency, auditability, and real-time insights** across multiple blockchain networks without central intermediaries.

Value Interoperability

Definition:

The ability to transfer tokens, cryptocurrencies, or other digital assets from one blockchain to another while maintaining the original asset's value and integrity.

Examples:

- **Wrapped tokens:** Bitcoin wrapped as WBTC on Ethereum allows BTC holders to participate in Ethereum DeFi applications.
- **Cross-chain payment networks:** Sending a stablecoin from Binance Smart Chain to Polygon via a bridge.

Significance:

Value interoperability **unlocks liquidity** across chains, reduces siloed financial ecosystems, and encourages multi-chain decentralized finance (DeFi) solutions.

Functional Interoperability

Definition:

The ability to execute operations or trigger smart contract actions across chains. This goes beyond data or value transfer—it allows **interaction between decentralized applications on different chains**.

Examples:

- **Cross-chain smart contract invocation:** A contract on Ethereum triggers an action on Binance Smart Chain using LayerZero or Axelar protocol.
- **Multi-chain governance:** A vote on one chain influencing decision-making or protocol updates on another chain.

Significance:

Functional interoperability allows **full operational integration** between networks, enabling decentralized apps to be truly multi-chain and interoperable.

Interoperability Layers

It is helpful to conceptualize interoperability in **three layers**, each addressing different aspects of blockchain interaction:

Table 1 – Interoperability Layers

Layer	Description	Example
Data	Shared state or data exchange	Oracle or cross-chain query
Value	Transfer of tokens or assets	Wrapped tokens or bridges
Function	Remote calls triggered across chains	Cross-chain smart contract invocation

The above table shows the basic categorization used in many interoperability frameworks. Data and value interoperability are more common today, while function interoperability is harder due to security and consensus differences.

CHALLENGES IN ACHIEVING INTEROPERABILITY (ELABORATED)

Blockchain interoperability is a complex problem because blockchain networks were originally designed to operate as **independent, trustless systems**. While decentralization and unique consensus rules provide security and autonomy, these same features **complicate cross-chain interactions**. Effective interoperability frameworks must overcome these challenges while maintaining security, efficiency, and usability.

Below, we explore the key challenges in detail:

Diverse Consensus Protocols

Definition:

Different blockchains use distinct consensus mechanisms to achieve agreement on the network state. Examples include:

- **Proof of Work (PoW):** Used by Bitcoin, relies on computational work to validate transactions.
- **Proof of Stake (PoS):** Used by Ethereum 2.0, validators stake tokens to secure the network.
- **Byzantine Fault Tolerant (BFT) protocols:** Used in Tendermint-based chains, providing fast finality.

- **Hybrid or other variants:** Some networks combine PoW and PoS or introduce novel consensus models.

Challenge:

- Cross-chain communication requires verifying state changes from one chain to another.
- The **finality time** differs between chains—PoW may take minutes to confirm blocks, while BFT networks finalize in seconds.
- A transaction deemed "final" on one chain may still be reversible on another, creating **risk of double-spending** or inconsistent state.

Example:

Transferring BTC (PoW chain) to Ethereum (PoS chain) via a bridge requires careful coordination to ensure that the BTC transaction is confirmed irreversibly before minting the corresponding token on Ethereum.

Security Assumptions

Definition:

Each blockchain has its own security model based on assumptions about adversarial behavior, validator honesty, and network conditions.

Challenge:

- When two chains communicate, the **security assumptions may not align**.
- A chain with lower tolerance to adversaries may be more vulnerable when linked to a higher-risk network.
- Cross-chain verification must **prove the authenticity of state changes** without compromising either chain's security.

Example:

- A BFT-based chain assumes fewer than one-third of validators are malicious.
- Linking it to a PoW chain, which assumes economic majority honesty, may require cryptographic proofs to reconcile the differing assumptions.

Data Formats

Definition:

Blockchain networks often store transactions, state, and smart contract data in unique formats. Differences include block structure, hashing algorithms, and serialization methods.

Challenge:

- Interoperability solutions must **translate or map data formats** between chains to ensure correct interpretation.
- Even subtle differences in timestamp, nonce, or block encoding can cause failed cross-chain operations.

Example:

- Ethereum transactions include nonce, gas price, and sender signature.
- Bitcoin transactions have inputs, outputs, and locktime.
- A cross-chain bridge must extract relevant data from each format and ensure consistency during verification.

Trust Dependencies

Definition:

Some interoperability solutions rely on **trusted third parties**, such as custodial bridges, oracles, or centralized validators.

Challenge:

- Introducing trust undermines the **decentralization principle** of blockchain.
- Bridges controlled by a single entity can become targets for attacks, as seen in multiple bridge hacks in recent years.
- Trust assumptions must be minimized or replaced with cryptographic proofs to maintain security and user confidence.

Example:

- A wrapped BTC bridge that relies on a centralized custodian requires trust that the custodian holds the BTC securely.
- Decentralized alternatives use **multi-signature wallets or threshold signatures** to reduce single points of failure.

Additional Challenges

Beyond the main four, other challenges include:

1. **Latency and Performance:** Cross-chain operations can be slower due to verification and consensus differences.
2. **Atomicity of Transactions:** Ensuring that a cross-chain transaction is **all-or-nothing** is difficult without HTLCs or relay mechanisms.

3. **Standardization:** Lack of common protocols, messaging standards, or token formats increases development complexity.
4. **Governance and Upgrades:** Upgrades on one chain may break compatibility with cross-chain frameworks if not coordinated.

Balancing Scalability and Security

Interoperability frameworks must **balance three competing goals**:

- **Security:** Prevent fraud, double-spending, or inconsistent states.
- **Scalability:** Support high volumes of cross-chain transactions without bottlenecks.
- **Decentralization:** Minimize reliance on trusted parties while maintaining efficiency.

Most solutions trade-off one or more aspects. For instance:

- Centralized bridges are fast and scalable but less secure.
- Layer-0 solutions like Polkadot prioritize security and trust minimization but are more complex to scale.

INTEROPERABILITY APPROACHES

Many interoperability solutions exist. We categorize them broadly:

Centralized Bridges

In simple bridges, a trusted operator locks assets on one chain and issues corresponding assets on another. While this works for some use cases, it introduces trust, which many blockchain users want to avoid.

Hashed Time-Lock Contracts (HTLC)

HTLC techniques originated in payment channels, enabling atomic swaps. They create a time window where both sides must complete a transaction or it is rolled back. This allows peer-to-peer exchange without trusted intermediaries.

Relays

In relay systems, a node or set of nodes monitors one chain and relays information to another. The receiving chain must be able to verify the data cryptographically. A relay thus functions like a light client of another chain.

Layer-0 Networks

Layer-0 frameworks, like Polkadot and Cosmos, use a shared base layer or hub that connects multiple blockchains. Each chain (called a parachain or zone) connects to the hub, which governs consensus and message passing.

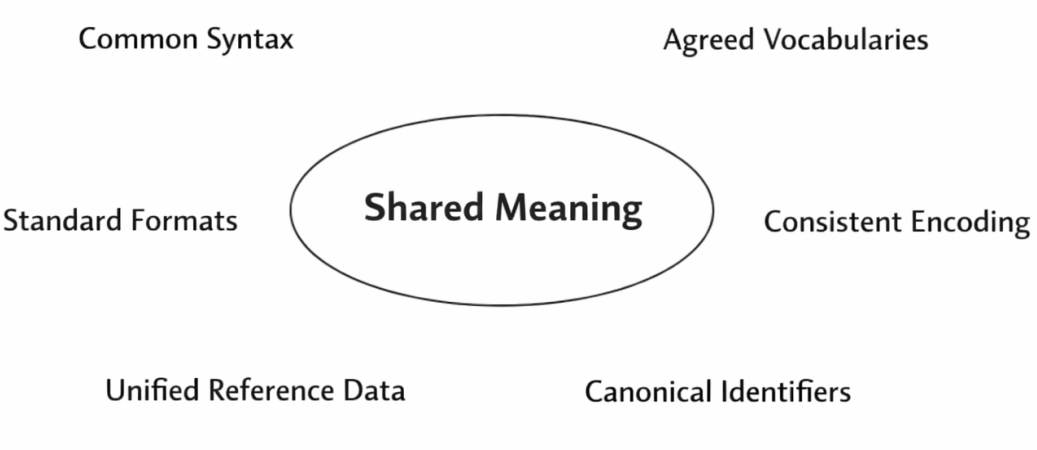

Figure 1 – Layer-0 Interoperability Model (Textual)

The above shows that a central relay/hub coordinates interactions but consensus is shared or unified. This can reduce reliance on external bridges.

Smart Contract Messaging

Some frameworks use special smart contracts on each chain to send and receive messages. These contracts handle verification, event watching, and dispatching instructions based on proof data.

CROSS-CHAIN FRAMEWORKS OVERVIEW

Here we discuss several representative frameworks and how they realize interoperability.

Polkadot

Polkadot uses a **Relay Chain** that maintains consensus and connects diverse parachains. Cross-chain messages are passed through the relay chain. Parachains benefit from shared security and can exchange messages quickly. Polkadot was designed to enable heterogeneous blockchains to interoperate without central bridges.

Cosmos

Cosmos proposes an **Internet of Blockchains** model with a central hub (Cosmos Hub) and zones (independent blockchains). It uses the **Inter-Blockchain Communication (IBC)** protocol. IBC defines a way to send packets between zones with authenticated proofs. Unlike Polkadot, each chain retains full autonomy including its own validator set.

Wrapped Tokens & Bridges

Many ecosystems use wrapped versions of tokens (for example, wrapped BTC on Ethereum). These require custodial or decentralized bridges that lock the original asset and mint a wrapped version on another chain. While common, security remains a challenge.

Cross-Chain Messaging Protocols (XCMP / Celer / LayerZero)

Protocols like **LayerZero**, **Axelar**, **Celer Network**, and others use combinations of relayers and on-chain verification to deliver reliable cross-chain messages. They use oracles, light clients, and specialized contracts.

COMPARISON OF FRAMEWORKS

To better understand difference, we summarize strengths and weaknesses:

Table 2 – Framework Comparison

Framework	Model	Security	Autonomy	Scalability	Trust Assumption
Polkadot	Relay Chain	High	Medium	High	Shared validators
Cosmos-IBC	Hub & Zones	Medium	High	Medium	Light client proof
Wrapped Bridges	Custodial	Low	High	Variable	Bridge operator
LayerZero	Messaging	High	High	High	Oracle + Relayer

APPLICATION USE CASES

Interoperability enables many use cases:

Cross-Chain DeFi

Users can use assets from one chain as collateral on another. For example, BTC from Bitcoin chain can be used in Ethereum DeFi markets via bridges.

Cross-Chain NFTs

NFTs can move across chains, allowing marketplaces to host cross-chain assets.

Multi-Chain Identity & Reputation

User identities and reputation can be shared across decentralized apps on different chains.

Enterprise Supply Chain

Enterprises can track asset movement across multiple blockchain systems used by partners.

SECURITY AND RISK FACTORS

Cross-chain solutions introduce new attack surfaces. Common risks include:

- **Bridge hacks:** Vulnerable bridges have been exploited due to poor multisig or oracle failures.
- **Replay attacks:** Without proper safeguards, an event on one chain may be replayed falsely on another.
- **Economic attacks:** Validators or relayers can be bribed to send false state information.

Framework designers use cryptographic proofs, finality checks, and multi-party signatures to reduce these risks, but tradeoffs exist.

EMERGING TRENDS AND FUTURE WORK

Standardized Messaging Protocols

Efforts are underway to standardize cross-chain message formats. Standardization will reduce fragmentation and improve composability.

Native Light Clients

Chains running native light clients of other chains can verify proofs themselves without external attestations. Progress here will reduce trust assumptions.

Cross-Chain Governance

As interacting chains begin to coordinate governance, networks will need shared decision protocols.

Interoperability as a Service

Software platforms that offer modular cross-chain solutions may grow, similar to web APIs today.

DISCUSSION

While interoperability is improving, challenges remain. True functional interoperability — where contracts can invoke actions across chains natively — is still rare. Many current

solutions focus on value transfer or simple messaging. Also, performance and cost can be issues when bridging high-traffic networks.

Despite these, the industry has made strong progress. Chain-agnostic applications, multi-chain DeFi, and bridges are widely used today. The trend toward layer-0 frameworks and standardized protocols suggests a move to deeper integration.

CONCLUSION

Interoperability is central to the future of blockchain ecosystems. Cross-chain frameworks enable networks to share data, transfer value, and cooperate. This paper reviewed different approaches, including relay-based frameworks, smart contract messaging, wrapped asset bridges, and layered interoperability standards such as Polkadot and Cosmos. We compared models and discussed advantages and risks.

As technology evolves, interoperability will likely improve with standardized protocols, native light clients, and better security practices. While challenges remain, the ecosystem is moving away from siloed chains toward a more connected multi-chain environment.

REFERENCES

1. Buterin, V., "On Interoperability," *Ethereum Research Blog*, 2016.
2. Poon, J. & Dryja, T., "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 2016.
3. Wood, G., "Polkadot: Vision for a Heterogeneous Multi-Chain Framework," *Polkadot Whitepaper*, 2016.
4. Kwon, J. et al., "Cosmos IBC Protocol Specification," *Cosmos Network*, 2020.
5. Wang, H. & Feng, D., "Cross-Chain Communication Protocols: A Survey," *Journal of Blockchain Research*, vol. 2, pp. 33-48, 2021.
6. Zhou, L. & Zheng, Z., "Security Analysis of Blockchain Bridges," *Decentralized Systems Journal*, 2022.
7. Celer Network, "Celer cBridge: Interoperability & Liquidity," *Celer Documentation*, 2023.
8. LayerZero Labs, "LayerZero: Cross-Chain Messaging Protocol," *LayerZero Docs*, 2024.
9. Miller, A. et al., "FlyClient: Super-Light Clients for Lightweight Verification," *Crypto Conference Papers*, 2021.
10. Xu, X. et al., "A Survey on Blockchain Interoperability: Past, Present, Future," *IEEE Access*, 2022.