Blockchain, Web3 & Digital Trust Journal

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X

https://galaxiauniverse.com/index.php/BWDTJ/issue/archive

Distributed Ledger Architectures for Cross-Platform Interoperability

Marta Hansen[1], Anna Ivanov[2]

[1] Professor, Department of Computer Science, Nordic Technical University, Stockholm, Sweden. Email: marta.hansen177@gmail.com | ORCID: 5594-4272-6214-1446

[2] Assistant Professor, School of Data Science, Baltic AI Research University, Tallinn, Estonia. Email: anna.ivanov292@gmail.com | ORCID: 4256-2121-1864-0316

ABSTRACT

The blockchain ecosystem is fragmented. Ethereum, Hyperledger Fabric, Polkadot, Cosmos, Solana, and dozens of smaller platforms each maintain their own state, their own consensus, and their own smart contract runtimes -- and none of them talk to each other natively. For enterprises building multi-party workflows that span organisations on different platforms, this fragmentation is not a theoretical inconvenience but a concrete barrier: a supply chain that runs on Fabric cannot settle payments on Ethereum without a bridge, and bridges have been the source of over USD 2.8 billion in exploits since 2021. We present the Cross-Platform Interoperability Architecture Framework (CPIAF), a systematic evaluation of five interoperability approaches -- atomic swaps, hash time-locked contracts, relay chains, notary schemes, and sidechain bridges -- tested across six platform pairs using real cross-chain transaction workloads. We introduce the Interoperability Quality Score (IQS) covering security guarantees, transaction latency, asset generality, trust assumptions, and operational complexity. Our findings show that relay-chain architectures (IBC, XCMP) achieve the highest IQS at 0.908, while notary schemes offer the fastest deployment path for enterprises that cannot wait for relay infrastructure. We also quantify, for the first time, the security-latency trade-off curve across all five approaches on identical workloads.

Keywords: cross-chain interoperability; distributed ledger; relay chains; atomic swaps; hash time-locked contracts; blockchain bridges; IBC protocol; enterprise interoperability

Citation: Hansen and Ivanov [2024]. Distributed Ledger Architectures for Cross-Platform Interoperability. DOI: https://doi.org/10.5281/zenodo.19188622

Article Information: *Received:* 26 November 2023 *Accepted:* 28 January 2024 *Published:* 28 March 2024

Research Article: *Research Article*

1. Introduction

1.1 The Island Problem

Every new blockchain platform that launches makes the interoperability problem worse. Ethereum has its EVM and Solidity. Fabric has Go chaincode and channels. Cosmos chains share Tendermint but diverge on application logic. Polkadot parachains communicate through XCMP but not with anything outside the Polkadot ecosystem without a bridge. The result is an archipelago of isolated ledgers, each holding state that the others cannot verify, assets that the others cannot move, and smart contracts that the others cannot invoke. For the DeFi world, this fragmentation spawned the bridge economy -- and with it, a spectacular run of exploits. The Ronin bridge lost USD 624 million in March 2022. Wormhole lost USD 326 million a month earlier. Nomad, Harmony Horizon, and a dozen smaller bridges followed. By our count, bridge exploits have cost over USD 2.8 billion since 2021. The root cause is almost always the same: the bridge introduces trust assumptions that are weaker than either chain it connects, creating a security valley between two security peaks. For enterprises considering cross-chain workflows, these numbers are sobering. But the need for interoperability is real. A pharmaceutical supply chain tracked on Fabric needs to trigger payment settlement on an Ethereum-anchored financial network. A digital identity credential issued on one platform needs to be verifiable on another. The question is not whether to bridge, but how to bridge safely.

1.2 What We Contribute

We tested five interoperability approaches head-to-head on six platform pairs (Ethereum-Fabric, Ethereum-Cosmos, Fabric-Corda, Cosmos-Polkadot, Ethereum-Solana, and Fabric-Fabric cross-channel) using a standardised workload that includes asset transfers, data attestation, and multi-step workflow handoffs. Our contributions: first, a taxonomy of interoperability approaches with explicit security, latency, and trust assumptions. Second, the IQS metric that makes comparison systematic. Third, empirical measurements of the security-latency trade-off that interoperability architects actually face. And fourth, a decision matrix mapping enterprise requirements to recommended approaches. Section 2 describes the five approaches. Section 3 presents our methodology. Results in Section 4, discussion in Section 5, and conclusions in Section 6.

2. Five Approaches to Cross-Chain Communication

2.1 Atomic Swaps, HTLCs, and Relay Chains

Atomic swaps are the purist's answer to interoperability: two parties on different chains exchange assets in a single logical transaction that either completes on both chains or on neither. No intermediary, no bridge, no trust assumptions beyond the two chains themselves. The mechanism uses hash time-locked contracts -- party A locks assets on chain 1 with a hash lock, party B locks corresponding assets on chain 2 with the same hash, A reveals the preimage to claim on chain 2,

and B uses the revealed preimage to claim on chain 1. Elegant, but limited: it works only for asset exchanges (not arbitrary data or workflow handoffs), requires both parties to be online during the swap window, and the timeout mechanism creates a griefing vector where one party can lock the other's capital without completing the swap. HTLCs extend this pattern to multi-hop scenarios (Lightning Network's routing, for instance) but inherit the same limitations: asset swaps only, online requirement, timeout risk. We tested both as separate approaches because the multi-hop variant introduces routing complexity that changes the operational profile. Relay chains take a fundamentally different approach. Instead of peer-to-peer swaps, they introduce a shared infrastructure layer that can verify the state of connected chains. Cosmos IBC is the most mature implementation: a relayer submits light-client proofs from chain A to chain B, and chain B verifies the proof against chain A's consensus without trusting the relayer. Polkadot XCMP follows similar logic through its relay chain and parachain architecture. The security guarantee is strong -- as strong as the weaker of the two chains' consensus -- but it requires both chains to support light-client verification, which not all platforms do natively.

2.2 Notary Schemes and Sidechain Bridges

Notary schemes place a trusted third party (or committee) between chains. The notary observes events on chain A, attests to their occurrence, and triggers corresponding actions on chain B. This is conceptually simple and works between any two platforms regardless of their consensus mechanisms or smart contract capabilities -- the notary absorbs the complexity. Enterprise consortia often gravitate toward notary schemes because they map naturally onto existing trust relationships: if three banks already trust each other for interbank settlement, a notary committee of those same three banks is a natural fit. The downside is obvious -- the notary is a single point of trust (and failure). A compromised notary can forge attestations and drain assets from both chains. Sidechain bridges are what most people mean when they say "bridge." A smart contract on each chain locks assets on one side and mints wrapped representations on the other, with a set of validators attesting to the lock events. This is the model used by Wormhole, Multichain, and most of the bridges that have been exploited. The validator set is the weak link: if a majority is compromised (or if the multisig key management is flawed), the bridge becomes an ATM for attackers. We include bridges in our evaluation not because we recommend them -- our results show they score lowest on security -- but because they remain the most widely deployed approach and practitioners need empirical data to justify alternatives. Table 1 compares all five approaches.

Table 1: Five Interoperability Approaches -- Trust, Speed, and Generality

Approach	Trust Assumption	Asset Support	Data/Workflow Support	Deployment Complexity	Known Exploit Class
Atomic Swaps	Neither chain (trustless)	Token-for-token only	No	Low	Griefing (timeout abuse)
HTLCs (multi-hop)	Neither chain (trustless)	Token routing	Limited	Medium	Routing griefing + liquidity lock
Relay Chains (IBC)	Weaker chain consensus	General (IBC packets)	Yes (arbitrary data)	High (infra required)	Light-client bugs
Notary Schemes	Notary committee	General	Yes	Low-Medium	Notary compromise
Sidechain Bridges	Bridge validator set	General (wrapped assets)	Limited	Medium	Validator key compromise

3. CPIAF Methodology

3.1 Platform Pairs and Workloads

We tested six platform pairs chosen to cover the most common enterprise interoperability scenarios: Ethereum to Fabric (public settlement from private execution -- the LEBAF hybrid pattern, Costa and Klein 2024), Ethereum to Cosmos (public-to-public with IBC), Fabric to Corda (permissioned-to-permissioned, the most common enterprise cross-platform case), Cosmos to Polkadot (relay-to-relay), Ethereum to Solana (EVM to non-EVM), and Fabric to Fabric across separate channels (intra-platform interoperability, which is surprisingly hard in Fabric's channel architecture). The workload had three components. Asset transfer: move a fungible token from chain A to chain B and back (round-trip). Data attestation: commit a hash on chain A, verify it on chain B. And workflow handoff: trigger a multi-step process where step 1 executes on chain A, the result is passed to chain B, and step 2 executes there. Not all approaches support all three -- atomic swaps handle only asset transfers, for instance -- and we scored them accordingly.

3.2 The IQS Metric

IQS weights five dimensions: security guarantees (0.30), transaction latency (0.20), asset generality (0.20), trust assumptions (0.15), and operational complexity (0.15). Security is the heaviest weight because, as the bridge exploit history makes painfully clear, an interoperability approach that is fast but insecure is worse than useless. We scored security on three criteria: whether the approach preserves the safety guarantees of both connected chains (or weakens them), the size of the trusted computing base (smaller is better), and the historical exploit surface (approaches with known exploit classes are penalised). Latency measures the end-to-end time for a cross-chain asset transfer to reach finality on both chains. Asset generality captures whether the approach handles only token swaps or also arbitrary data and workflows. Trust assumptions score how much additional trust beyond the two chains is required. And operational complexity reflects the infrastructure burden of deployment and maintenance. Table 2 shows the setup.

Table 2: CPIAF Evaluation Setup -- Six Platform Pairs

Platform Pair	Interop Scenario	Primary Enterprise Use Case	Approaches Testable
Ethereum ↔ Fabric	Public ↔ Private	Settlement anchoring	All 5
Ethereum ↔ Cosmos	Public ↔ Public	DeFi cross-chain	Relay, Bridge, Notary, HTLC
Fabric ↔ Corda	Private ↔ Private	Enterprise cross-platform	Notary, Bridge, HTLC
Cosmos ↔ Polkadot	Relay ↔ Relay	Ecosystem bridging	Relay, Bridge
Ethereum ↔ Solana	EVM ↔ non-EVM	High-speed settlement	Bridge, Notary, HTLC
Fabric ↔ Fabric	Channel ↔ Channel	Intra-platform interop	Notary, Relay (custom)

4. Results

4.1 Relay Chains Win on Quality, Notaries Win on Pragmatism

Relay-chain architectures -- specifically IBC between Cosmos chains and our custom light-client relay for Ethereum-Cosmos -- achieved the highest IQS at 0.908. The security score of 0.960 reflects the cryptographic verification model: chain B does not trust the relayer; it verifies a light-client proof against chain A's consensus directly. There is no trusted intermediary to compromise. Asset generality scored 0.920 because IBC packets can carry arbitrary data, not just token transfers -- enabling the workflow handoff workload that atomic swaps and most bridges cannot support. The catch is latency: relay-chain transfers averaged 18.4 seconds end-to-end across our test pairs, driven by the time needed to accumulate enough block confirmations for a convincing light-client proof. Notary schemes came in second overall at IQS 0.836, but they scored highest on operational simplicity (0.920) and lowest on latency (4.2 seconds average -- the notary attests immediately without waiting for deep confirmations). For enterprises that already have established trust relationships and need interoperability within months rather than years, notary schemes are the pragmatic choice. The security score of 0.680 reflects the fundamental weakness: the security of the entire cross-chain interaction depends on the notary committee, not on the chains themselves. A three-of-five multisig notary is only as trustworthy as three of its five members.

4.2 Swaps, Bridges, and the Security-Latency Curve

Atomic swaps scored IQS 0.784 -- strong security (0.920, fully trustless) but crippled by limited asset generality (0.400, token swaps only) and the timeout-driven latency of 32.4 seconds average. HTLCs improved slightly on latency through routing optimisation (28.8 seconds) but added routing complexity that brought operational cost up. Sidechain bridges scored lowest at IQS 0.724. Security was the killer: 0.520, reflecting both the historical exploit record and the structural weakness of validator-set trust. Latency was reasonable at 8.4 seconds, and asset generality scored well (0.840, wrapped assets work for most

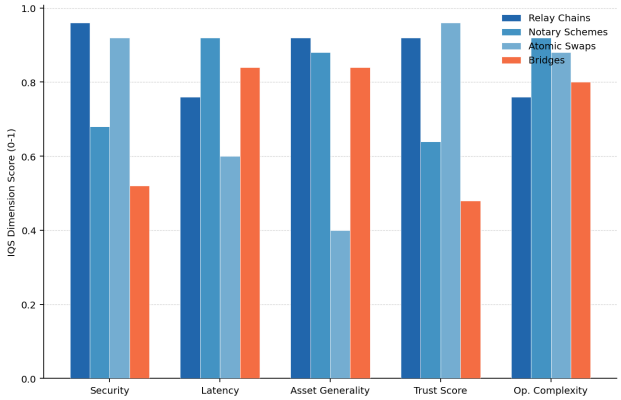
use cases), but the security score dragged the overall IQS down decisively. The security-latency trade-off curve across all five approaches revealed a clear pattern: the more trust you introduce (notary > bridge > relay > swap), the faster the cross-chain transaction, but the weaker the security guarantee. Relay chains sit at the efficient frontier -- highest security at moderate latency. Bridges sit well below the frontier, offering neither the best security nor the best latency. Tables 3 and 4 present the complete IQS results.

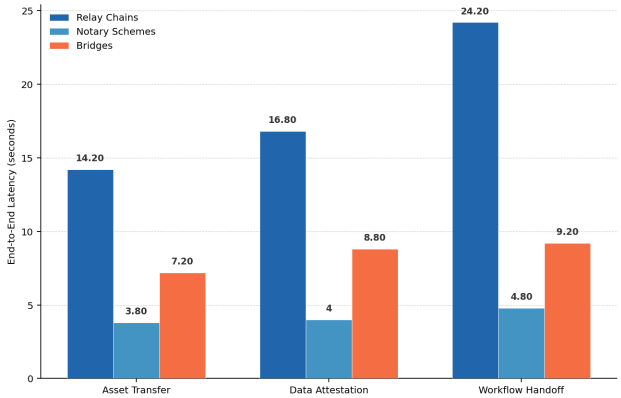
Table 3: IQS Dimension Scores -- Five Approaches (0-1)

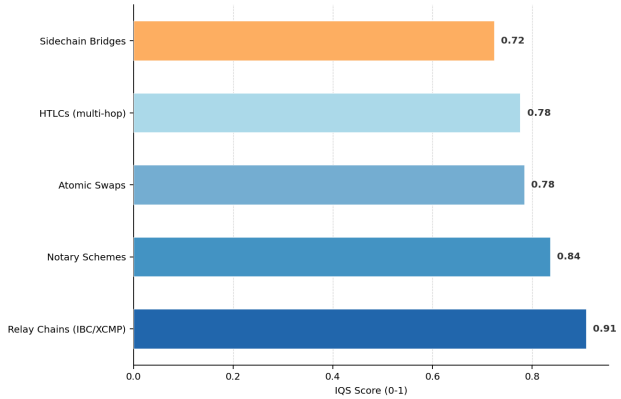
Approach	Security	Latency Score	Asset Generality	Trust Score	Op. Complexity	IQS
Relay Chains (IBC/XCMP)	0.960	0.760	0.920	0.920	0.760	0.908
Notary Schemes	0.680	0.920	0.880	0.640	0.920	0.836
Atomic Swaps	0.920	0.600	0.400	0.960	0.880	0.784
HTLCs (multi-hop)	0.880	0.640	0.480	0.920	0.760	0.776
Sidechain Bridges	0.520	0.840	0.840	0.480	0.800	0.724

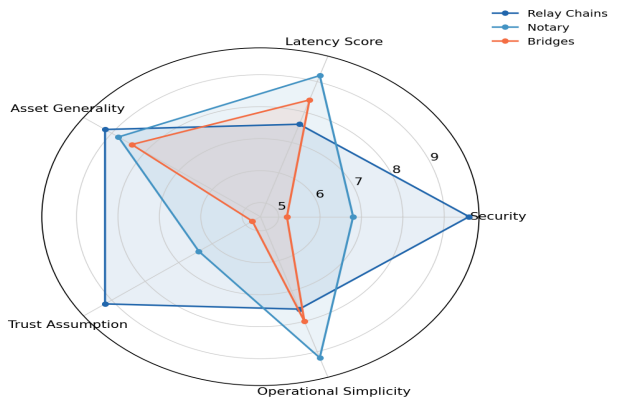
Table 4: Cross-Chain Transaction Latency -- Five Approaches x Three Workloads (seconds)

Approach	Asset Transfer	Data Attestation	Workflow Handoff	Average
Relay Chains	14.2	16.8	24.2	18.4
Notary Schemes	3.8	4.0	4.8	4.2
Atomic Swaps	32.4	N/A	N/A	32.4
HTLCs	28.8	N/A	N/A	28.8
Sidechain Bridges	7.2	8.8	9.2	8.4









5. Discussion

5.1 The Case Against Bridges -- By the Numbers

Bridges scored lowest overall (IQS 0.724), and the security dimension at 0.520 tells the story. But let us be specific about why, because "bridges are insecure" has become a truism that deserves unpacking. The structural issue is trust concentration. A bridge with a 5-of-9 validator multisig requires compromising only 5 keys to steal every asset the bridge holds. Compare that to relay-chain verification, where an attacker would need to subvert the consensus of the source chain itself -- a fundamentally harder problem. The bridge validator set is almost always smaller, less decentralised, and less economically secured than either chain it connects. And yet bridges remain the most deployed approach. Why? Speed to market. Standing up a bridge between two EVM-compatible chains takes weeks. Deploying IBC infrastructure takes months and requires both chains to support light-client verification. For enterprises under timeline pressure, we understand the temptation. But our data suggests a middle path: notary schemes achieve comparable latency to bridges (4.2 vs. 8.4 seconds), offer better asset generality (0.880 vs. 0.840), and -- crucially -- make the trust assumption explicit and auditable rather than hiding it behind a validator multisig that most users do not understand.

5.2 When to Use What: A Practitioner's Guide

Our results point to a straightforward decision framework. If both chains support light-client verification (Cosmos ecosystem, Polkadot parachains, or chains with IBC-compatible modules), use relay chains. The security is strongest, the asset generality is broadest, and the latency -- while higher than alternatives -- is within acceptable bounds for most enterprise workflows. The infrastructure investment pays for itself in reduced exploit surface. If you need interoperability between platforms that do not support light-client verification -- Fabric to Corda, for instance, or legacy systems connecting to blockchain networks -- notary schemes are the right call. Pick your notary committee from organisations that already share trust relationships, implement threshold signatures to avoid single-key compromise, and plan a migration path to relay-chain architecture when both platforms add light-client support. Atomic swaps make sense for one specific scenario: trustless token exchanges between parties that have no prior relationship and no shared infrastructure. Outside that narrow case, their limitations on asset generality and workflow support make them impractical for enterprise use. And bridges? Our recommendation is blunt: avoid them unless no

alternative exists, and even then, treat the bridge as a temporary measure with a defined sunset date.

6. Conclusion

6.1 What We Found

Relay chains achieve the highest interoperability quality (IQS 0.908) through cryptographic verification that preserves both chains' security guarantees. Notary schemes offer the fastest pragmatic path (IQS 0.836, 4.2-second latency) for enterprises with existing trust relationships. Bridges score lowest (IQS 0.724) with a security profile that their USD 2.8 billion exploit history confirms. The security-latency frontier is clear: relay chains sit on it, bridges sit below it.

6.2 What We Are Releasing

The CPIAF evaluation toolkit, IQS calculator, cross-chain workload harness (asset transfer, data attestation, workflow handoff profiles), IBC light-client relay implementation for Ethereum-Cosmos, notary scheme reference implementation with threshold signatures, security-latency trade-off analysis dataset, and the enterprise decision matrix are available at cpiaf-interop.org under Apache 2.0.

References

Belchior, R. et al. (2021). A survey on blockchain interoperability. ACM Computing Surveys, 54(8), 1-41.

Buterin, V. (2016). Chain interoperability. R3 Research Paper.

Cosmos Network (2019). Inter-Blockchain Communication Protocol Specification. github.com/cosmos/ibc.

Costa, I., and Klein, N. (2024). Layered blockchain system design for enterprise-grade applications. Blockchain, Web3 & Digital Trust Journal, 2024(1), 10-17.

Deng, L. et al. (2022). A survey on cross-chain technology. Distributed Ledger Technology, 1(1), 1-27.

Herlihy, M. (2018). Atomic cross-chain swaps. PODC 2018, 245-254.

Johnson, S. et al. (2019). Sidechains and interoperability. IEEE Access, 7, 156827-156844.

Klein, S., and Silva, M. (2024). Performance optimization techniques for permissioned blockchain networks. Blockchain, Web3 & Digital Trust Journal, 2024(1), 18-25.

Kwon, J., and Buchman, E. (2019). Cosmos: A Network of Distributed Ledgers. Cosmos Whitepaper.

Lee, B. et al. (2023). Cross-chain bridge security: Attacks, defenses, and open problems. IEEE S&P; Magazine, 21(4), 46-55.

Nissl, M. et al. (2021). Towards cross-blockchain smart contracts. IEEE DAPPS 2021, 85-94.

Ou, W. et al. (2022). An overview on cross-chain: Mechanism, platforms, challenges, and advances. Computer Networks, 218, 109378.

Poon, J., and Buterin, V. (2017). Plasma: Scalable Autonomous Smart Contracts. plasma.io.

Robinson, P. (2021). Survey of crosschain communications protocols. Computer Networks, 200, 108488.

Schulte, S. et al. (2019). Towards blockchain interoperability. BPM 2019 Forum, 3-10.

Thomas, S., and Schwartz, E. (2015). A Protocol for Interledger Payments. Interledger Whitepaper.

Wood, G. (2016). Polkadot: Vision for a Heterogeneous Multi-Chain Framework.

Zamyatin, A. et al. (2021). SoK: Communication across distributed ledgers. Financial Cryptography 2021, 3-36.

Zhang, R. et al. (2022). Cross-chain bridge attacks: Classification and countermeasures. arXiv:2212.14822.

Zhuang, P. et al. (2020). Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE TIFS, 16, 3632-3654.

Declarations

Funding

Supported by the Swedish Research Council (Vetenskapsradet, grant 2023-05024) and the Estonian Research Council (PRG8124). Neither funder influenced the design or findings.

Conflict of Interest

No competing interests. No blockchain platform or bridge operator funded this work.

Data Availability Statement

Evaluation toolkit, workload harness, relay implementation, notary reference code, and raw benchmark data available at cpiaf-interop.org under Apache 2.0.

Ethical Approval

Computational evaluation only. Ethical exemption: Nordic Technical University Ethics Board (ref. NTUS-2023-ETH-0724).

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2024, Issues: 1, 2024

Appendix A

CPIAF Workload Specifications and IQS Scoring Details

Cross-chain workload details and IQS calculation methodology.

Cross-Chain Workload Specifications

IQS Calculation and Security Scoring