KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Settlement Layer Connecting Sovereign Financial Networks

What the 2025 loss data reveals about the infrastructure enabling CBDCs, stablecoins, and cross-border settlement

CROSS-CHAIN BRIDGE SECURITY SERIES

March 2026

The next generation of financial infrastructure—CBDCs, continental payment rails such as PAPSS, multi-currency settlement platforms such as mBridge, tokenised asset systems—shares a common architectural requirement: value must move across independent networks that operate under different rules, different governance structures, and different consensus mechanisms.

The infrastructure enabling this movement is known as a **bridge**. It functions, in effect, as the settlement layer connecting sovereign financial networks—analogous to the role SWIFT and correspondent banking play in connecting sovereign currency systems, but operating across a new class of digital financial architecture.

The loss data associated with this infrastructure warrants attention independent of any direct exposure to digital assets. Cross-network financial infrastructure documented approximately **$4 billion** in losses during 2025 alone. These are not isolated incidents in a peripheral market; they represent stress tests of the same settlement architecture that institutions are now deploying for regulated stablecoin infrastructure, CBDC interoperability, and cross-border payment settlement.

Source: Hacken 2025 Yearly Security Report; Chainalysis 2026 Crypto Crime Report

How Cross-Network Settlement Works

The settlement mechanic is structurally familiar to anyone who has worked with custodial or escrow arrangements. An asset held on one network cannot move natively to another operating under different rules—the same way a payment instruction in one currency system cannot settle natively in another without an intermediary.

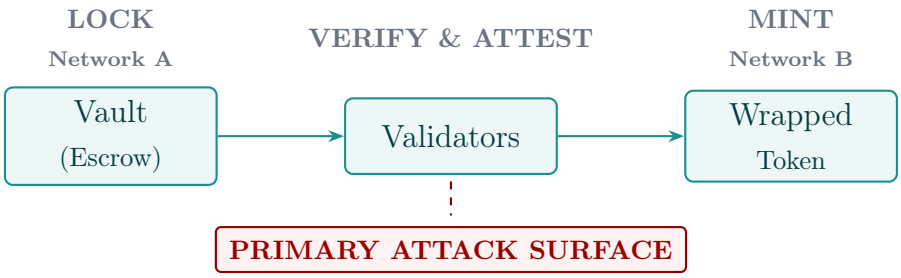

Figure 1: Simplified bridge settlement mechanic. The vault holds the original asset; validators attest to the lock event; a representative token is minted on the destination chain. The validator network concentrates the critical trust.

The original asset is held in the vault while a representative claim circulates on the destination network, redeemable against the original upon return. The critical risk question, as with any custodial arrangement, is who controls the vault — and what happens when that control is compromised.

The Risk Architecture

Individual blockchains achieve security through massive distribution. Bitcoin's network comprises thousands of mining operations globally; compromising it requires controlling more than half of the entire network's computing power—an undertaking that is, for practical purposes, infeasible.

Bridges operate under fundamentally different constraints. Most are secured by a small group of **5 to 21 validators** — the range across widely deployed configurations. If an attacker can compromise a sufficient threshold—in some configurations, as few as three out of five—they can authorise fraudulent transactions and drain the vault.

> *The structural analogy is dual-control treasury access: the broader institution may have robust perimeter controls, but if an attacker compromises the specific individuals holding authorisation keys, access is complete.*

The 2025 data confirms a significant shift in attack methodology. Bridge-specific code exploits have declined to historic lows. The threat has migrated to operational infrastructure—validator keys obtained through targeted phishing, supply chain compromise, or direct infrastructure breach. For institutions with AML obligations, a further dimension warrants attention: bridge infrastructure has become the preferred post-theft laundering channel for state-sponsored actors, with Chainalysis attributing the majority of 2025 stolen assets to DPRK-affiliated actors using bridges as their primary opacity mechanism.

The Bridge Trilemma

An intuitive response is to suggest that bridges should simply use thousands of validators, replicating the decentralisation model that makes individual blockchains secure. The reasoning is sound in principle but encounters structural obstacles in practice.

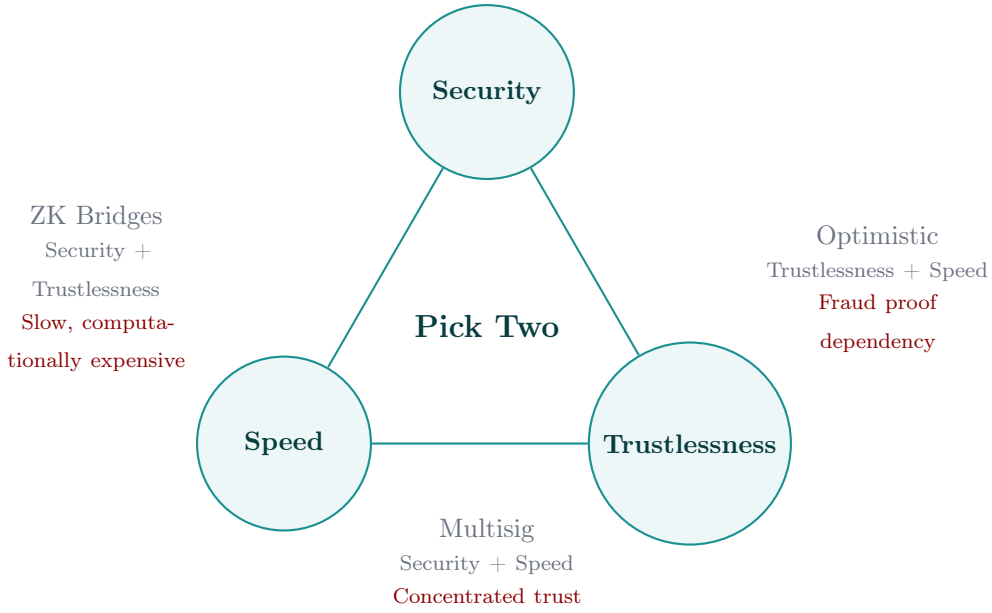

Figure 2: The bridge trilemma: security, speed, and trustlessness are not simultaneously achievable. Current bridges accept managed trust concentration as a necessary trade-off for operational viability.

Performance collapses at scale: requiring even a fraction of a large validator set to participate in every bridge transaction creates communication overhead that makes real-time settlement impossible. Economic centralisation emerges organically—only well-resourced operators can maintain infrastructure across multiple networks, recreating concentration through market dynamics rather than architectural choice.

The result is a fundamental constraint. The question is not whether to accept trust concentration, but how to manage the residual risk it creates.

> *The 2025 loss data suggests that current approaches to managing this residual risk are not adequate. The next article in this series examines the specific attack surface that trust concentration creates.*

Sources: Hacken, "2025 Yearly Security Report." Chainalysis, "2026 Crypto Crime Report." Quantstamp/Zircuit, "SoK: A Review of Cross-Chain Bridge Hacks," arXiv:2501.03423 (January 2025). G7 Cyber Expert Group, "Financial Sector Roadmap for Quantum Readiness" (January 2026). NIST FIPS 203/204/205 (August 2024).

KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Window for Design Decisions Is Narrowing

Infrastructure deployed today under classical cryptography will require remediation within the decade. The question is whether to incur the cost of post-quantum migration now—when it can be integrated architecturally—or later, when it becomes a retrofit.

Reach out if you are building or evaluating cross-network settlement infrastructure.

Follow for ongoing analysis on bridge security, post-quantum migration, and institutional-grade digital asset infrastructure.

Tswa-wen Pierre-Patrick Banga-Banga

Founder & CEO, Kolm Shield | www.kolmshield.com