KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

Inside the Attack Surface

Validator architecture, economic rationality, and the laundering infrastructure dimension

CROSS-CHAIN BRIDGE SECURITY SERIES

March 2026

The Exposure

Cross-chain bridges concentrate trust in small validator sets—a structural constraint that follows directly from how cross-network settlement works. This piece examines the attack surface that concentration creates: the specific validator architecture patterns, the economic conditions under which attacks become rational, and the laundering dimension that transforms bridges from targets into infrastructure for state-sponsored financial crime.

$2.1B

Access control exploits in 2025

Hacken 2025 Yearly Security Report

~$4B

Total cross-network losses in 2025

Hacken 2025 Yearly Security Report

Access control exploits alone account for ~54% of total losses—the single largest loss category in 2025.

Bridge-specific code exploits reached all-time lows in 2024. The threat migrated: from smart contract vulnerabilities to operational infrastructure compromise, and from direct theft to the systematic use of bridge infrastructure as laundering channels.

Validator Architecture Patterns

The choice of validator architecture determines both the trust model and the attack surface. Three dominant patterns exist in production deployments, each with distinct risk profiles.

	Multisig Threshold e.g., 5-of-9	**PoS Validator Set** 20–100+ validators	**Optimistic** 1-of-N trust
Risk Exposure	HIGH	MEDIUM	LOWER
Attack Vector	Compromise m keys gives full vault access	>66% stake collusion enables fraudulent attestations	Any single honest watcher suffices
Structural Constraint	Key management burden	Attack rational if TVL exceeds stake	7-day delay limits production usability

Table 1: Validator architecture comparison by attack surface. In multisig schemes, attack complexity is a function of threshold; in proof-of-stake systems, a function of collusion economics relative to stake.

Key Compromise and Economic Rationality

Private Key Extraction

The Hacken 2025 data confirms this as the dominant attack vector. Adversaries target validator infrastructure through phishing, supply chain compromise, dependency poisoning, and insider threat pathways. In threshold schemes, compromising m keys provides immediate treasury access. The $2.1 billion in access control losses is consistent with a threat landscape that has shifted decisively from code-level exploitation to operational infrastructure compromise.

The Inverse Security Model

In proof-of-stake bridges, validators controlling more than 66% of stake can collude to sign fraudulent attestations. This creates what amounts to an **inverse security model**: if the bridge treasury exceeds total validator stake, a coordinated attack becomes economically rational. The more value a bridge holds, the greater the incentive to compromise it relative to the cost of the stake at risk. Figure 1 illustrates the dynamic.

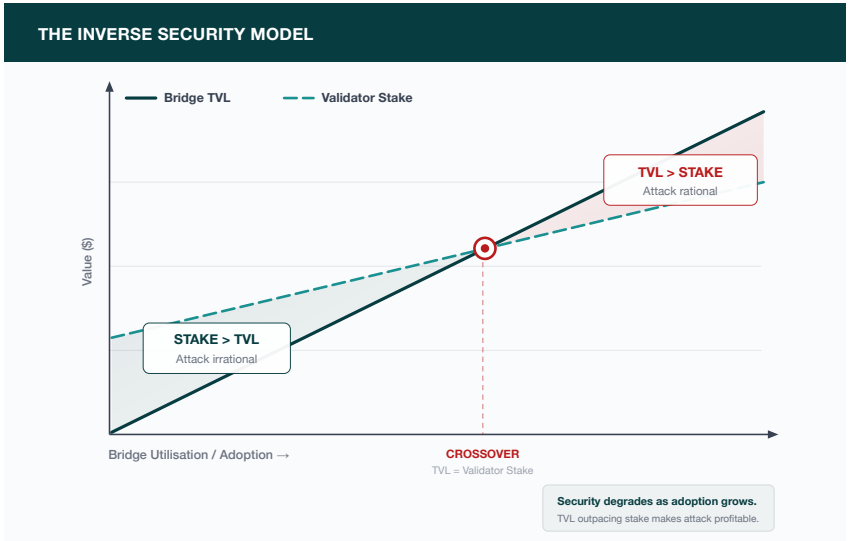

Figure 1: The inverse security model. As bridge utilisation grows, TVL rises faster than validator stake. Beyond the crossover point, the cost of a coordinated attack falls below the potential gain—making exploitation economically rational.

> *Risk professionals will recognise this as a variant of the same dynamic that governs custody concentration risk in traditional finance: as assets under custody grow, the attack surface widens proportionally unless the security architecture scales independently.*

Oracle Infrastructure Attacks

Validators depend on RPC endpoints to observe blockchain state. Sophisticated attacks target this layer—DNS hijacking, BGP routing manipulation, direct RPC provider compromise. By feeding validators false

blockchain state, attackers can trigger fraudulent attestations without any key compromise at all. This category of attack operates entirely outside the cryptographic layer, rendering key management controls and threshold schemes irrelevant. For institutions evaluating bridge counterparty risk, it means that cryptographic hygiene alone is not a sufficient proxy for operational security.

The Laundering Infrastructure Dimension

The Laundering Channel

> **~59%**
>
> Share of 2025 stolen assets attributed to DPRK-affiliated actors, using bridges as their key laundering channel
>
> *Chainalysis 2026 Crypto Crime Report*

A development that emerged in the 2025 data with particular clarity is the role of bridge infrastructure in post-theft laundering. State-sponsored actors demonstrate strong and consistent preference for cross-chain bridges as opacity channels, paying fee premiums for the obfuscation that rapid cross-chain movement provides.

The BIS has identified what it terms a "waterbed effect" in AML/CFT frameworks: tightening controls on intermediated payment instruments—bank deposits, hosted wallets—shifts illicit activity toward non-intermediated alternatives where monitoring obligations are weakest or absent (BIS Papers No. 166, March 2026). Cross-chain bridges function as the operational mechanism through which this shift executes at scale.

The Compliance Dimension

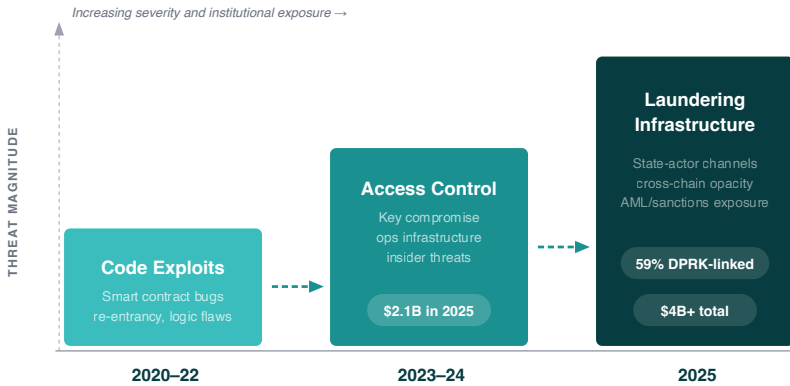

Figure 2: Attack surface migration 2020–2025. The threat has evolved from code-level exploitation through operational compromise to systematic use as state-actor laundering infrastructure.

This transforms the threat model in ways that matter for institutional risk assessment. For institutions with AML and sanctions compliance obligations, the exposure is not hypothetical: correspondent relationships with entities that operate or integrate digital asset settlement layers create indirect risk that regulatory frameworks are now beginning to formalise. The FATF's March 2026 targeted report on stablecoins explicitly identifies cross-chain bridges as the post-theft laundering infrastructure of choice for DPRK-affiliated actors, and treats correspondent exposure to non-compliant virtual asset settlement infrastructure as a material AML/CFT risk for regulated institutions.

The attack surface migration—from code to operations to laundering infrastructure—means that single-layer security models, however sophisticated their individual mechanism, leave significant portions of the threat landscape unaddressed. The evidence points toward multi-layered architectures with post-quantum cryptographic foundations as a baseline requirement for institutional-grade deployment.

Sources: Hacken, "2025 Yearly Security Report." Chainalysis, "2026 Crypto Crime Report." Quantstamp/Zircuit, "SoK: A Review of Cross-Chain Bridge Hacks," arXiv:2501.03423. NIST FIPS 203/204/205 (August 2024). BIS Papers No. 166, "From Cash to Crypto: Towards a Consistent Regulatory Approach to Illicit Payments" (March 2026). FATF, "Targeted Report on Stablecoins and Unhosted Wallets—Peer-to-Peer Transactions" (March 2026).

KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Attack Surface Has Migrated. Security Architecture Must Reflect That.

Access control losses now account for the majority of bridge losses—a shift that single-layer defences cannot address. The next article in this series examines the architectural logic behind multi-layered post-quantum security.

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