KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Independent Failure Domains Doctrine

Cross-chain bridge infrastructure has three independent failure domains. Post-quantum cryptography addresses one

CROSS-CHAIN BRIDGE SECURITY SERIES

March 2026

Two preceding analyses in this series — *The Settlement Layer*, which examined the structural properties of the protocols connecting sovereign financial networks, and *Inside the Attack Surface*, which mapped the validator architecture patterns, economic rationality conditions, and laundering dimension that the 2025 data make visible — have established the problem's shape. The 2025 loss data is consequential: approximately **$4 billion**, with the majority attributable to operational compromise rather than code-level exploits, and with bridge infrastructure serving as both the primary attack target and the preferred laundering channel for state-sponsored actors.

Understanding what an adequate architectural response looks like — and why the category of defence the market currently offers falls short — is the subject of this piece.

In this analysis

The Architectural Logic

The principle informing our approach is not novel. It is borrowed from military and critical infrastructure security doctrine, and it has been standard practice in financial services risk management for decades: **defence in depth**. Multiple independent security layers, each addressing different categories of threat, are collectively far more resilient than any single layer, however sophisticated.

What is novel is the application of this doctrine to cross-chain bridge infrastructure at the protocol level—embedded within the bridge's operational architecture rather than applied as an external monitoring overlay.

External monitoring detects threats after they manifest in observable behaviour; protocol-level integration can intervene at the attestation stage, before fraudulent transactions are finalised — a difference in kind, not degree.

Post-Quantum Cryptography as Foundation

Any bridge security architecture that aims to be durable must address both the **present-day threat** — validator key compromise through phishing, supply chain attacks, and infrastructure breach — and the emerging **quantum threat** that the NIST August 2024 standards and the G7 January 2026 roadmap have now formalised on a documented deprecation schedule.

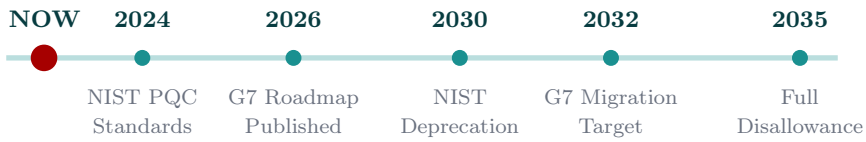

Figure 1: Post-quantum cryptography regulatory timeline. NIST deprecates RSA/ECC in 2030; full disallowance by 2035. The G7 Cyber Expert Group has set 2032 as the target for critical financial system migration.

Kolm Shield's architecture uses post-quantum cryptography aligned with NIST standards as its foundation. The "harvest now, decrypt later" threat means that adversaries may already be recording encrypted validator communications with the intention of decrypting them when quantum computing matures. For institutions whose infrastructure decisions today must remain viable over a ten-year horizon, classical cryptography is a known liability on a documented deprecation schedule.

The cryptographic layer is designed for **crypto-agility**—the ability to swap algorithmic primitives as standards evolve without requiring fundamental architectural changes.

What Post-Quantum Cryptography Alone Cannot Solve

Post-quantum cryptography hardens the cryptographic layer against both current and future threats. It does not address the operational compromise vectors that dominated 2025 losses—coordinated validator compromise, social engineering of key holders, manipulation of the data feeds validators rely upon to assess blockchain state.

> *The Ronin exploit is instructive precisely because the cryptography held. Five of nine authorised key holders were compromised through targeted attacks on operational infrastructure. The vault was opened by people with legitimate credentials — credentials that had been extracted from the legitimate holders. The cryptographic layer was irrelevant to the outcome.*

The same gap applies to the economic structure of bridge security. When a bridge treasury exceeds total validator stake, a coordinated attack becomes economically rational regardless of how robust the cryptographic primitives are. The cryptographic layer verifies the credential, not the intent.

These are fundamentally different categories of threat, and they require fundamentally different categories of defence.

The Doctrine

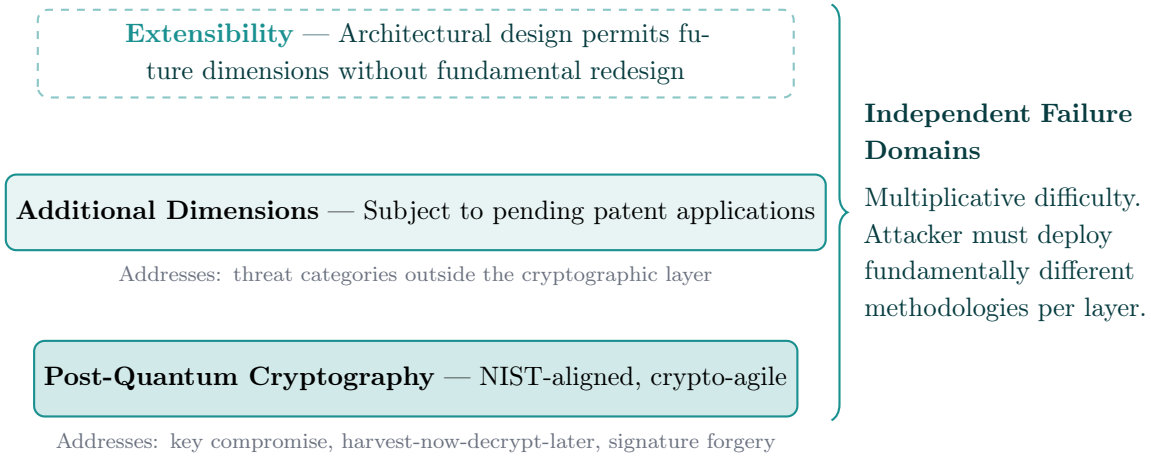

Figure 2: Kolm Shield's layered architecture. Each dimension addresses a distinct category of threat; the difficulty of defeating the system is multiplicative, not additive.

Kolm Shield's architecture addresses these distinct threat categories through independent security dimensions. This is designed so that defeating any single dimension provides no advantage in circumventing the others: the methodologies required are not transferable across layers, and no capability accumulated against one dimension reduces the cost of attacking another. The difficulty compounds.

This is the property that the 2025 loss data makes necessary and that no single-layer solution can replicate by design. An architecture that hardens one category of threat while leaving others structurally unchanged has not reduced the attack surface—it has relocated it. The question for institutional decision-makers is therefore not which layer to prioritise, but whether the architecture in evaluation addresses all three independently.

What This Means for Institutional Decision-Makers

The architecture's independent failure domains do not map onto a single institutional function—they map onto three, each carrying its own regulatory and operational weight.

The **compliance** mandate operates on two distinct timelines. The near-term obligations are already live: FATF's Travel Rule requires demonstrable transactional integrity across chain boundaries, and the Basel Committee's crypto-asset framework introduces capital charge consequences for institutions whose bridge exposure lacks adequate operational controls. The forward obligation is fixed: NIST's deprecation schedule and the G7 Cyber Expert Group's January 2026 roadmap place quantum migration on a regulatory timeline that is now a matter of when, not whether.

The **risk and governance** mandate owns the internal control dimension. Validator collusion and the compromise of authorisation infrastructure are not purely technical failures—they are breakdowns in

the governance structures that boards and audit committees are directly accountable for. The 2025 loss data places these failures squarely within the CRO's ownership, not the CISO's alone.

The **cybersecurity** mandate owns the attack surface in its entirety—across all three threat categories, across both the current and quantum threat horizon.

An architecture that addresses all three independently is therefore not a cybersecurity procurement decision. It is a governance decision with compliance, risk, and cybersecurity implications that converge on the same answer—and that touches three institutional budget holders whose mandates, under current regulatory conditions, are already under pressure.

The Architectural Consequence

Multi-layered architecture delivers a property that no single-layer approach can replicate: **independence between failure domains**. An attacker who defeats the cryptographic layer has gained no capability against the remaining dimensions. The methodologies required are not transferable. This is not a marginal improvement in resilience — it is a structural change in the cost of a successful attack.

The architecture achieves this without requiring wholesale replacement of existing infrastructure. Protocol-level integration embeds these properties within a bridge's operational logic, and crypto-agility ensures that as post-quantum standards evolve, the architecture adapts without fundamental redesign. The security properties compound; the operational disruption does not.

Multi-layered security raises the cost and complexity of successful attack to the point where residual risk becomes manageable for institutional participants — shifting the conversation from binary assessments of *"secure or insecure"* to the more productive question of whether residual risk falls within acceptable parameters for the specific deployment context.

The window for architectural decisions is narrowing. Infrastructure deployed today without post-quantum foundations will require remediation within the decade—at considerably greater cost and operational disruption than building it correctly from the outset. The compliance obligations already in force make that remediation timeline shorter than the quantum threat horizon alone would suggest.

Sources: Hacken, "2025 Yearly Security Report." Chainalysis, "2026 Crypto Crime Report." G7 Cyber Expert Group, "Financial Sector Roadmap for Quantum Readiness" (January 2026). NIST FIPS 203/204/205 (August 2024). NIST IR 8547 (November 2024). Ronin Network post-mortem (March 2022).

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. The next article in this series examines what that architecture looks like in practice: how multi-layered post-quantum security shifts the security-speed trade-off curve, and why the migration calculus favours acting now.

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