KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Institutional Convergence

Four institutional signals — from capital markets infrastructure, central bank experimentation, macrofinancial research, and payments analytics — are converging on the same conclusion about cross-network security

KOLM SHIELD ANALYSIS

April 2026

The previous four analyses in the *Cross-Chain Bridge Security Series* examined the problem from the vantage point of the protocols themselves: what the settlement architecture looks like, where the attack surface sits, why independent failure domains matter, and what multi-layered security changes in production terms. Those analyses remain current and the conclusions hold.

What has changed in the intervening weeks is the institutional context surrounding them. Four publications released between February and March 2026 — from substantially different vantage points and with no coordination between them — have arrived at conclusions whose combined weight shifts the institutional calculus around cross-chain security — from a protocol-level engineering concern to a question that sits on the agenda of capital markets infrastructure decision-makers.

In this analysis

The Infrastructure Signal

In February 2026, DTCC, Clearstream, Euroclear, and Boston Consulting Group published a joint white paper on digital asset securities interoperability — the second in a collaborative series that began with the Digital Asset Securities Control Principles (DASCP) in 2024. The significance lies less in any single recommendation than in the collective institutional weight behind the analysis: these are the organisations that operate the settlement infrastructure through which the majority of global securities transactions are finalised.

Their central conclusion is direct. Without interoperability, digital asset securities remain trapped in isolated pools, operational costs stay elevated, and both regulatory and operational risk compound as volume increases. The paper identifies 29 interoperability building blocks across five capital market foundations — assets and liabilities, ownership recognition, asset lifecycle and movement protocols, ledgers, and legal and regulatory compliance — and maps them against settlement, custody, collateral management, and asset lifecycle use cases.

For the purposes of this analysis, two findings warrant particular attention.

> **Cross-DLT protocol security is identified as a critical building block for every use case examined.** The paper notes that without robust cross-DLT protocols, blockchains remain isolated, partial or failed transfers create unbacked tokens or frozen assets, and double-spend exploits can capitalise on lags between chains. Bridge-specific vulnerabilities are cited explicitly as a major risk vector.

> **The operating model is evolving into a network-of-networks.** The paper concludes that no single ledger will dominate, and that the future architecture will require standards, gateways, and regulated service providers linking on-chain assets to off-chain finance. This is the operating environment that any cross-network security architecture must be designed for — one in which interoperability is structural rather than optional, and the number of ledger-to-ledger boundaries scales with adoption.

The paper also identifies the responsibility gap that current bridge architectures leave unresolved. Novel roles — bridge operators, oracle providers, relay networks — lack the licensing, oversight, and liability frameworks that traditional financial market intermediaries operate under. The authors call for clear assignment of intermediary responsibilities and obligations, with defined SLAs and liability structures, as a condition for institutional-grade cross-network operations.

Experimental Validation: Bank of Canada Project Samara

The DTCC framework identifies interoperability risks at the analytical level. A separate initiative — Project Samara, published by the Bank of Canada in March 2026 in collaboration with RBC Capital Markets, TD Securities, and Export Development Canada — encountered those same risks experimentally.

Project Samara tested end-to-end DLT-based bond issuance, secondary trading, and lifecycle management using a tokenised CAD-denominated bond settled in wholesale central bank digital money on Hyperledger Fabric. The experiment achieved T+0 atomic settlement through smart contracts and interledger protocols — and in doing so, documented a set of operational risks that map directly onto the security concerns the DTCC paper identifies theoretically.

> **Atomic settlement across independently governed ledgers reduced counterparty and settlement risk but introduced new operational risks** related to key management, auditability, and fallback mechanisms. The experiment found that decentralised architecture created challenges for coordination, reporting, and platform oversight — precisely the categories of vulnerability that single-layer cryptographic security leaves unaddressed.

The overlap is not incidental. The operational risk categories Samara documented — key management, auditability, fallback coordination — are substantively the same categories the DTCC framework identifies as unresolved interoperability building blocks. The analytical and the experimental arrive at the same gap independently.

The Macrofinancial Signal

A separate line of evidence comes from the IMF's March 2026 working paper *Stablecoin Shocks* (WP/26/44), which isolates exogenous stablecoin demand shocks — distinct from broader crypto-driven volatility —

and traces their causal transmission into US financial markets. The contribution matters because it establishes, with conventional econometric rigour, that stablecoin demand is now a measurable channel of asset-market transmission rather than a contained phenomenon within the crypto ecosystem.

The data is specific: a stablecoin demand shock corresponding to a one percent increase in combined market capitalisation lowers the one-month US Treasury bill yield by approximately 1.9 basis points, with the effect persisting and strengthening over roughly 24 weeks. The broad dollar index depreciates modestly. The Bloomberg Galaxy Crypto Index rises, consistent with stablecoin demand facilitating lower-cost access to crypto trading infrastructure.

> *What makes this relevant to the security question is the implication for settlement volume. As stablecoin circulation has grown from under $5 billion in 2019 to over $300 billion by late 2025 — and with credible projections placing it in the $2–4 trillion range by 2030 — the volume of value that must transit cross-network infrastructure is growing at a rate that makes the security properties of that infrastructure a macrofinancial consideration, not merely a technical one.*

The Adoption Trajectory

McKinsey's February 2026 analysis with Artemis Analytics applied granular on-chain transaction classification to separate actual stablecoin payment activity from the trading, internal rebalancing, and automated contract interactions that dominate raw blockchain transaction volumes.

Their adjusted figure is significantly more conservative than headline numbers suggest: approximately $390 billion in annualised true stablecoin payments — roughly 0.02 percent of global payment volumes. The analysis is valuable precisely because it imposes discipline on a dataset that has been routinely overstated. However, two aspects of the underlying data are more consequential than the headline figure.

First, the $390 billion represents a doubling from 2024 levels. B2B payments account for approximately $226 billion of this total and grew over 700 percent year-on-year. The trajectory, rather than the absolute number, is the relevant signal for infrastructure planning.

Second, stablecoin-linked card spending — the most direct interface between stablecoin rails and traditional payment networks — grew from approximately $580 million to $4.5 billion in a single year. This is the category of growth that creates the demand for institutional-grade settlement infrastructure, and the one that places cross-network security on the critical path.

What Converges

Each of these analyses approaches the digital asset landscape from a different institutional vantage point — settlement infrastructure, central bank experimentation, monetary policy transmission, and payment analytics — and none references the others. The convergence is therefore structural rather

than coordinated, which makes the pattern more, not less, significant.

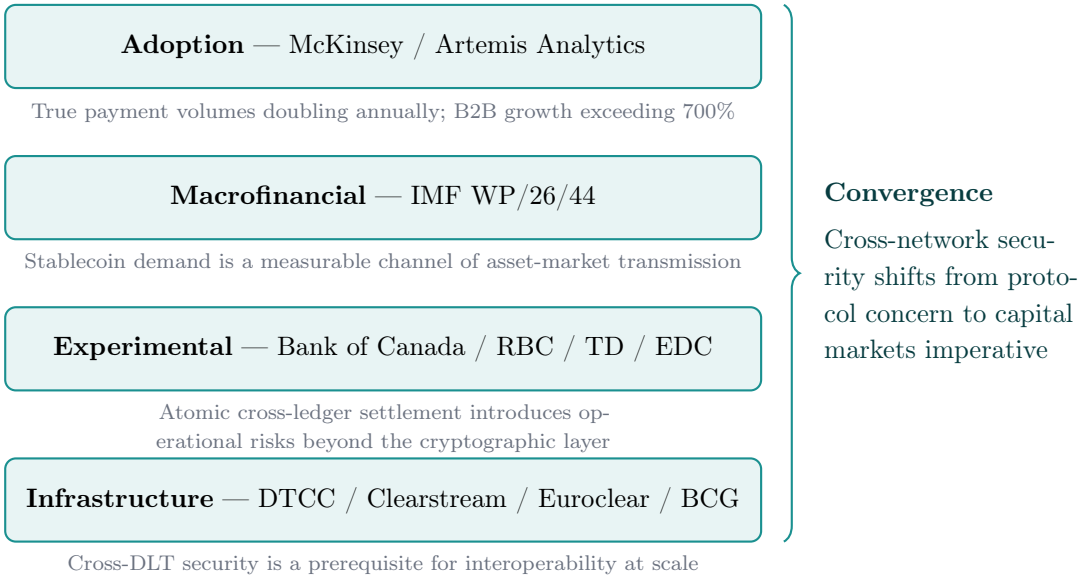

Figure 1: Four independent institutional signals converging on the same conclusion. The security properties of cross-network infrastructure are now a precondition for the adoption trajectory that each analysis documents.

The institutional infrastructure providers have identified what needs to be interoperable. A G7 central bank has experimentally confirmed the operational risks that interoperability introduces at the cross-ledger boundary. The IMF has demonstrated that the financial instruments flowing through that infrastructure are now large enough to generate measurable effects on sovereign debt markets. And the McKinsey data shows that the payment volumes — modest in absolute terms — are growing at a rate that makes today's infrastructure decisions consequential for the next decade's operational reality.

What connects all four is the security layer. Interoperability without adequate cross-network security produces the exact failure modes that the DTCC paper catalogues and that Project Samara encountered experimentally: partial transfers, key management vulnerabilities, coordination failures across independently governed ledgers. The volume trajectory that McKinsey documents ensures these failure modes will be tested at increasing scale. And the macrofinancial transmission channel the IMF identifies means that when failures occur, the effects will not be contained within the crypto ecosystem.

Implications for Security Architecture

For institutions evaluating infrastructure decisions in this environment, the convergence produces a specific set of requirements that the earlier *Cross-Chain Bridge Security Series* addressed from the protocol perspective and that can now be restated in institutional terms.

The security architecture that bridges cross-network settlement must satisfy three properties simultaneously: it must be cryptographically durable across the post-quantum migration timeline documented in the G7's January 2026 roadmap; it must address the operational compromise vectors that drove the

majority of the approximately $2.9 billion in cumulative bridge losses since 2021; and it must do so without introducing latency that renders the infrastructure commercially unviable for the settlement use cases that the institutional demand now requires.

No single-layer approach satisfies all three. This was the conclusion of the *Independent Failure Domains Doctrine* in this series, and it is the conclusion that the institutional evidence published since then reinforces from four independent directions.

The Procurement Consequence

The convergence documented here changes the nature of the decision. When the security gap was identified only at the protocol level, it could be treated as a technical procurement item — owned by the CISO's team, evaluated against a cybersecurity budget line. The institutional evidence now available — from FMI operators, a G7 central bank experiment, the IMF, and independent payments analytics — places it simultaneously within the compliance mandate (regulatory migration timelines), the risk and governance mandate (operational compromise accountability), and the cybersecurity mandate (attack surface ownership). The architecture selected must satisfy all three, and the evaluation therefore cannot sit with any one of them alone.

The window described in the preceding series has not changed. The institutional evidence base surrounding it has.

Sources: DTCC, Clearstream, Euroclear, and BCG, "Building the Path Towards Digital Asset Securities Interoperability" (February 2026). Bank of Canada, "Project Samara Research Paper," Staff Analytical Paper 2026-8 (March 2026). IMF Working Paper WP/26/44, "Stablecoin Shocks" (March 2026). McKinsey and Artemis Analytics, "Stablecoins in Payments: What the Raw Transaction Numbers Miss" (February 2026). 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).

KOLM SHIELD | Quantum-Resistant Security for Financial Infrastructure

The Evidence Base Has Shifted. The Architecture Question Has Not.

DTCC, Clearstream, Euroclear, the Bank of Canada, the IMF, and McKinsey have each — through independent work published in Q1 2026 — identified cross-network security as a precondition for the institutional adoption trajectory now underway.

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