



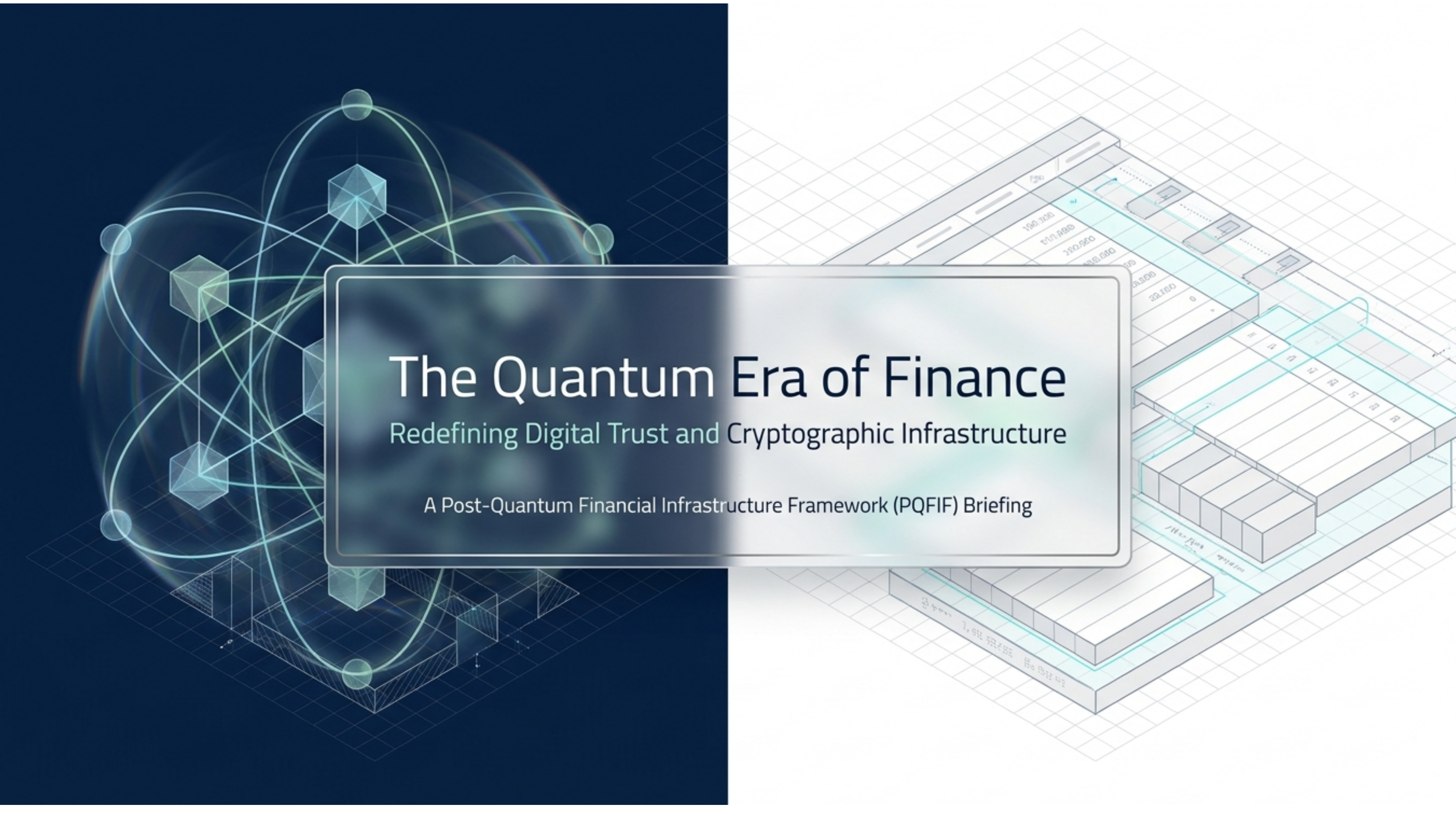
AI-Driven Cybersecurity for
Financial Service Providers

Learning Center

Tutorial 2 | The Quantum Era of Finance

Redefining Digital Trust and Cryptographic Infrastructure

A post-Quantum Financial Infrastructure Framework (PQFIF) Briefing

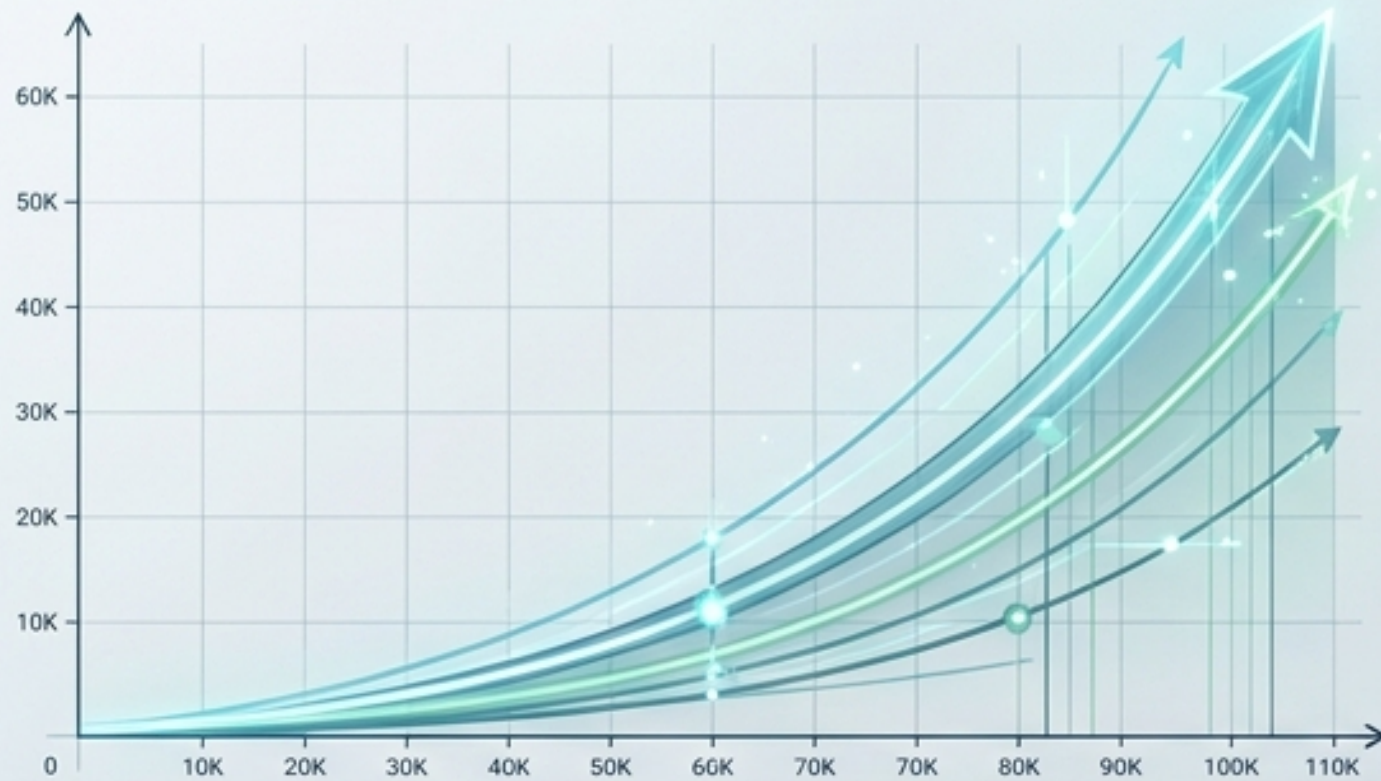


The Quantum Era of Finance

Redefining Digital Trust and Cryptographic Infrastructure

A Post-Quantum Financial Infrastructure Framework (PQFIF) Briefing

The \$600B Value Engine



Derivative Pricing: Processing highly complex, multi-dimensional market variables simultaneously.



Collateral Optimization: Solving immense asset-matching equations for corporate credit lines.



Fraud Detection: Quantum Machine Learning (QML) isolating subtle transaction anomalies instantly.

The Cryptographic Collapse



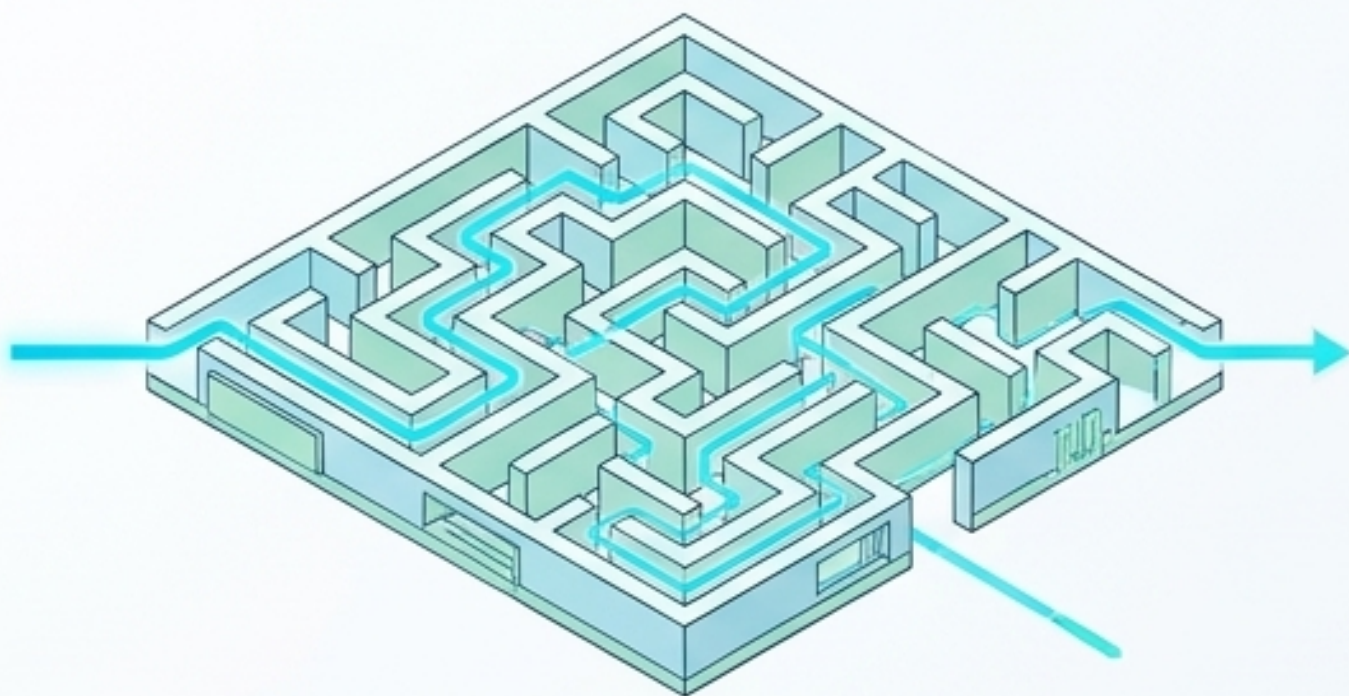
A Cryptographically Relevant Quantum Computer (CRQC) will break the RSA and ECC algorithms currently securing trillions of dollars in interbank communications, settlement data, and digital asset ledgers.

The Threat Mechanics: Classical vs. Quantum

Classical Cryptography

RSA / ECC (Public-Key Systems)

Relies on the extreme time required to solve prime factorization problems.

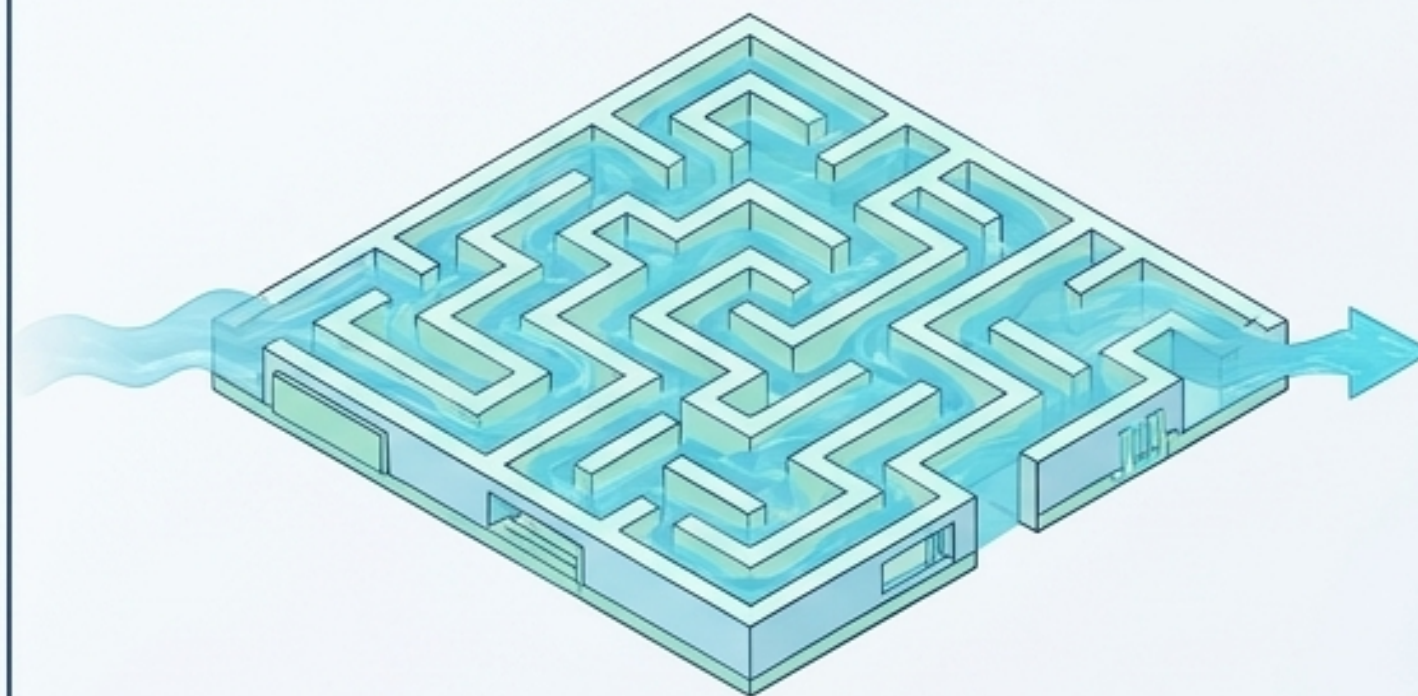


Time limit = Thousands of years

Quantum Algorithms

Shor's & Grover's Algorithms

Leverages superposition and quantum entanglement to bypass mathematical time limits.



Time limit = Hours or minutes

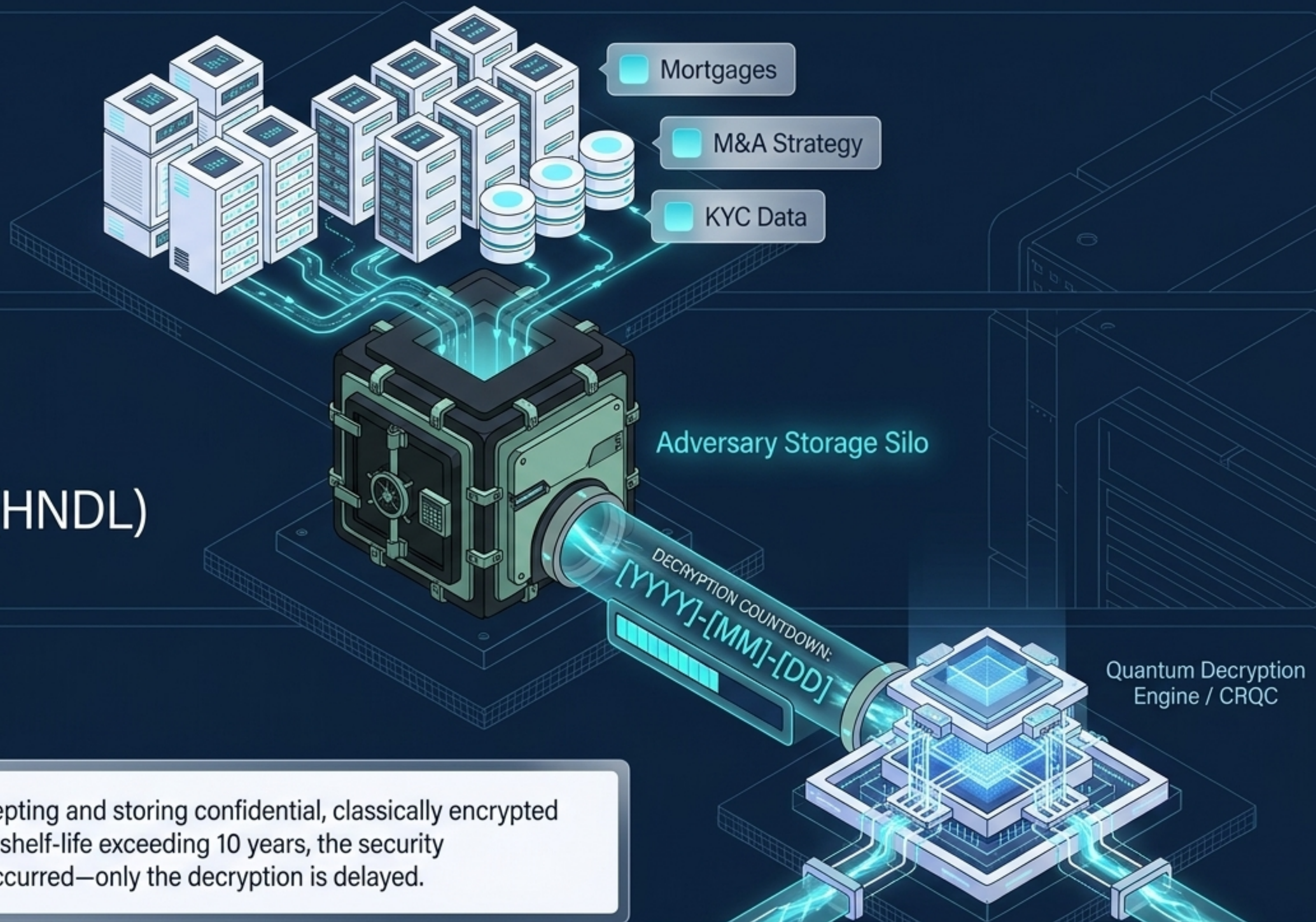
Critical Vulnerability: Shor's Algorithm specifically targets the public-to-private key reverse-engineering vulnerabilities in blockchains (ECDSA) and digital signatures.

Present Day

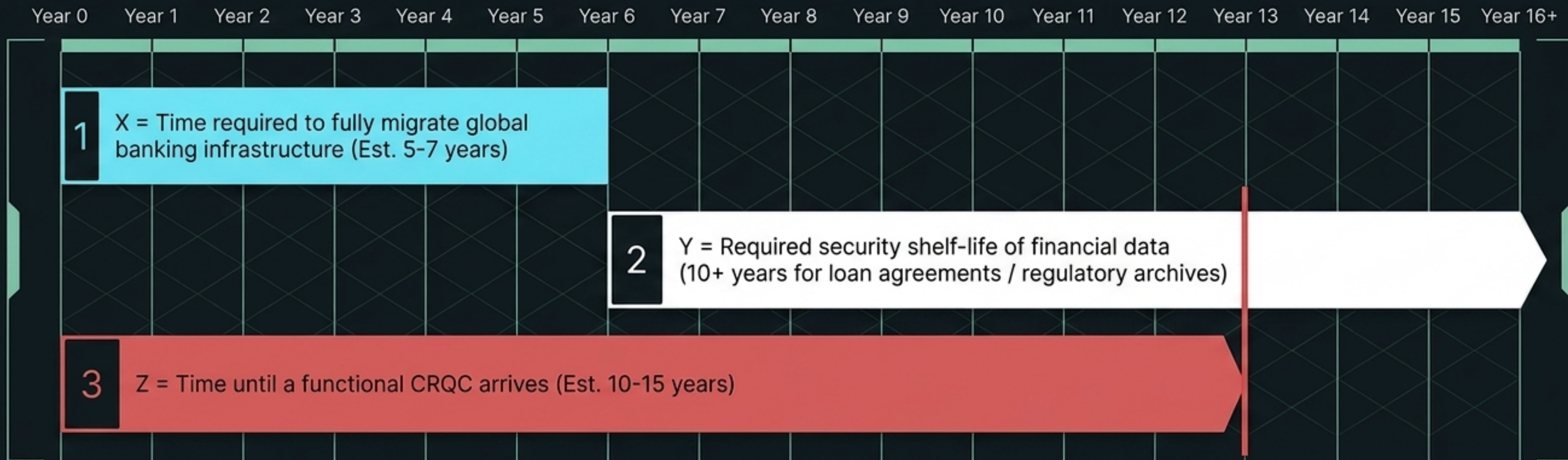
The Action: Harvest Now, Decrypt Later (HNDL)

Future State

Malicious actors are intercepting and storing confidential, classically encrypted data today. For data with a shelf-life exceeding 10 years, the security compromise has already occurred—only the decryption is delayed.



$X + Y > Z$ (Mosca's Theorem)



The Synthesis: If the time to migrate (X) plus the time data must remain secure (Y) is greater than the time until a quantum computer arrives (Z), the financial system is already operating in a deficit.

The Financial Attack Surface

Strike Point 1: Digital Loan Agreements

Vulnerability: RSA-2048.

Impact: Forgery of digital signatures and loss of legal enforceability.

Strike Point 2: Blockchain Ledgers

Vulnerability: ECDSA.

Impact: Extraction of tokenized assets from reused addresses.

Strike Point 3: API Gateways

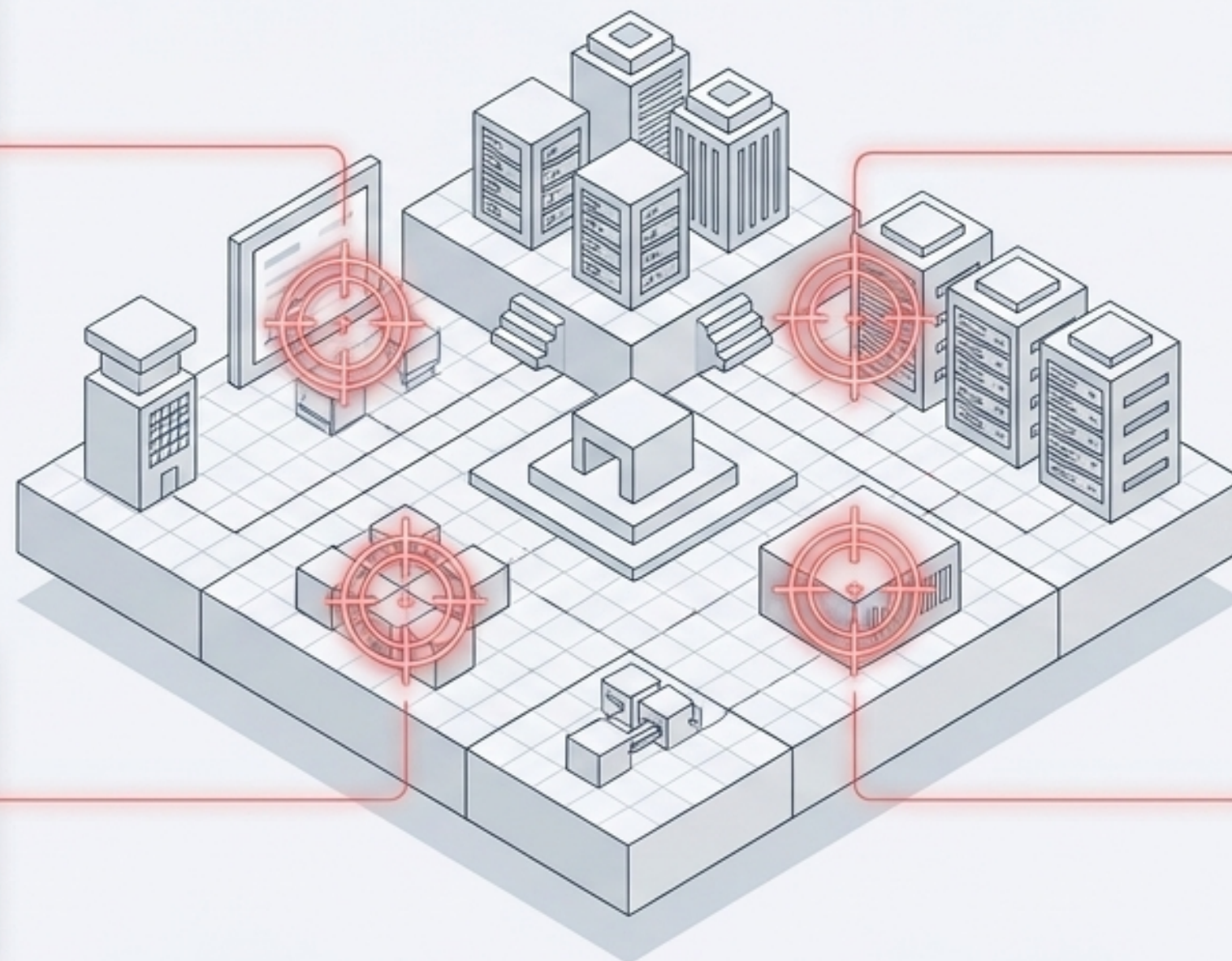
Vulnerability: TLS/HTTPS Decapsulation.

Impact: Interception of mobile banking APIs and inter-service meshes.

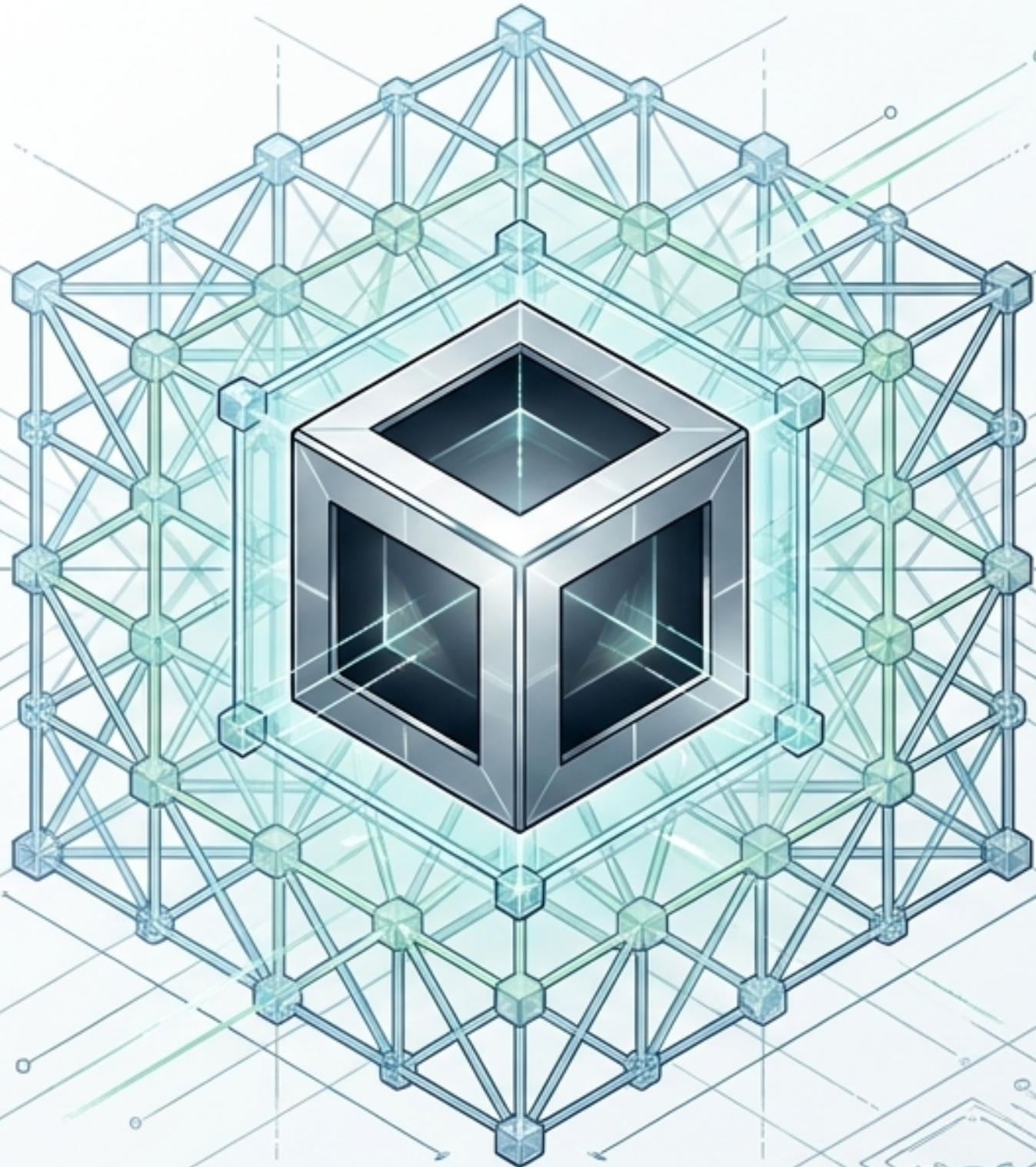
Strike Point 4: Hardware Vaults (HSMs)

Vulnerability: Secure Boot Manipulation.

Impact: Forged root CA certificates allow injection of malicious boot-level firmware.



Defense Vector 1: Post-Quantum Cryptography (PQC)



Nature

Software-based, utilizing new mathematical paradigms (like lattice grids) complex enough to defeat quantum algorithms.

Standards

NIST-approved FIPS 203 (ML-KEM), 204 (ML-DSA), and 205 (SLH-DSA).

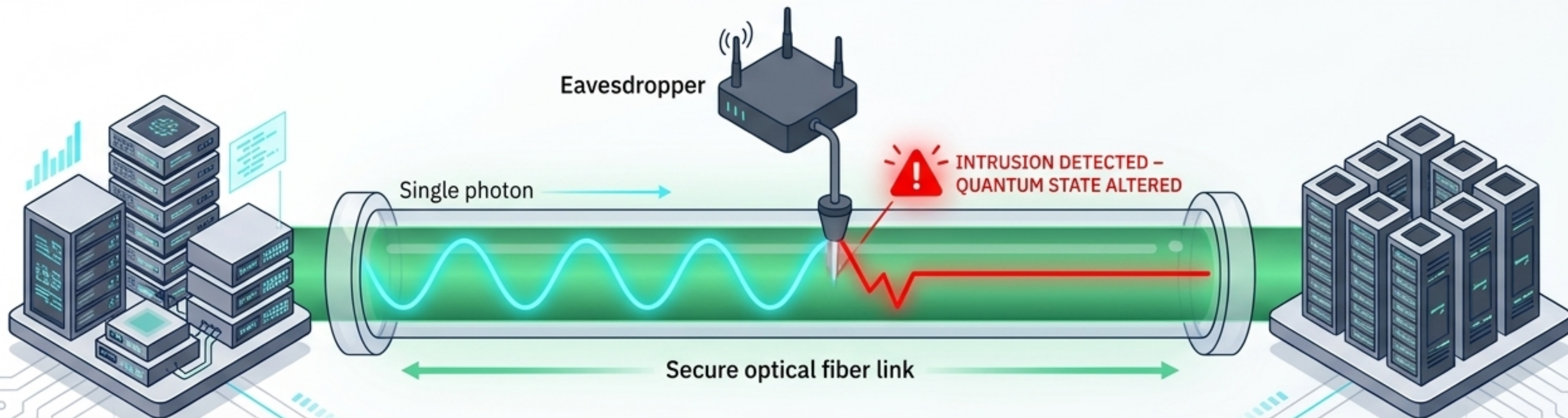
Deployment

Can be deployed on existing classical hardware and IT infrastructure without physical overhauls.

Primary Function

Securing the Application Layer (User endpoints, digital signatures, API authentication, and web sessions).

Defense Vector 2: Quantum Key Distribution (QKD)



Headquarters

Data Center

Nature

Hardware-based, relying on the fundamental laws of quantum mechanics rather than mathematical complexity.

Security Guarantee

Mathematically provable, unconditional security. Any observation physically alters the quantum state.

Deployment

Requires specialized optical hardware and dedicated, high-capacity fiber networks.

Primary Function

Securing the Physical/Network Layer (Data Center Interconnects, Interbank backbones).

The Cryptographic Matrix: PQC vs. QKD

	Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
Foundation	Mathematical Complexity	Quantum Physics
Implementation	Software Upgrade	Hardware Integration (Optical Fiber)
Operational Layer	Application / Transport Layer	Physical / Network Layer
Deployment Timeline	Immediate / Near-Term	Medium / Long-Term (Infrastructure dependent)
Primary Banking Use Case	Digital Signatures, Web APIs, Mobile Banking, Tokenization	Interbank Backbones, Disaster Recovery Data Center Interconnects

Synthesis: The Dual-Remediation Architecture



PQC Shield - Application & Endpoints

PQC provides end-to-end user authentication and secures transaction signatures over public networks (ML-DSA).

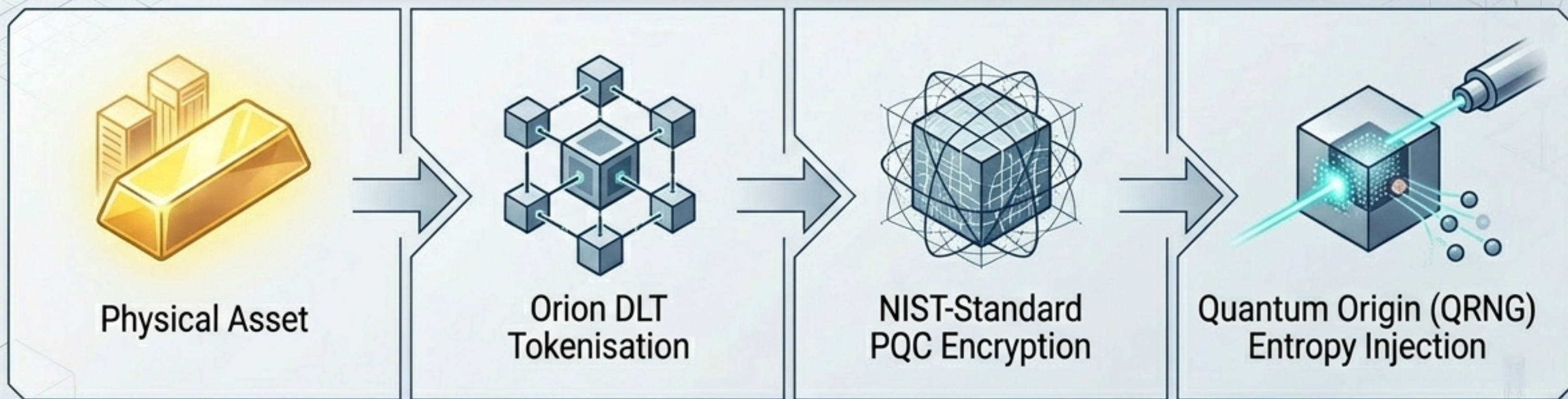
QKD Backbone - Physical & Network

QKD protects high-capacity Data Center Interconnects (DCIs) linking primary banking systems to disaster recovery sites.

**True Crypto-Agility requires both.
Math protects the transaction; Physics protects the network.**

Real-World Precedent: Protecting Digital Assets

Case Study: HSBC & Quantinuum (Tokenised Gold)



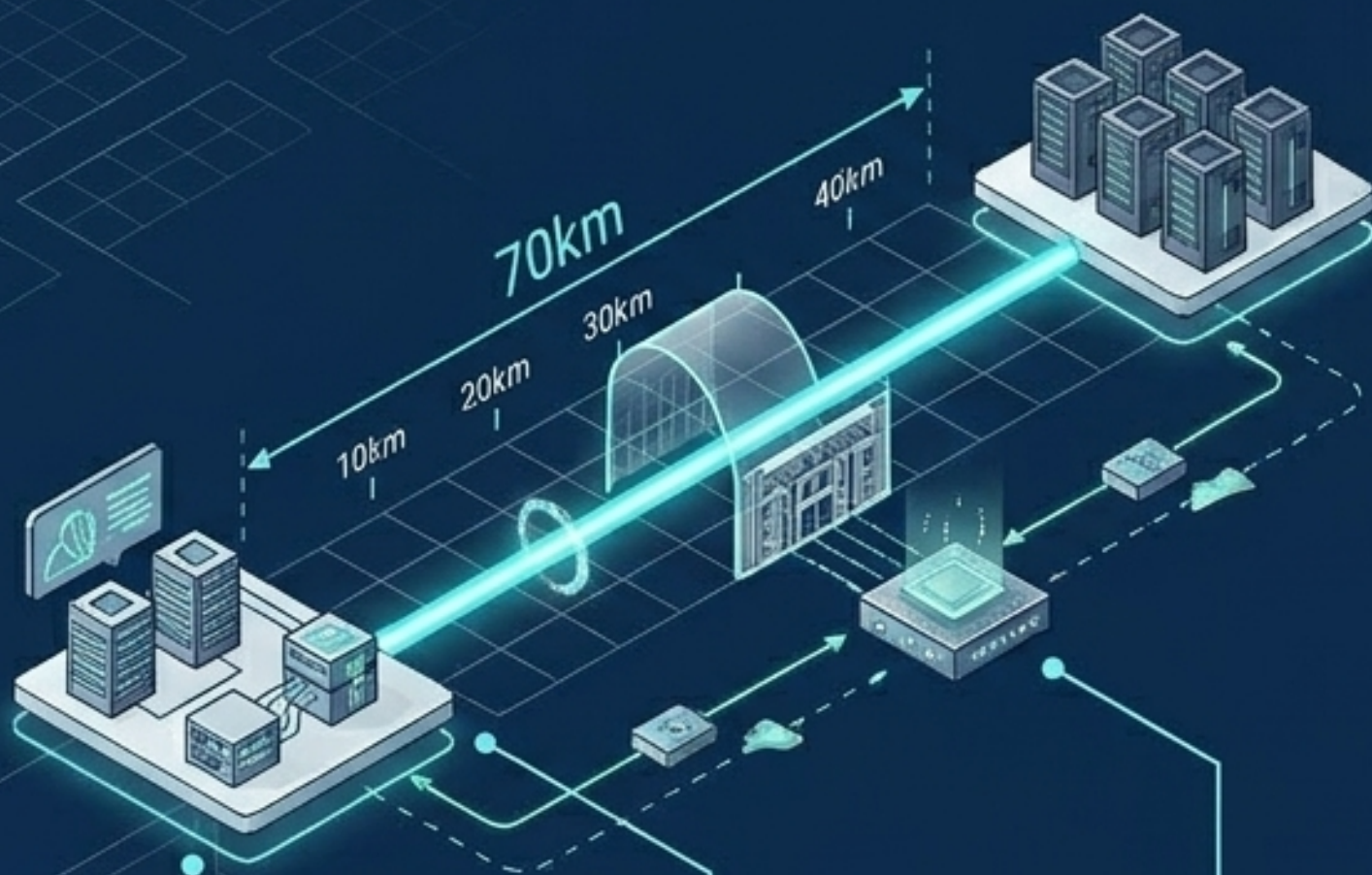
Overcame Harvest Now, Decrypt Later (HNDL) and Store Now, Decrypt Later (SNDL) attacks on distributed ledgers.

Successfully converted gold tokens into ERC-20 fungible tokens across secure, interoperable DLTs.

Proved that quantum-safe encryption seamlessly integrates into existing blockchain systems without operational disruption.

JPMorgan Chase

800 Gbps QKD Metro Network



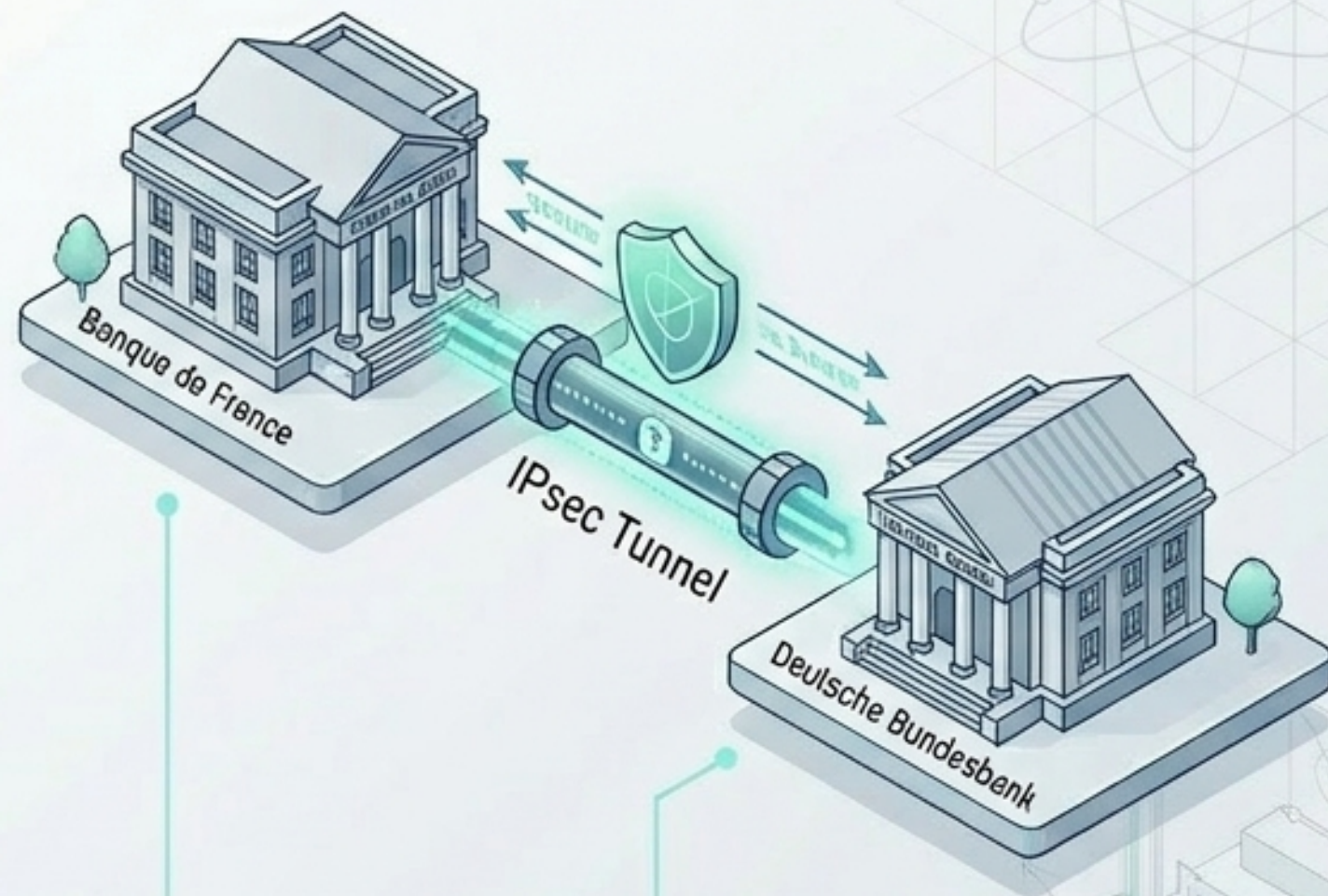
Multiplexed a quantum channel with 800 Gbps optical channels over 70km of commercial fiber.

Secured the Link peer-to-peer production blockchain.

Achieved key generation sufficient for 258 AES-256 encrypted streams running concurrently.

BIS Project Leap

Central Bank VPNs & Payment Networks



Phase 1: Created a hybrid IPsec tunnel between Banque de France and Deutsche Bundesbank.

Phase 2: Replaced standard signatures with PQC during live, active liquidity transfers.

Successfully integrated ML-DSA and ML-KEM on the Eurosystem's Target2 payment network without disrupting settlement flows.

The Post-Quantum Financial Infrastructure Framework (PQFIF)

USA: NSM-10 & CNSA 2.0

The White House mandates a strict 2035 deadline for the migration of all federal systems to quantum-resistant cryptography.

Europe: DORA

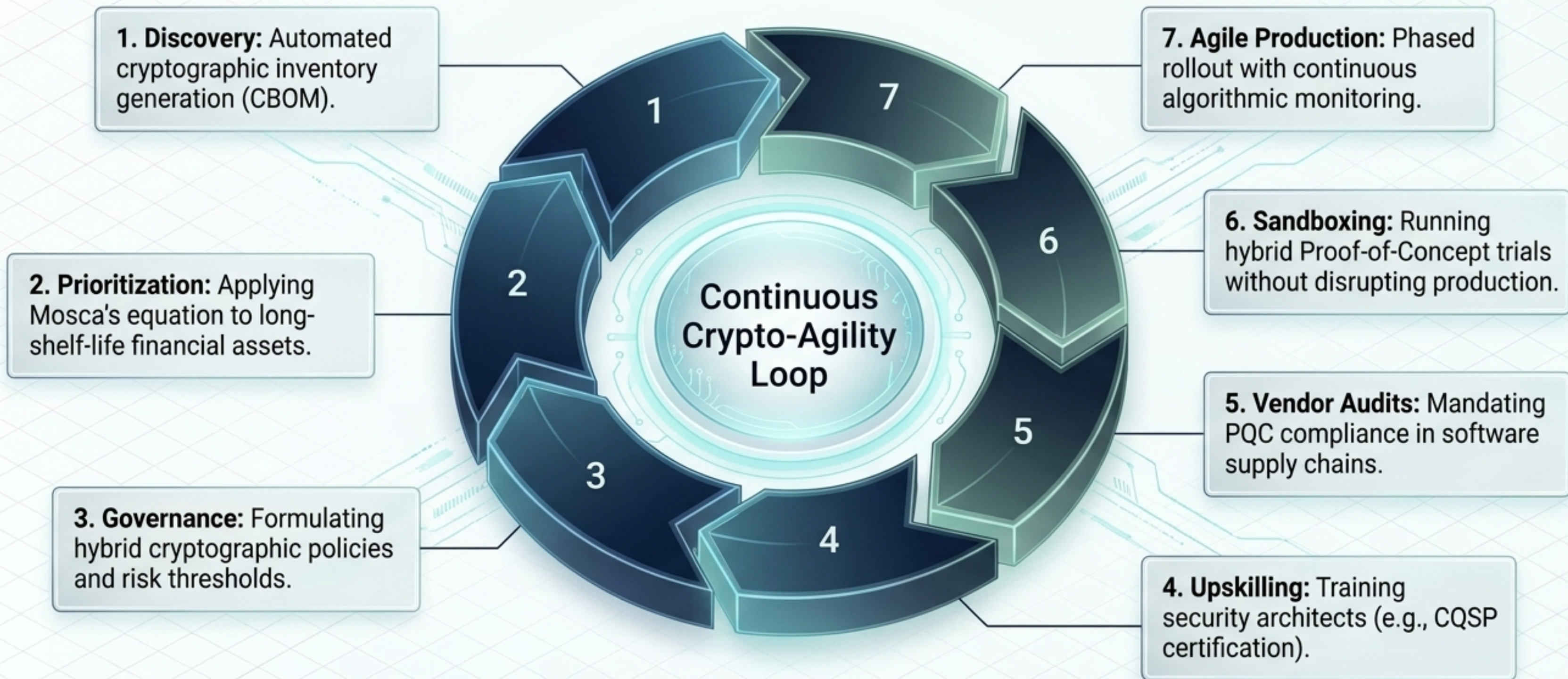
The Digital Operational Resilience Act legally obligates EU financial entities to maintain rigorous, future-proofed data confidentiality standards.

Singapore: MAS Sandbox

The Monetary Authority of Singapore successfully validated QKD production networks with major banks (DBS, HSBC, UOB).

The Solution: The PQFIF provides a multi-jurisdictional compliance engine for global banks to unify disparate regulatory requirements into a single transition blueprint.

The 7-Phase Migration Roadmap



The Strategic Imperative

Stop Harvesting

Immediate PQC migration for long-shelf-life data is required to cut off current HNDL intelligence gathering by malicious actors.

Build the Architecture

Invest immediately in Dual-Remediation models: integrate PQC for endpoints and transactions, and deploy QKD for high-capacity fiber backbones.

Embrace Crypto-Agility

Quantum readiness is not a one-time software patch; it is the new permanent operational state of modern financial cybersecurity.

*Cryptographic agility is no longer a future state; it is a **present-day operational requirement** to protect trillions in global economic value.*



Thank you!

Connect With CyberAid:

Linkedin: CyberAid