Government Blockchain Association
Quantum Working Group

Report

THE IMPACT OF QUANTUM COMPUTING ON FINANCIAL SERVICES

September 29, 2026

Status: Final Draft
Version: Version 0.3

Table of Contents

Acknowledgements

Special thanks to the authors & contributors:

Kevin Jackson, Working Group Leader
Executive Director
Institute for Digital Asset Innovation (IDAI)

John Medellin, PhD, CPA
CTO and CFO
TruDecision, Inc.

Gerard Dache
Executive Director
Government Blockchain Association (GBA)

Members of the GBA Quantum Working Group

Dr. Ingrid Vasiliu Feltes
World Business Angels Investment Forum (WBAF)
Vice President-WBAF Research Institute

Paul F. Dowding
Head of Design
L4S Corporation

1. Executive Summary

Quantum computing is no longer a distant theoretical concern — it is an accelerating engineering reality with profound implications for the security, integrity, and operational continuity of the global financial system. This report, produced by the Government Blockchain Association's Quantum Working Group, examines the intersection of quantum technologies and financial services across three dimensions: the risks related to quantum portfolios computing poses to current cryptographic infrastructure; the opportunities quantum capabilities create for financial optimization and modeling; and the governance and transition strategies that financial institutions, regulators, and technology providers must adopt to remain resilient.

Current financial infrastructure relies on public-key cryptographic algorithms. The public-key algorithms securing virtually all global financial infrastructure today, RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), are fundamentally vulnerable to quantum computing attacks. While cryptographically relevant quantum computers capable of breaking RSA and ECC are estimated to be 5 to 15 years away, the harvest-now-decrypt-later (HNDL) threat vector is already active. Adversaries may be collecting encrypted financial data today, positioning to decrypt it once quantum capabilities mature.

At the same time, quantum capabilities offer transformative opportunities: quantum optimization can improve portfolio construction and fraud detection; quantum simulation enables more accurate modeling of financial instruments; and quantum-enhanced artificial intelligence (AI) creates new capabilities for risk analysis.

The path forward requires multistakeholder coordinated action. The U.S. National Institute of Standards and Technology (NIST) finalized its first Post-Quantum Cryptography (PQC) standards in 2024. However, the financial sector's complex, interconnected infrastructure, spanning legacy core banking systems, payment rails, blockchain networks, and regulatory reporting makes migration a multi-year undertaking that must begin now, before adversaries harvest today's encrypted data.

This document is one of three companion documents, authored by the relevant GBA workgroup, that address the impact of selected advanced technologies on financial services:

- The Impact of Blockchain on FInancial Services
- The Impact of Artificial Intelligence on Financial Services
- The Impact of Quantum on Financial Services

A fourth executive compilation briefing document was also produced and released by GBA.

Key Findings for Government Decision Makers

- The cryptographic foundations of digital banking, payment networks, and blockchain systems are vulnerable to quantum attack within a 5–15 year horizon.
- "Harvest Now, Decrypt Later" attacks represent an immediate — not future — threat to financial data confidentiality.
- NIST's PQC standards (FIPS 203, 204, 205) provide a viable migration pathway, but require significant institutional investment.
- Quantum technologies also offer financial institutions material competitive advantages in optimization, simulation, and AI.
- Blockchain-based systems can uniquely enable crypto-agility — the ability to rapidly swap cryptographic algorithms as standards evolve.

Key Actions Required of Government Decision Makers

- Mandate cryptographic inventories for all government financial systems within 12 months.
- Issue quantum-resilience compliance timelines for regulated financial institutions.
- Require NIST PQC standards in all new Central Bank Digital Currency (CBDC), government payment, and financial infrastructure procurements.
- Fund quantum-security workforce development programs.
- Engage internationally through Financial Stability Board (FSB), Bank for International Settlements (BIS), and G7/G20* to harmonize global financial quantum-resilience standards.

*The G7 and G20 are informal international groups that coordinate global economic and political policies. Group of Seven (G7) comprises Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and the European Union. Focuses heavily on shared democratic values, political cooperation, and security issues. Represents roughly 10% of the global population and smaller share of total world GDP. Group of Twenty (G20) includes all G7 members plus 12 major emerging countries and both the European Union and the African Union. Focuses on global financial stability, trade, climate change, and sustainable development. Represents about 85% of global GDP and two-thirds of the world's population.

2. Context & Background

The Government Blockchain Association's Quantum Working Group supports the goal of strengthening the governance, standards, and resilience of digital financial infrastructure globally. The convergence of quantum computing with financial systems represents one of the most consequential technology transitions the sector has faced since the introduction of the internet.

The financial sector is among the most cryptography-dependent industries in the global economy. Every digital transaction, every authenticated login, every encrypted wire transfer, every digitally signed regulatory submission relies on mathematical assumptions that quantum computers are specifically designed to challenge. The asymmetric encryption algorithms that protect these systems including RSA, ECC, and Diffie-Hellman, derive their security from mathematical problems that a sufficiently powerful quantum computer running Shor's algorithm could solve in hours.

This report was developed in response to growing urgency within the working group regarding the quantum readiness of financial systems, particularly those incorporating blockchain and distributed ledger technology (DLT), where cryptographic integrity is foundational to the entire trust model. It draws on published research, regulatory guidance, and working group expertise to provide a comprehensive assessment of the quantum threat landscape and a practical framework for quantum-resilient transition.

Financial Services Exposure

Like many other industry sectors, financial services face a compounded challenge: (1) legacy systems with decades-long upgrade cycles; (2) regulatory requirements that mandate specific cryptographic standards; (3) interconnected global infrastructure where a single weak node can compromise entire payment networks. One unique aspect, however, is (4) the irreversibility of financial transactions — meaning compromised past data has permanent consequences. The sector must balance urgency with the risk of premature or disruptive migration.

3. Introduction to Quantum Technologies

Quantum technology refers to devices and systems that exploit quantum mechanical phenomena—superposition, entanglement, and quantum tunneling—to perform functions that classical physics can't replicate or can only do less efficiently. It spans several main areas: quantum computing, which uses qubits capable of existing in multiple states simultaneously to solve certain problems (like factoring large numbers or simulating molecules) far faster than classical computers; quantum communication, which uses entangled particles to transmit information with security guaranteed by physics rather than just mathematical complexity (as in quantum key distribution); and quantum sensing, which achieves extreme precision in measuring time, gravity, or magnetic fields by exploiting quantum states' sensitivity to their environment.

The common thread is that these technologies manipulate individual quanta (photons, electrons, atoms) directly, rather than treating matter and energy as continuous, classical quantities—which is what separates them from earlier "quantum-enabled" technologies like transistors and lasers that rely on quantum effects in bulk material but don't manipulate individual quantum states. Understanding the core concepts, terminology, and current state of development is essential for any decision maker responsible for financial system resilience.

3.1 Core Concepts

Classical computers process information as binary bits — each bit is either 0 or 1. Quantum computers use quantum bits (qubits) that exploit two phenomena to perform certain computations dramatically faster:

- **Superposition:** A qubit can exist in a combination of 0 and 1 simultaneously, like a coin spinning in the air until measured. This allows quantum computers to evaluate many possible solutions simultaneously.
- **Entanglement:** Two qubits can become linked so the state of one instantly influences the other, regardless of physical distance. This enables exponential parallelism for specific computation types.
- **Coherence:** a quantum system's ability to maintain a fixed phase relationship between states in a superposition, allowing them to interfere with one another rather than behave as a simple probabilistic mixture. It's treated as a fragile resource because interactions with the environment cause decoherence, degrading quantum behavior into classical behavior over a characteristic coherence time.

3.1.1 Quantum Computing

Quantum computing uses superposition and entanglement to execute certain algorithms exponentially faster than classical computers. One of the most cryptographically significant is Shor's algorithm, which can factor large numbers efficiently — directly threatening RSA and ECC encryption. Grover's algorithm provides a quadratic speedup for searching unsorted data, effectively halving the effective key length used in symmetric encryption.

Current quantum computers (2026) are Noisy Intermediate-Scale Quantum (NISQ) devices — having between dozens and a few thousand qubits but constrained by high error rates. Fault-tolerant quantum computers capable of breaking 2048-bit RSA would require millions of stable, error-corrected logical qubits. This is a capability researchers estimate is 5–15 years away.

3.1.2 Quantum Sensing

Quantum sensing exploits the sensitivity of quantum systems to measure physical phenomena such as magnetic fields, gravity, time, and temperature with precision far beyond classical sensors. In financial services, near-term applications include secure timing for trading synchronization, GPS-independent positioning for asset tracking, and tamper detection in financial hardware security modules (HSMs).

3.1.3 Quantum Simulation

Quantum simulation models complex systems that exceed classical computational capacity including credit risk correlation scenarios, climate risk models for Environmental, Social, and Governance (ESG) reporting, and complex derivatives pricing structures. For financial regulators, quantum simulation may enable stress testing at a scale and fidelity that current classical infrastructures cannot support.

3.1.4 Quantum Communications

Quantum communications uses quantum mechanics to transmit information with theoretically unbreakable security. Quantum Key Distribution (QKD) uses individual photons to exchange cryptographic keys. Any interception attempt disturbs the quantum state and immediately reveals eavesdropping. Central banks in Europe and Asia are piloting QKD for high-value secure communications, including Bank Digital Currency (CBDC) infrastructure.

3.2 Terms and Definitions

3.2.1 Quantum Threats — Key Terminology

Cryptographically Relevant Quantum Computer (CRQC)	A quantum computer able to execute Shor's algorithm against real-world encryption. Does not yet exist but is credible within a 5-to-15-year horizon.
Grover's Algorithm	A quantum search algorithm providing quadratic speedup, effectively halving the effective key length of symmetric encryption algorithms (e.g., AES-128 becomes AES-64 equivalent against a quantum adversary).
Harvest Now, Decrypt Late (HNDL)	Malevolent actors collect and store currently-encrypted data with the intent to decrypt it once a quantum computer becomes available. Also called "store now, decrypt later."
Quantum-Day (Q-Day)	The moment at which a cryptographically relevant quantum computer first becomes operational, marking the point at which current classical public-key cryptography is broken.
Quantum Threat	Any quantum technology capability that undermines the security, integrity, or confidentiality of digital financial systems
Shor's Algorithm	A quantum algorithm that can factor large integers in polynomial time — directly breaking RSA and ECC encryption. Developed by mathematician Peter Shor in 1994.

3.2.2 Quantum Risks — Key Terminology

Cryptographic Risk	The risk that quantum-enabled cryptographic attacks compromise the confidentiality, integrity, or authenticity of encrypted financial data and communications.
Migration Risk	Operational and financial risk associated with transitioning classical legacy systems to quantum-resistant standards, including cost overruns, compatibility failures, service disruption, and implementation errors.
Regulatory Risk	The risk that financial institutions face penalties or sanctions for failing to meet quantum-security requirements under emerging and updated regulatory frameworks.
Systemic Risk	The risk that quantum attacks on critical financial infrastructure, including payment rails, central bank systems, and clearing houses, trigger cascading failures across the financial system.
Vendor Risk	The risk that third-party technology providers fail to achieve quantum readiness within required timeframes, exposing financial institutions to cascading cryptographic vulnerabilities.

3.3 Recent Developments

The quantum computing landscape has advanced rapidly. Key milestones relevant to financial services risk assessment:

- **OMB Memorandum M-23-02** (November 2022) — established the federal compliance precedent for inventorying quantum-vulnerable systems.
- **NIST finalizes first PQC standards** (August 2024) — FIPS 203, 204, 205.
- **BIS working paper on quantum risk** (2024).
- **Rakhra et al., IEEE** (2024) — hybrid PQC+QKD transition strategy for financial institutions.
- **Ren et al., Proceedings of the IEEE** (November 2024) — bidirectional quantum-blockchain relationship.
- **Google's Willow chip** (December 2024) — error correction below the fault-tolerance threshold.
- **HSBC and IBM demonstrate quantum-enabled algorithmic bond trading** (September 25, 2025) — the first production-scale validation of Egger's research program: using an IBM Quantum Heron processor on real European corporate bond market data, the trial improved trade-fill prediction accuracy by up to 34% over classical-only methods — described as the first empirical evidence of quantum advantage in a live financial workflow, moving Egger et al.'s theoretical simulation/optimization/ML work into practice.
- **Vanguard and IBM explore quantum-enhanced portfolio optimization** (2025) — applying VQE and QAOA to portfolio construction under real-world constraints, complementing the HSBC trading result with a second IBM financial-sector use case.
- **IBM's 2025 Quantum Roadmap update: Nighthawk and Loon unveiled** (November 12, 2025) — Nighthawk, a 120-qubit processor (first of a four-generation series scaling to 15,000+ two-qubit gates by 2028), and Loon, an experimental chip validating fault-tolerant components for IBM's planned Starling system — both reaffirming IBM's public target of demonstrating quantum advantage by the end of 2026.
- **G7 Cyber Expert Group publishes PQC roadmap for the financial sector** (January 15, 2026).
- **Estimated qubit threshold to break RSA/ECC drops** (early 2026) — to ~100,000 qubits.
- **Japan's FSA instructs financial institutions to formalize PQC migration plans** (early-to-mid 2026).
- **Coinbase Quantum Advisory Council publishes June position paper** (~June 13, 2026).
- **Trump signs EO-14412 and EO-14413** (June 22, 2026).
- **IQM announces a fault-tolerance milestone in quantum error correction** (June 23, 2026).
- **OMB issues Memorandum M-26-15** (June 24, 2026).
- **Multiple vendors report logical-qubit-scale demonstrations** (mid-2026) — Quantinuum Helios (48), QuEra (96), Atom Computing (24).

Research Foundation: Peer-Reviewed Literature Supporting This Report

This report draws on seven peer-reviewed sources from IEEE conferences and journals (2023–2025) covering: (1) quantum cryptography and QKD security proofs (Rakhra et al.); (2) the convergence of quantum computing and finance including ML and optimization (Aggarwal et al., 2025; Egger et al., IEEE TQE); (3) feasible quantum applications across financial and security domains (Chamma et al., 2023); (4) quantum vault architectures for digital currency and CBDC (Broadbent et al., IEEE QCE 2024); (5) quantum-resilient Web 3.0 and blockchain infrastructure (Ren et al., Proceedings of the IEEE 2024); and (6) quantum money security frameworks (Mishra et al., 2023). Full citations appear in Annex C.

Supplementary Industry Sources and Real-World Demonstrations

These findings are corroborated by contemporaneous industry reporting and IBM Research documentation: HSBC's September 2025 announcement of the first known quantum-enabled algorithmic bond trading trial with IBM, with independent technical analysis from The Quantum Insider; IBM's November 2025 unveiling of its Nighthawk and Loon processors, reported by IBM Newsroom and The Next Platform; The Quantum Insider's March 2026 survey of 15+ global banks piloting quantum technologies; IBM's institutional research on quantum use cases for financial services; and the published research profile of IBM's Daniel Egger, whose IEEE TQE work is cited above.

4. Quantum Risks to Financial Systems

Quantum risk in financial services is not uniform; it unfolds across multiple timeframes and varies in severity by system and domain. This section provides a structured analysis of both immediate and long-term risks to support prioritization decisions by government and regulatory bodies.

4.1 Immediate Risks (2026-2030)

"Immediate" in a financial services context does not mean "imminent quantum attack". It means risks that financial institutions must act on today, because the preparation required cannot be completed quickly and because there is evidence of active adversarial data collection.

4.1.1 Cryptographic Vulnerabilities

The cryptographic systems underpinning modern financial infrastructure were designed with the assumption that factoring large numbers is computationally intractable. Quantum computers directly invalidate this assumption.

4.1.1.1 RSA and ECC Risk: Shor's Algorithm

RSA and ECC are the two dominant public-key cryptographic algorithms in financial infrastructure. A 2048-bit RSA key that would take classical computers longer than the age of the universe to factor falls to Shor's algorithm on a sufficiently powerful quantum computer in hours. ECC is equally vulnerable, as Shor's algorithm also solves the elliptic curve discrete logarithm problem that ECC relies

The practical implication is stark: TLS/SSL certificates securing banking websites, digital signatures on financial messages, and authentication tokens for payment systems, all rely on RSA or ECC and would be instantly breakable once a CRQC becomes operational.

4.1.1.2 Digital Banking System Risks

Digital banking platforms rely on RSA/ECC for user authentication, encryption of data in transit (via TLS), digital signing of transaction records, and certificate-based mutual authentication between systems. An adversary who had previously collected TLS-encrypted session traffic from systems lacking forward secrecy could retroactively decrypt account credentials, transaction histories, and personally identifiable information (PII) once cryptographically relevant quantum computers are available. TLS 1.3 uses ephemeral key exchange (ECDHE), which provides forward secrecy. TLS 1.2 and earlier, or any TLS 1.3 misconfiguration using static keys, does not have forward secrecy and is vulnerable to retroactive decryption. In real-time, a quantum-capable adversary could impersonate banks, forge digital signatures on transactions, or conduct man-in-the-middle attacks on banking APIs.

4.1.1.3 Payment Infrastructure Risks (SWIFT, CBDCs, Real-Time Payments)

SWIFT — used by over 11,000 financial institutions in 200+ countries relies on RSA/ECC-based PKI for message authentication and non-repudiation. CBDCs currently in development across 130+ countries are largely architected with ECC digital signatures. These systems are designed for multi-decade lifetimes, meaning they will outlive their cryptographic foundations unless migration begins now.

Real-time payment networks (FedNow, UK Faster Payments, India's UPI) present a particular migration challenge: they process millions of transactions per second with sub-second settlement requirements,

creating performance constraints that PQC algorithms, with larger key sizes and slightly higher computational overhead must meet.

4.1.1.4 Blockchain Networks and Digital Wallet Risks

Blockchain networks, including both public chains and enterprise DLT platforms used in financial services, rely on elliptic curve digital signature algorithms (ECDSA and EdDSA) for transaction authentication, wallet security, smart contract execution, and node identity. Research indicates approximately 25% of Bitcoin in circulation is held in wallets with exposed public keys are directly vulnerable once a CRQC becomes available. For enterprise blockchain applications in trade finance, securities settlement, and CBDCs, the consequences of cryptographic compromise are systemic and immediate.

Blockchain Quantum Vulnerability — Special Consideration for Government

Unlike traditional financial systems where cryptographic migration occurs through administrative updates to certificate authorities, blockchain networks require protocol-level upgrades, consensus among all participants to migrate to quantum-resistant schemes. Enterprise blockchain networks used in government financial applications have defined governance structures that can execute planned migrations, but require significant lead time. Government procurement rules for blockchain-based systems should require quantum-resilience by design to ensure they are hardened enough to outlive the cryptographic assumptions on which they are built.

4.1.2 "Harvest Now, Decrypt Later" (HNDL) Risk

HNDL is the most immediately actionable quantum risk. Unlike a quantum attack — which requires a CRQC — HNDL can be conducted today using classical infrastructure. IBM Distinguished Engineer Jeff Crume, who has been a leading public voice framing this threat, warns that cryptographically relevant quantum computers could arrive as early as 2030–2035 and stresses that "Q-Day" won't announce itself: encrypted traffic captured now becomes readable retroactively the moment a sufficiently powerful quantum computer exists, regardless of when that day falls. Nation-state adversaries with the capability and motivation to compromise long-term financial intelligence have strong incentives to collect encrypted data now.

This is no longer theoretical. GCHQ/NCSC assessments have confirmed active HNDL operations targeting UK government, defense, and financial-sector communications by multiple nation-state actors, and the Cyber Threat Alliance's "Approaching Quantum Dawn" report (February 2026) documented adversaries systematically archiving banking records, state secrets, and intellectual property against future decryption. Executing HNDL at meaningful scale requires bulk collection infrastructure — submarine cable taps, satellite intercept stations, ISP-level collection agreements — limiting it to state-level operators: Five Eyes-aligned services, China's Ministry of State Security, and Russia's FSB/GRU are the actors most frequently identified. Since over 95% of intercontinental data transits via submarine cables, financial institutions' cross-border communications are structurally exposed to this collection method today, independent of current encryption strength.

The risk is particularly acute for data with long sensitivity lifecycles: long-term debt and structured finance documentation; sovereign debt negotiation records; central bank policy deliberations

transmitted via secure channels; KYC/AML databases retaining personal financial histories for years; and strategic financial intelligence relevant to national security.

HNDL's evidentiary consequences extend beyond financial and intelligence data to the legal record itself. Court filings, regulatory submissions, and attorney-client communications encrypted under classical schemes and archived today could be decrypted years or decades later — retroactively exposing privileged legal strategy, undermining the finality of settled matters, and calling into question the integrity of evidence whose confidentiality was assumed permanent at the time it was created. Financial institutions engaged in litigation, regulatory enforcement, or sensitive negotiations should treat privileged and evidentiary communications with the same migration urgency as the long-lifecycle financial data described above.

This threat model has now moved from advisory guidance into binding federal policy. Executive Order 14412 (June 22, 2026) explicitly cites "ongoing cyber activity [that] presents the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational" as the rationale for its accelerated PQC deadlines, and NIST's own migration pilot is now scheduled for 2027, ahead of the broader 2030 federal compliance deadline.

Financial institutions and government agencies that have not begun migrating the most sensitive communications to quantum-resistant channels are accepting risk that accumulates with every passing month, regardless of when Q-Day arrives.

4.2 Long-Term Risks (2030-2045)

The long-term risk horizon (5–15 years, post-Q-Day) involves not just data confidentiality, but the fundamental integrity and authenticity of financial records, transactions, and system identities. It should be noted that these long-term risks apply to both traditional and blockchain-based financial systems.

- **Transaction Repudiation Risk:** Digital signatures on historical financial transactions could be forged retroactively — enabling fraudulent claims that transactions were never authorized or that records were altered.
- **Identity Infrastructure Collapse:** PKI hierarchies underpinning bank certificate authorities, payment network identity, and regulatory credential systems would require complete rebuilding if root certificate authorities are compromised.
- **Smart Contract Exploit Risk:** Smart contracts on quantum-vulnerable blockchain networks could be exploited through signature forgery, enabling unauthorized fund transfers or governance manipulation.
- **Sovereign Debt and Treasury Risk:** Government bond issuances, treasury auctions, and sovereign payment systems secured by quantum-vulnerable cryptography face long-term integrity risk if migration is not completed before Q-Day.
- **Interbank settlement integrity risk:** Once quantum computers can forge digital signatures, the interbank messages and settlement instructions institutions rely on as authentic and final could be fabricated or altered without detection, undermining the trust assumption the entire settlement system depends on.

- **Market manipulation risk due to cryptographic forgery:** Quantum-forged signatures could let bad actors fabricate trade records, orders, or market data that appear cryptographically authentic, enabling manipulation that evades detection systems built to distinguish genuine from falsified activity.
- **Contractual enforcement risks:** If the digital signatures underlying a contract or smart contract become forgeable, courts and counterparties can no longer reliably establish who actually agreed to its terms, weakening the legal enforceability of digitally executed agreements.
- **Auditing risks:** Auditors depend on cryptographically signed records as trustworthy evidence of what happened and when, so once those signatures can be forged or retroactively broken, the integrity of the audit trail itself — not just the transactions it documents — comes into question.

4.3 Quantum Risk by Financial Services Domain

Quantum risk does not affect all financial services domains equally. In the following table, Immediacy and Priority apply to both regulators and financial institutions.

Financial Domain	Key Quantum Vulnerabilities	Immediacy	Priority
Banking	Customer authentication, TLS for digital banking, core banking API security, digital signatures on loan documentation	HIGH	**CRITICAL**
Digital Assets & Tokenization	Blockchain wallet security, smart contract execution integrity, DeFi protocol signatures	HIGH	**CRITICAL**
Financial Infrastructure	Core banking systems, identity management, KYC/AML databases, cloud security, custodian communications	HIGH	**CRITICAL**
Government & Public Finance	Central bank operations, sovereign debt issuance, treasury authentication, benefits disbursement	HIGH	**CRITICAL**
Payments & Money Movement	SWIFT PKI, CBDC signature schemes, real-time payment authentication, card network tokenization	HIGH	**CRITICAL**
Capital Markets	Trade order authentication, settlement system integrity, exchange API security	HIGH	HIGH
Capital Markets	Trade order authentication, settlement system integrity, FX confirmation signing	HIGH	HIGH
Regulatory, Risk & Compliance	Regulatory submission signing, audit trail integrity, AML/KYC record confidentiality	HIGH	HIGH
Investment & Asset Management	Portfolio data confidentiality, client communication encryption, advisor authentication	MEDIUM	HIGH

Financial Domain	Key Quantum Vulnerabilities	Immediacy	Priority
Lending & Credit	Loan origination documentation, credit bureau data transmission, syndicated loan communications	MEDIUM	HIGH
Insurance	Actuarial data confidentiality, claims signature authentication, reinsurance treaty signing	MEDIUM	MEDIUM

5. Post-Quantum Cryptography (PQC) and Quantum-Resilient Systems

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms resistant to attacks from both classical and quantum computers. Unlike quantum cryptography — which uses quantum physics itself — PQC algorithms run on classical hardware and are designed as practical replacements for vulnerable algorithms in existing financial infrastructure.

5.1 NIST PQC Standards

NIST finalized its first three PQC standards in August 2024, providing the cryptographic foundation for the quantum-resilient transition:

FIPS 203 (ML-KEM)	Module-Lattice Key Encapsulation Mechanism — based on CRYSTALS-Kyber. Used for key exchange and encryption. Recommended for general-purpose encryption of data in transit — replacing RSA and ECC key exchange in TLS and payment network protocols.
FIPS 204 (ML-DSA)	Module-Lattice Digital Signature Algorithm — based on CRYSTALS-Dilithium. Used for digital signatures. Recommended for transaction authentication, document signing, and code integrity verification.
FIPS 205 (SLH-DSA)	Stateless Hash-Based Digital Signature Algorithm — based on SPHINCS+. A mathematically conservative alternative for high-assurance signing applications, including regulatory filings and central bank operations.
FALCON (FIPS 206, pending)	A lattice-based signature scheme with smaller signature sizes — pending final standardization which is expected in late 2026 or early 2027. Relevant for resource-constrained environments such as payment terminals and IoT devices in financial infrastructure.

The mathematical security of these standards rests on problems believed to be hard for both classical and quantum computers — the hardness of finding short vectors in high-dimensional mathematical structures called lattices, and the collision resistance of cryptographic hash functions. None of these problems are known to be efficiently solvable by classical or quantum algorithms..

5.2 Migration Challenges for Financial Institutions

- **Cryptographic Inventory Gap:** Most large financial institutions lack a comprehensive inventory of where vulnerable algorithms are deployed across systems, vendors, and third-party dependencies.
- **Legacy System Constraints:** Core banking systems with decades-long upgrade cycles may require hardware replacement — not just software updates — to support PQC algorithms.
- **Algorithm Performance:** Current PQC algorithms carry larger key and signature sizes than their classical counterparts. For high-frequency transaction systems, this creates measurable bandwidth and storage implications.

- **Interoperability:** International payment networks require coordinated migration — no single institution can complete the transition without counterpart cooperation.
- **Third-Party Dependencies:** HSMs, certificate authorities, payment terminals, and software libraries must all support compatible PQC standards versions before migration is complete.
- **Regulatory Sequencing:** Some frameworks specify mandatory cryptographic algorithms; migration to PQC may require regulatory waivers and process overhead.

5.3 Hybrid Cryptographic Approaches

Given migration complexity and continued uncertainty about quantum timelines, multiple peer-reviewed studies independently confirm that hybrid quantum/classical cryptographic approaches are the most viable near-term transition strategy (Rakhra et al.; Aggarwal et al., 2025; Egger et al., IEEE TQE). Hybrid cryptography combines a classical algorithm with a PQC algorithm — maintaining security against both classical and quantum adversaries. Even if one algorithm is later found to have a flaw, the other provides a fallback.

Looking further ahead, Quantum Key Distribution (QKD) — specifically BB84 and Continuous Variable QKD protocols — offers information-theoretic security, provably secure against any computational attack, classical or quantum. Research demonstrates that QKD provides a verifiable defense against eavesdropping where classical systems fail (Rakhra et al.). For the highest-sensitivity government financial channels — central bank policy communications, sovereign debt negotiations, national security financial intelligence — QKD represents the long-term gold standard as infrastructure matures and costs decline.

Implementation Recommendation

Financial institutions should adopt a "quantum-hybrid first" posture for all new system deployments and major upgrades. A quantum-hybrid first posture implements hybrid TLS (classical ECDH + ML-KEM) for new secure communications infrastructure, hybrid digital signatures for new transaction signing systems, and PQC-ready HSMs for all new cryptographic hardware. This protects against HNDL attacks today while maintaining backward compatibility during the transition period. For government financial infrastructure that handles the most sensitive communications, a longer-term QKD implementation roadmap should be initiated alongside PQC migration planning.

5.4 Role of Blockchain in Enabling Crypto-Agility

Crypto-agility refers to the ability of a system to rapidly transition between cryptographic algorithms without fundamental architectural change — treating the cryptographic layer as a configurable component rather than a hard-coded assumption. Well-designed blockchain architectures can enable crypto-agility through modular signature scheme abstraction, versioned transaction formats with algorithm identifiers, and smart contract-based cryptographic policy enforcement updatable through governance.

This design pattern is now directly validated in the technical literature. Santos, Ferrin, Kahat, and Lodder's "Post-quantum Blockchains with Agility in Mind" (2026) presents an EVM-compatible blockchain built for cryptographic agility from genesis, introducing cryptographically agile transactions (CATX) — a format that decouples transaction body from signature so users can select their own signature scheme — alongside a consensus-layer key registration mechanism letting validators migrate between signature schemes without hard forks. Tested across 30,000 blocks and 11 million transactions using ECDSA, Falcon-512, and ML-DSA signatures, the CATX format introduced no measurable performance overhead, giving a concrete existence proof that the modular abstraction this section describes is implementable at production scale without a throughput penalty.

The maturity-model literature reinforces why this matters for governance. Hohm, Heinemann, and Wiesmaier's Crypto-Agility Maturity Model (CAMM, 2022) frames crypto-agility as an assessable organizational capability rather than a binary property, and Alnahawi and Schmitt's "On the State of Crypto-Agility" (2023) found that most existing systems — blockchain included — still treat cryptographic algorithm choice as a fixed design-time decision rather than a governed, updatable one. That gap is precisely what public-sector financial applications with long operational lifetimes cannot afford, and it is the gap IDAI and the GBA's reference architecture work is positioned to close.

As experts in blockchain governance and implementation, IDAI and the GBA are well-positioned to develop reference architectures for crypto-agile blockchain implementations in public sector financial applications, particularly for CBDC infrastructure, government payment systems, and public procurement platforms where long operational lifetimes make quantum-resilience planning essential.

6. Quantum Opportunities in Financial Services

Financial institutions that move early on quantum readiness gain competitive advantage; the transition is both a risk to manage and an opportunity to capture. Quantum technologies offer material advantages across three distinct modalities — computing, sensing, communications, and artificial intelligence — each with its own opportunity set for the financial services industry.

6.1 Quantum Computing

Quantum computing offers the most direct path to computational advantage in optimization and simulation problems that are intractable or expensive at classical scale.

6.1.1 Optimization.

Many computationally expensive financial problems are optimization problems: portfolio construction across thousands of assets; payment routing across correspondent banking networks; hedging strategy optimization across complex derivatives portfolios. Quantum optimization algorithms — including QAOA (Quantum Approximate Optimization Algorithm) — have demonstrated potential to find materially better solutions to these problems than classical approximation methods.

IBM researchers have demonstrated quantum algorithms for specific financial applications — including simulation, optimization, and machine learning — on IBM Quantum backends, providing concrete evidence of emerging quantum advantage in financial services (Egger et al., IEEE Transactions on Quantum Engineering). A comprehensive 2025 review of quantum computing in finance confirms that quantum algorithms for financial modeling, portfolio optimization, and risk management are advancing from theoretical promise toward practical application, with quantum machine learning showing particular near-term potential (Aggarwal et al., 2025 Global AI Summit). Portfolio optimization and risk management are among the most promising near-term quantum application areas in financial services (Chamma et al., 2023).

6.1.2 Simulation and Modeling.

Quantum simulation offers the potential to model complex financial systems that exceed classical computational capacity:

- **Monte Carlo Acceleration:** Quantum amplitude estimation provides a quadratic speedup over classical Monte Carlo methods for pricing derivatives and computing risk metrics — potentially reducing computation times for complex structured products from hours to minutes. IBM Quantum demonstrations have validated this speedup on financial simulation problems (Egger et al., IEEE TQE).
- **Credit Risk Modeling**: Quantum machine learning may enable more accurate modeling of correlated default scenarios in large credit portfolios — improving stress testing under systemic risk conditions.

- **Climate and ESG Risk Modeling:** Quantum simulation's ability to model complex, correlated systems has direct applications in climate risk scenario modeling for financial institutions' climate disclosures and regulatory stress tests.
- **Central Bank Stress Testing:** Quantum simulation could enable central banks and financial regulators to model systemic risk scenarios at a scale and correlation depth that current infrastructure cannot support — a significant advancement for financial stability monitoring.

6.2 Quantum Sensing

Quantum sensing exploits the extreme sensitivity of quantum states to measure time, position, and field strength with precision unattainable by classical instruments — offering the financial sector a different category of advantage than computing: not faster answers to hard problems, but higher-fidelity inputs to the problems it already solves.

- **Ultra-Precise Trade Timestamping:** Quantum optical atomic clocks deliver roughly 100x the precision of conventional atomic clocks. For high-frequency trading, this enables tighter synchronization of trading algorithms across venues and more accurate reconstruction of trade sequencing and market impact — directly relevant to MiFID II-style timestamping and best-execution compliance requirements.
- **Infrastructure and Fraud-Adjacent Monitoring:** Quantum magnetometers and related sensors are being explored for physical infrastructure monitoring — including data center security and detection of unauthorized physical access to network chokepoints such as fiber and cable junctions that carry financial transaction traffic.
- **Optimization Linkage:** Because quantum sensing improves the precision of the data feeding risk and execution models (timestamps, positioning, environmental measurements for physical asset-backed instruments), it functions as an optimization multiplier — sharpening the inputs to the same portfolio, execution, and risk-scenario optimization problems addressed in 6.1, rather than replacing the computation itself.

6.3 Quantum Communications

Quantum communications — principally quantum key distribution (QKD) — offers information-theoretic security guarantees for the highest-sensitivity financial channels, complementing the PQC migration path with a physics-based layer for use cases where the stakes justify it.

- **Interbank Pilot at Scale:** The Monetary Authority of Singapore, together with DBS, HSBC, OCBC, and UOB, published a technical report in September 2025 on a QKD sandbox proof-of-concept evaluating QKD's viability for securing financial communications — one of the largest coordinated multi-bank QKD trials to date.
- **Quantum-Secured Tokenized Assets:** HSBC and Quantinuum demonstrated quantum-secure technology for distributing tokenized physical gold on HSBC's Orion platform, combining post-quantum cryptography with Quantinuum's Quantum Origin quantum-randomness technology to protect digital assets against "store now, decrypt later" attacks — a direct optimization-adjacent use case, since tokenized commodity settlement depends on trust in the transaction channel to unlock the efficiency gains tokenization promises.

- **European Infrastructure Buildout**: EuroQCI, the EU's quantum communication infrastructure initiative, is deploying national terrestrial QKD networks across 26 member states with a satellite component (Eagle-1) targeted for 2026, aiming for full operational status by 2027 — creating a public-infrastructure backbone European financial institutions can eventually connect into rather than building bilateral QKD links independently.
- **Additional Institutional Pilots:** Erste Group piloted quantum encryption in banking infrastructure in February 2026, and research on quantum-safe IPsec for banking networks points toward hybrid architectures that layer QKD atop existing network security protocols during the transition period.

6.4 Artificial Intelligence + Quantum Convergence

Beyond quantum computing, sensing, and communications as standalone modalities, a fourth opportunity is emerging at their intersection with AI: hybrid quantum-classical machine learning. The dominant near-term pattern is not replacement of existing AI stacks but augmentation — quantum components inserted into classical pipelines at the specific points where optimization, sampling, or complex search spaces strain classical methods.

- **Fraud and Anomaly Detection:** Quantum kernel methods and variational quantum models are being tested as components within larger fraud-detection pipelines, exploiting superposition and entanglement to sharpen sensitivity to faint, non-linear signals in transaction graphs and time-series data that are difficult for classical models to isolate. Recent research, including the Q-SYNTH hybrid quantum-classical adversarial augmentation framework for imbalanced fraud detection (2026), reports faster training and strong classification performance versus classical-only baselines on the class-imbalance problem that characterizes real-world fraud data.
- **Market and Risk Prediction:** Hybrid classical-quantum neural networks are being applied directly to financial forecasting — for example, HQNN-FSP, a hybrid architecture for regression-based stock market prediction, and a 2026 benchmark study comparing quantum and classical machine learning specifically for financial prediction tasks — providing early empirical grounding for where quantum-enhanced models do and don't outperform classical ones.
- **Generative Modeling:** Quantum generative models are an active research frontier with direct relevance to financial modeling and synthetic data generation. In February 2026, Lockheed Martin and Xanadu launched a joint research initiative on quantum-native, Fourier-based generative operations designed to capture data structure that classical generative methods cannot — with finance explicitly named alongside defense and pharmaceuticals as a target application domain. Related IEEE research on hybrid classical-quantum generative algorithms points toward applications in synthetic financial data generation and scenario modeling.
- **Institutional Adoption:** Quantum-AI pilots are now a standard component of bank quantum research programs rather than a novelty — Crédit Agricole is working with Pasqal, HSBC with Quantinuum, and more than 15 global banks (including JPMorgan Chase, Goldman Sachs, BBVA, and Barclays) have active programs spanning fraud detection, risk modeling, and derivative pricing that increasingly incorporate a quantum machine learning component.

This opportunity carries a dual-use dimension worth naming explicitly, consistent with the risk/opportunity framing at the start of this section: generative AI is simultaneously one of the financial

sector's most significant emerging fraud threats, meaning the same convergence of AI and quantum techniques that strengthens institutions' detection capabilities is also available to adversaries. Institutions pursuing quantum-AI opportunities for defense should assume the same tools are being evaluated offensively.

A more acute version of this risk emerges once quantum and generative AI target the same layer: authentication. Once a cryptographically relevant quantum computer can forge digital signatures under today's signature schemes, AI-generated content — synthetic documents, fabricated communications, manipulated transaction records — could be signed with forged but cryptographically valid credentials, making it indistinguishable from legitimate, authentically-signed records. This is a different failure mode than fraud evading a detection model: it is the collapse of the evidentiary basis for distinguishing real records from fabricated ones at all. Signature-scheme migration (ML-DSA, SLH-DSA, and eventually FN-DSA) should therefore be prioritized on the same urgency as encryption migration, not treated as a secondary concern behind confidentiality.

This compounding risk is also structural, not just technical. Oversight institutions — courts, financial regulators, standard-setting bodies — operate on rulemaking timelines measured in years, while quantum-AI capability is compounding on a timeline measured in months. This is not a temporary lag that regulation will eventually close: if enforcement mechanisms, evidentiary standards, and audit methodologies are built on assumptions — stable cryptographic guarantees, distinguishable authentic records, humanly-auditable AI decisions — that quantum-AI convergence invalidates, the resulting enforcement gaps can persist independent of how quickly rules are eventually updated. Institutions should not assume regulatory catch-up is guaranteed, and should build internal governance — provenance tracking, cryptographic audit trails, human-in-the-loop review — that does not depend on external oversight closing this gap on any particular timeline. (See Section 4.1.2 for the related retroactive exposure of legal and evidentiary records under HNDL.)

Beyond that dual-use risk, quantum-AI convergence raises a distinct set of ethical questions institutions should address before, not after, deployment. The first is explainability: quantum algorithms are inherently harder to audit than classical models, and the absence of established methods for quantum AI explainability complicates accountability in exactly the high-stakes, regulated applications — credit scoring, lending, fraud adjudication — where this convergence is being piloted. This is not hypothetical: the EU AI Act classifies credit scoring and lending as high-risk and mandates transparency, human oversight, and record-keeping, while the CFPB has affirmed that institutions remain responsible for outcomes produced by AI and must provide adverse-action notices that meaningfully explain AI-driven decisions — obligations a hybrid quantum-classical model must still satisfy even where its internal mechanics resist conventional interpretability techniques. The second is access equity, sometimes termed the "quantum divide": quantum computing's capital and infrastructure requirements mean that only well-resourced institutions can currently access these capabilities, raising the risk that quantum-AI advantage compounds rather than levels existing disparities in credit access, pricing, and competitiveness between large and smaller financial institutions. UNESCO and other bodies have proposed ethical principles for quantum development — transparency, accountability, equity, and non-maleficence — that map directly onto financial regulators' existing fair-lending and model-governance frameworks, suggesting institutions can extend current AI governance structures to cover quantum-AI systems rather than building parallel ones from scratch.

Quantum + AI: Guard and Attack

Quantum-enhanced AI can defend financial systems or dismantle trust in them. Quantum machine learning can sharpen fraud and anomaly detection at transaction scale. But the same convergence lets adversaries generate synthetic transaction patterns that defeat classical fraud models, optimize social engineering at machine speed, and — once quantum computers can forge signatures — sign fabricated records so they're indistinguishable from real ones. Regulators must treat AI system security and signature integrity as core components of quantum risk, not adjacent concerns.

7. Intersection of Quantum, AI, and Blockchain

Three of the most consequential technology transformations of the current era are converging in ways that create compounding risks and amplified opportunities. Understanding this convergence is essential for designing resilient financial infrastructure.

7.1 How the Technologies Converge

Each technology addresses a different dimension of trust and capability in financial systems: Blockchain provides decentralized, tamper-evident record-keeping and programmable transaction logic. AI provides intelligent pattern recognition, prediction, and optimization. Quantum computing provides exponentially faster computation for specific problem classes — including those that underpin blockchain security and AI training.

Their convergence creates a layered architecture for quantum-era financial infrastructure: quantum-resilient cryptography provides the security foundation; blockchain provides the transparent, auditable data and transaction layer; AI provides the intelligence and optimization layer. The integrity of this architecture depends on each layer being quantum-resilient — a weakness in any layer propagates upward and compromises the entire architecture.

7.2 Use Cases

- **Quantum-Secured Tokenized Assets:** Real-world asset (RWA) tokenization platforms — a core IDAI focus area — built on quantum-resilient blockchain infrastructure, where digital representations of bonds, real estate, or commodities carry quantum-resistant digital provenance certificates.
- **AI-Augmented Quantum Risk Management:** AI systems trained on quantum simulation outputs to generate real-time quantum-risk scores for financial institution cryptographic infrastructure — flagging systems approaching vulnerability thresholds as quantum hardware advances. The 2025 Global AI Summit research confirms that quantum-supervised and unsupervised machine learning are advancing rapidly toward financial risk applications (Aggarwal et al.).
- **Quantum Vault Architecture for Digital Currency:** A novel model proposed by Broadbent et al. (IEEE QCE 2024) delegates quantum storage and processing to a trusted intermediary — a "quantum vault" — alleviating the need for end-user quantum hardware. This architecture is directly applicable to CBDC design: central banks or regulated custodians could operate quantum vaults that provide quantum-grade security for digital currency transactions without requiring quantum-capable devices in consumers' hands. This is the most immediately practical pathway to quantum-native digital currency infrastructure.
- **Quantum Money and Anti-Counterfeiting:** The quantum mechanical principle of no-cloning — which makes it physically impossible (not merely computationally difficult) to copy a quantum state — provides the foundation for digital currencies that are intrinsically immune to counterfeiting. Unlike classical cryptographic security, quantum money security does not depend on computational hardness assumptions that future technology could overcome (Mishra et al., 2023; Broadbent et al., 2024). Governments and central banks designing next-generation digital

currency should evaluate quantum money principles as a long-term framework for unforgeable sovereign digital assets.

- **Decentralized Quantum Key Distribution Networks:** DLT-based coordination layers for QKD networks, enabling financial institutions to share quantum-secured channels without centralized key management infrastructure.
- **Quantum-AI Fraud Detection:** Real-time transaction monitoring using quantum optimization to search anomaly patterns in high-dimensional transaction graphs, with blockchain providing an immutable audit trail of detection events.
- **Quantum-Enhanced Web 3.0 Financial Infrastructure:** Beyond defending blockchain against quantum threats, quantum and post-quantum encryption and verification algorithms can actively improve blockchain performance — enabling a more secure, decentralized, and value-driven Web 3.0 financial ecosystem (Ren et al., Proceedings of the IEEE 2024). Decentralized Autonomous Organizations (DAOs), Decentralized Finance (DeFi) platforms, and digital identity systems built on quantum-resilient Web 3.0 infrastructure will be foundational to the next generation of government financial services.

7.3 Novel Risks from Quantum-AI-Blockchain Convergence

The risks created by this convergence are not simply the sum of quantum risk, AI risk, and blockchain risk considered separately — they compound. A vulnerability in one layer (say, a forgeable signature scheme) becomes materially more dangerous once paired with a capability in another layer (an autonomous agent that can act on that forgery at machine speed, irreversibly, on-chain). The risks below are organized around where that compounding is most acute.

- **Agentic AI with Direct On-Chain Custody:** AI agents are no longer just analyzing blockchain data — they are holding private keys and executing transactions directly. Agent-settled on-chain transactions reached roughly 176 million, totaling more than $73 million, between May 2025 and April 2026. Giving an agent direct control of a private key means a leaked key or a hallucinated instruction produces immediate, irreversible loss; because DeFi is composable, a single flawed agent action can cascade across DEX routers, lending protocols, bridges, and token approvals before a human notices. Partial mitigations like Ethereum's EIP-7702 (scoped, temporary permissions) and session keys reduce blast radius but don't address the underlying exposure once the signature schemes securing those keys are themselves quantum-forgeable.
- **Multi-Agent Systemic Contagion:** Multi-agent frameworks (e.g., the TradingAgents architecture, now a reference implementation across major banks) mean a single error — an agent misclassifying a transaction, misreading a KYC document, misinterpreting a corporate action — can propagate through linked agents and produce compliance violations or real monetary losses at a scale no individual model failure would cause alone. This structural interdependency was significant enough that ACSC, CISA, NSA, and counterpart agencies in Canada, New Zealand, and the UK issued joint guidance on secure agentic AI adoption in May 2026.
- **Autonomous Exploit Discovery Outpacing Human Review:** As of early 2026, autonomous AI agents can identify, construct, and execute smart contract exploits faster than audit firms can review the underlying code — collapsing the assumption that attacks unfold on human timescales. Layered onto quantum-vulnerable signature schemes, this means the traditional

security model of "patch before exploitation" may not hold for either the code layer or the cryptographic layer going forward.

- **6G-Native Attack Surface Expansion:** 6G's device density and AI-native network management will connect vastly more endpoints to blockchain and DeFi rails, most of them running quantum-vulnerable cryptography. Systemic risk modeling of scenarios combining quantum cryptographic breakthroughs, AI model compromise, and financial automation failure shows cascade multipliers exceeding 8.0x — an order-of-magnitude amplification of systemic exposure relative to any single-layer failure.
- **Web3 Identity and Governance Manipulation:** Self-Sovereign Identity systems, which underpin Web3's decentralized-identity model, rely on the same asymmetric cryptography vulnerable to quantum forgery — meaning the identity layer itself, not just transaction confidentiality, is exposed. Separately, deepfake-powered social engineering is already being used to manipulate DAO governance votes and token approvals, undermining the trust assumptions decentralized governance depends on.
- **Non-Human Identity Explosion:** Non-human identities (AI agents, service accounts, API keys) now outnumber human identities roughly 80-to-1 inside enterprise environments, and 80% of 2026 identity breaches involved a compromised non-human credential. AI agents compound this by dynamically requesting new permissions at runtime and spawning sub-agents — meaning the identity-governance problem this convergence creates is arguably larger in raw attack surface than the human-facing risks the report has focused on so far, and it needs its own quantum-safe machine-identity strategy rather than being treated as a subset of user authentication.
- **Liability and Accountability Ambiguity:** When an autonomous agent transacting through a smart contract causes a loss, there is no settled framework for assigning liability among the AI model developer, the deploying institution, the smart contract's author, and the agent's own decision-making — a gap regulators and courts have not resolved and that compounds directly with the "regulatory obsolescence" risk already noted in Section 6.4.
- **Cascading/Compounding Systemic Risk as Its Own Category:** Rather than treating quantum, AI, and blockchain failures as risks to be assessed independently in institutional risk registers, the cascade-multiplier research above suggests this convergence should be modeled as a distinct systemic risk category with its own stress-testing methodology — since additive risk models will systematically understate exposure.

8. Quantum Implications for Blockchain Ecosystems

Blockchain and distributed ledger technology occupy a unique position in the quantum risk landscape. Blockchain systems are more exposed to quantum cryptographic attacks than many classical financial systems, because their signature schemes are public and immutable by design — but well-designed blockchain governance can also be a powerful enabler of quantum-resilient transition.

8.1 Vulnerability of Current Blockchain Cryptography

The cryptographic security of blockchain networks rests almost entirely on elliptic curve digital signature algorithms — directly vulnerable to Shor's algorithm. The vulnerability is structurally more severe than traditional PKI: once a transaction is broadcast on the blockchain, the sender's public key is exposed. A quantum adversary with a CRQC could derive a private key from its public key and inject fraudulent transactions before the original confirms — a race condition that worsens as quantum hardware matures.

Peer-reviewed research published in Proceedings of the IEEE (November 2024) frames this challenge through an "ambilateral" lens: quantum computing simultaneously (1) disrupts the classic computing cryptographic systems protecting blockchain data security, and (2) reshapes modern cryptography with enhanced quantum computing and communication capabilities that actively improve blockchain performance (Ren et al.). This ambilateral view is critical for government policy makers — the quantum transition is not purely defensive. Institutions that invest only in cryptographic defense while ignoring quantum-enhanced blockchain capabilities will be strategically disadvantaged relative to early movers who pursue both.

For government financial applications built on blockchain — including CBDCs, government payment systems, land registry tokenization, and public procurement — quantum cryptographic vulnerability directly impacts sovereign financial infrastructure. The urgency is compounded by the governance complexity of blockchain upgrades: unlike traditional systems, protocol changes require consensus among all network participants.

8.2 Timeline Considerations

The quantum threat to blockchain evolves in phases. Near-term (pre-Q-Day): HNDL attacks on encrypted off-chain communications between blockchain nodes represent the primary risk. As quantum hardware matures toward cryptographically relevant qubit thresholds, the window for real-time transaction replay attacks narrows. Post-Q-Day, exposed public keys on major blockchain networks could be targeted systematically.

Enterprise blockchain networks used in financial services typically require 18–36 months to plan, test, and execute a major protocol upgrade. Given Q-Day estimates of 5–15 years, migration planning must begin immediately.

8.3 Quantum Transition Strategies

- **NIST IR 8547 Migration Timeline:** NIST's finalized transition roadmap sets the timeline that should anchor all planning below: RSA, ECDSA, ECDH, and DH are formally deprecated by 2030, with full disallowance — meaning these algorithms may no longer be used at all — by 2035. Symmetric cryptography at 112-bit security is likewise disallowed from 2030, requiring longer key lengths going forward. NIST accepts hybrid PQ/T (post-quantum/traditional) solutions as a transitional measure but cautions against treating them as a permanent end-state; hybrid should be retired in favor of PQC-only algorithms once systems mature. Executive Order 14412 has since converted IR 8547's 2030 deprecation date into a binding compliance deadline for federal high-value assets and high-impact systems, while OMB M-26-15 sets 2035 as the full-migration date for remaining systems (see Section 4.1.2). Blockchain platforms and institutions in this ecosystem should treat 2030 — not 2035 — as the working internal deadline for signature and key-establishment migration, since regulatory and counterparty pressure will move faster than the outer legal limit. NIST frames the underlying planning logic through Mosca's Theorem: organizations must begin migration once the years data must remain secure (X) plus the time needed to complete migration (Y) exceeds the years remaining before a cryptographically relevant quantum computer arrives (Z) — an argument for starting now rather than waiting for further clarity.
- **Protocol-Level PQC Integration:** Work with blockchain platform developers (Hyperledger Foundation, Ethereum Foundation, R3) to integrate NIST-standard PQC signature schemes into core protocol upgrades, targeting the 2030 deprecation date above rather than the 2035 outer limit. Post-quantum migration methods and quantum-resistant signatures offer robust solutions to safeguard blockchain against quantum threats (Ren et al., Proceedings of the IEEE 2024).
- **Wallet Migration Guidance:** Issue guidance to institutional blockchain wallet operators on migrating to quantum-resistant wallet formats before Q-Day. For government-operated CBDC systems, evaluate quantum vault architectures (Broadbent et al., IEEE QCE 2024) as a practical pathway to quantum-grade security without requiring consumer-side quantum hardware.
- **Smart Contract Security Audit:** Audit smart contracts that implement cryptographic operations natively for quantum vulnerabilities. Replace exposed primitives with PQC equivalents.
- **Node Communication Security:** Upgrade inter-node communication protocols to use hybrid TLS with PQC key exchange — protecting network communications from HNDL attacks now.
- **Pursue Quantum Enhancement, Not Just Defense:** Post-quantum migration is necessary but not sufficient. Quantum and post-quantum encryption and verification algorithms can actively improve blockchain performance — creating a more secure, decentralized, and high-value Web 3.0 financial ecosystem (Ren et al.). Government blockchain programs should evaluate quantum-enhanced capabilities as part of their long-term architecture roadmap.
- **Governance for Crypto-Agility:** Establish formal governance processes — technical working groups, stakeholder approval thresholds, testnet validation procedures — for future cryptographic algorithm transitions without disruptive emergency upgrades.

8.4 Role of IDAI and the GBA in Standards and Coordination

IDAI and the GBA are nonprofit organizations jointly positioned to accelerate quantum-resilient blockchain standards across the public sector financial ecosystem:

- Develop quantum-resilient reference architectures for government blockchain applications — CBDC infrastructure, government payment systems, land registry tokenization, and public procurement.
- Coordinate with NIST, IETF, and ISO on financial sector use case requirements for PQC standards development.
- Work with government contracting authorities to include quantum-resilience requirements in blockchain procurement specifications — ensuring new government blockchain infrastructure is not built on already-obsolete cryptographic foundations.
- Address DAO governance quantum security: DAO governance mechanisms using ECC-signed on-chain ballots must migrate to quantum-resistant signatures without compromising decentralization.

9. Governance: Legal, Regulatory, and Standards, Considerations

The transition to quantum-resilient financial infrastructure requires coordinated regulatory, standards, and policy frameworks. No single institution or nation can achieve quantum resilience in isolation — the interconnected nature of global finance demands coordinated international action.

9.1 Legal

- **Contractual Liability for Quantum-Computing-as-a-Service (QCaaS):** Most institutional quantum access runs through vendor-controlled, cloud-hosted stacks. Liability is complicated by the probabilistic nature of quantum results — demonstrating that an erroneous output stems from a vendor breach rather than normal technological uncertainty requires precisely defined contractual metrics that most current agreements lack. Institutions should require standards-based proof of control (documented error rates, calibration logs, algorithm versioning) as a contractual deliverable rather than accepting vendor assurances alone.
- **Evidentiary Integrity Under Retroactive Decryption:** As addressed in Sections 4.1.2 and 7.3, HNDL creates a distinct legal exposure: court filings, regulatory submissions, and privileged attorney-client communications encrypted today could be decrypted years later, retroactively undermining privilege claims and the evidentiary finality of settled matters. Legal and compliance functions should treat privileged communications with the same migration urgency as financial data.
- **Liability Ambiguity for Autonomous Agent Actions:** No settled legal framework currently exists for assigning liability when an AI agent transacting through a smart contract — potentially secured by a quantum-forged signature — causes a loss. Responsibility may fall on the model developer, the deploying institution, the smart contract author, or some combination, and this ambiguity should be treated as an open legal risk rather than resolved by default through existing vendor contracts.
- **Data Protection Intersection:** GDPR and similar regimes treat data as "anonymized" based on present-day re-identification difficulty; HNDL-enabled decryption could retroactively re-identify data institutions certified as anonymized, creating potential compliance exposure under data protection law for disclosures made years before quantum decryption became feasible.
- **Insurance Coverage Gaps:** Cyber insurance policies are generally underwritten against present-day threat models and may not address harvest-now-decrypt-later losses that materialize years after the underlying breach. Institutions should review whether current policies cover retroactive decryption events and, where they don't, treat this as a named gap requiring either policy amendment or a documented risk acceptance.

9.2 Regulatory

- **United States (Advisory, Not Yet Mandatory):** The Federal Reserve, OCC, and FDIC have each incorporated post-quantum readiness into supervisory communications, but as of mid-2026 all sector-specific PQC guidance (OCC, Fed, SEC, FINRA, FFIEC) remains advisory — no binding US

private-sector PQC mandate exists yet. A documented, risk-based PQC readiness program aligned with NIST and CISA guidance is treated as evidence of due diligence under GLBA, the FFIEC IT Handbook, and OCC/Fed/FDIC examination programs, even absent a formal rule. Financial regulators are expected to move from advisory to binding guidance within the next 12–24 months, building on the OMB M-23-02 / M-26-15 and EO-14412 framework already established for federal systems (Section 4).

- **European Union — DORA (Currently the Strongest Binding Instrument):** The Digital Operational Resilience Act (Regulation (EU) 2022/2554), fully applicable since January 17, 2025, is the strongest EU instrument imposing explicit, binding quantum-security-adjacent obligations today. Its implementing technical standards (Commission Delegated Regulation (EU) 2024/1774) require EU financial entities to maintain a formal encryption and cryptographic-controls policy that addresses updating cryptographic technology in response to cryptanalysis developments — effectively mandating crypto-agility as a documented control, not just a best practice.
- **European Union — NIS2 Amendment (Proposed January 2026):** The European Commission's January 2026 proposal to amend NIS2 would require member states to adopt national PQC transition policies as part of their cybersecurity strategies, moving crypto-agility and migration planning from "good practice" to "expected practice" across critical infrastructure, including finance.
- **European Central Bank and EBA/ESMA/EIOPA:** The ECB has flagged a forthcoming supervisory letter on quantum computing implications, with institutional action plans due by October 31, 2026. The European Supervisory Authorities (EBA, EIOPA, ESMA) have jointly issued a statement supporting the ESRB's warning on quantum as an emerging systemic risk.
- **United Kingdom — FCA:** The FCA has published a research note on quantum computing applications in UK financial services, concluding that near-term new regulation is unlikely but that supervisory expectations for 2026–2027 will include documented quantum risk assessments, migration roadmaps, vendor verification, scenario testing, and explicit board-level accountability.
- **Singapore — MAS:** MAS continues to lead with the most forward-leaning guidance globally, building on the QKD sandbox described in Section 6.3, and is supporting the Q-FINEX testbed connecting quantum research to real-world banking applications.
- **Defense-Adjacent Standard Worth Tracking — NSA CNSA 2.0:** While not a financial regulator, CNSA 2.0 (the NSA's Commercial National Security Algorithm Suite) sets phased deadlines relevant to any financial institution serving government or defense-adjacent clients: CNSA 2.0 preferred for software/firmware signing by 2025 and exclusive by 2030; networking equipment (VPNs, routers) to prefer it by 2026 and use it exclusively by 2030; operating systems and custom applications to reach exclusive use by 2033. Institutions with government banking relationships should track CNSA 2.0 deadlines alongside NIST's civilian timeline, as the two will drive different parts of a vendor's stack on different schedules.
- **International Coordination:** The G7 Cyber Expert Group roadmap (Section 4) remains the primary coordinating mechanism across US, EU, UK, and other G7 regulators, recommending critical-system migration in the 2030–2032 window.

9.3 Standards

9.3.1 ISO Standards

- **ISO/IEC 14888 (Digital Signatures):** Under active revision to incorporate quantum-resistant signature schemes aligned with NIST PQC standards.
- **ISO/IEC 18033 (Encryption Algorithms):** Being updated to reference PQC key encapsulation mechanisms.
- **ISO/IEC 27001 (Information Security Management):** Future revisions expected to incorporate quantum-resilience requirements as a baseline control category.
- **ISO/TC 307 (Blockchain and DLT Standards):** Developing guidance on quantum-resilient DLT implementation — directly relevant to IDAI and GBA workstreams.
- **ISO/IEC 18033-2 (Update):** Classic McEliece achieved full ISO/IEC standardization on July 15, 2026 — the first post-quantum cryptographic algorithm to reach completed (not draft) ISO/IEC standard status. This is a more significant milestone than the current draft note suggests and should be flagged as such rather than left folded into a general "being updated" bullet.
- **ISO/IEC 14888-4:** Now at first committee draft stage, covering stateful hash-based signature mechanisms — relevant to the digital signature scheme discussion in 9.3.1 and should sit alongside the existing 14888 reference.

9.3. 2 US Government Standards and Guidelines

- **FIPS 203/204/205 (PQC Standards, 2024):** The foundational post-quantum cryptographic standards — see Section 5 for detail.
- **NIST SP 800-131A Rev. 3 (Transitioning Cryptographic Algorithms):** Migration guidance including timelines and backward-compatibility requirements for transitioning away from deprecated algorithms.
- **NIST Cybersecurity Framework 2.0:** The updated CSF includes provisions for emerging technology risks — quantum cryptography migration is an expected addition in forthcoming profile documents.
- **OMB M-23-02:** Requires federal agencies to inventory quantum-vulnerable cryptographic systems and submit migration plans — the direct regulatory precedent for financial sector requirements.
- **NIST SP 1800-38 (NCCoE Practice Guide):** A three-volume practical migration playbook — Volume A (preparation and use-case framing), Volume B (cryptographic discovery methodology and threat examination), and Volume C (interoperability and performance testing of PQC-ready algorithms) — that complements the higher-level IR 8547 timeline already cited in Section 8 with an operational how-to. This belongs in 9.3.2 alongside IR 8547 and SP 800-131A.
- **NSA CNSA 2.0:** Recommend cross-referencing the CNSA 2.0 timeline (detailed under the new 9.2 entry above) from 9.3.2, since it functions as a de facto standard for any institution with defense- or government-adjacent counterparties, distinct from but parallel to NIST's civilian-sector timeline.

(For U.S.-regulated financial institutions, OMB M-23-02 and NIST guidance provide the current compliance framework. Financial regulators (OCC, FDIC, Federal Reserve, SEC) are expected to issue quantum-resilience guidance building on the NIST standards framework within the next 12–24 months.)

9.3.3 ITU Standards

- **ITU-T X.1710 Series (Quantum-Resistant Cryptography Framework):** Security framework for quantum-resistant cryptography deployment in communications networks — relevant to cross-border payment infrastructure.
- **ITU-T Y.3800 Series (Quantum Key Distribution Networks):** Technical standards for QKD network architectures — relevant to central banks and financial market infrastructure operators exploring QKD for high-value secure communications.
- **ITU Focus Group on Quantum Information Technology for Networks (FG-QIT4N):** Produced technical reports on quantum computing threats to telecom and financial networks, including timelines and mitigation frameworks. ITU-T's QKD network standardization work now spans more than 40 active work items across four groups — Study Group 13 (network aspects), Study Group 17 (security aspects), Study Group 11 (high-layer protocols), and the concluded Focus Group FG-QIT4N, whose 2021 technical reports now feed directly into the SG13/SG17 work program for the 2025–2028 study period. This is a broader and more active effort than the current single-bullet treatment suggests, and the Y.3800-series standardization roadmap (last updated 2023, with a new supplement in progress as of September 2025) should be cited by name alongside X.1710 and Y.3800 as the document actually tracking near-term milestones.

(For international financial institutions, ITU standards provide the interoperability framework that aligns national PQC implementations with the global communications infrastructure payment networks depend upon.)

9.3.4 ETSI and IETF Standards

- **ETSI Quantum-Safe Cryptography Working Group:** Publishes implementation roadmaps and security analysis documents that complement the NIST standards with deployment-scenario and algorithm-selection guidance — useful as practical companion material to the more abstract NIST IR 8547 timeline already cited in Section 8. ETSI has also launched a standard for Key Encapsulation Mechanisms with Access Control ("Covercrypt"), relevant to fine-grained access control over encrypted financial data.
- **IETF Post-Quantum TLS (draft-ietf-tls-mlkem):** The IETF is standardizing ML-KEM as a NamedGroup for TLS 1.3 key agreement — the protocol underpinning most encrypted financial-system network traffic. As of July 2026 this remains an active Internet-Draft (draft-09), not yet a published RFC, and a real disagreement persists within the working group over whether standalone ML-KEM should be permitted or whether hybrid ECDHE-MLKEM (draft-ietf-tls-ecdhe-mlkem) should be required — the more conservative hybrid approach most vendors are deploying today. Institutions should track this as a standard still in motion rather than settled, and should not assume today's hybrid TLS configurations are the final target state.

- **Why This Matters Alongside ISO and ITU:** ISO/IEC and NIST standardize the algorithms; ITU-T standardizes how QKD networks are architected; ETSI and IETF standardize how those algorithms actually get deployed in the internet and telecom protocols (TLS, IPsec) that carry financial transaction traffic day to day. All four layers need to be tracked together — an institution can be fully compliant on algorithm choice and still be exposed if the transport-layer protocol carrying that algorithm hasn't finished standardizing.

10. Implementation Roadmap for Financial Institutions

Effective quantum-resilience migration begins not with a roadmap, but with an assessment. Financial institutions require a structured framework for understanding their specific quantum risk exposure before committing to migration timelines and investment levels.

10.1 Quantum Risk Assessment Framework (Phase 0)

1. Business Impact of Failure	Model the financial, operational, reputational, and regulatory impact of cryptographic compromise — both from a quantum attack and from a failed migration. This drives prioritization and investment levels.
2. Cryptographic Dependency Mapping	Inventory all systems using RSA, ECC (ECDSA, EdDSA, ECDH), or Diffie-Hellman. Map dependencies on third-party certificates, HSMs, and vendor-provided cryptographic libraries.
3. Data Sensitivity & Longevity	Identify data categories whose confidentiality must be protected for more than 5 years. This data is harvest-vulnerable today. Prioritize its cryptographic protection immediately, regardless of Q-Day timeline.
4. System Migration Complexity	Score each system on upgrade cycle length, vendor quantum-readiness, regulatory constraints on algorithm changes, and interconnectedness. High-complexity systems require longer lead times.
5. Threat Actor Exposure	Assess whether encrypted data is of sufficient strategic value to attract nation-state HNDL collection. Institutions with significant sovereign, defense, or critical infrastructure clients face elevated risk.

10.2 Phased Implementation Roadmap

Phase 1: Prepare (Now — 18 Months)

- Complete cryptographic inventory across all systems, vendors, and third-party dependencies
- Classify all data by sensitivity lifetime; identify harvest-vulnerable data categories
- Deploy hybrid TLS (classical + ML-KEM) for highest-sensitivity external communications
- Engage HSM vendors on PQC roadmap commitments and certification timelines
- Brief board and executive team on quantum risk; assign executive accountability
- Engage regulators proactively to understand expected quantum-resilience requirements
- Assess third-party and supply chain quantum readiness for critical vendors

Phase 2: Transition (18 Months — 5 Years) Change to 3 years given that NIST recommends transition by 2030?

- Migrate highest-priority systems (core banking authentication, payment network interfaces) to NIST PQC algorithms
- Replace expiring TLS certificates with hybrid PQC/classical certificates across customer-facing systems
- Upgrade or replace HSMs to PQC-capable hardware as current devices reach end-of-life
- Implement crypto-agility frameworks for blockchain-based systems; execute governance processes for PQC protocol upgrades
- Establish continuous quantum-risk monitoring capability — tracking quantum hardware progress against migration status

Phase 3+: Sustain (5+ Years — Ongoing)

- Complete migration of all systems to PQC-standard cryptography
- Maintain crypto-agility as an organizational capability — institutionalize the ability to respond to future cryptographic transitions
- Engage in industry and regulatory working groups to contribute implementation experience to standards evolution
- Begin exploration of quantum opportunity capabilities — optimization, simulation, and quantum-enhanced AI
- Monitor for cryptanalytic advances against PQC algorithms; maintain contingency plans for rapid algorithm substitution

10.3 Risk Management

10.3.1 Risk Categories

- **Implementation Risk:** PQC algorithms are newer and less battle-tested than classical algorithms. Incorrect implementation can introduce vulnerabilities independent of quantum attacks. Require independent cryptographic audits of all PQC implementations.
- **Interoperability Risk:** During transition, mixed environments where some systems use PQC and others classical algorithms must be carefully managed to prevent security gaps at the interface.
- **Algorithm Risk:** While NIST's PQC standards represent the current best available options, the possibility of cryptanalytic breakthroughs against lattice-based algorithms cannot be excluded. Maintain algorithm diversity — combining lattice-based and hash-based algorithms — to reduce this risk.
- **Timeline Risk:** If quantum hardware advances faster than consensus estimates, the transition window narrows. Monitor quantum computing progress quarterly and adjust migration velocity accordingly.
- **Budget and Resource Risk:** PQC migration requires specialized cryptographic expertise that is currently scarce. Invest in staff training and retain external quantum-security specialists for migration planning and execution.
- **Vendor and Supply Chain Risk:** Institutions depend on third parties — cloud QCaaS providers, HSM and PKI vendors, blockchain platform developers (Hyperledger, Ethereum Foundation, R3) — whose own PQC readiness is outside institutional control. A vendor lagging on migration becomes an institution's exposure by extension, and probabilistic quantum results make vendor breach even harder to prove contractually (Section 9.1).
- **Legacy and Embedded System Risk:** Some systems — embedded hardware, fixed-function HSMs, long-lived payment terminals — cannot be upgraded through normal software patching and may require full replacement to become quantum-resistant. These systems often go undiscovered until a cryptographic inventory is complete, and can become the long pole in an otherwise on-schedule migration.
- **Performance and Operational Impact Risk:** PQC algorithms have materially larger key and signature sizes than their classical counterparts (e.g., ML-DSA signatures are several times larger than ECDSA's). This can degrade latency-sensitive systems — high-frequency trading infrastructure, blockchain transaction throughput (Section 6, Section 8) — in ways that are a real operational cost of migration, not just an implementation detail.
- **Cryptographic Agility Debt Risk:** Migrating to PQC without also building modular, swappable cryptographic architecture (Section 5.4) simply recreates today's fragility for the next transition. A hard-coded PQC implementation is not meaningfully safer, long-term, than a hard-coded classical one.
- **Regulatory and Compliance Divergence Risk:** US (NIST/EO-14412), EU (DORA/NIS2), and other jurisdictions' PQC mandates carry different algorithms, timelines, and enforcement mechanisms (Section 9.2), and requirements are still actively evolving. Migration plans built around today's rules may require costly rework as binding guidance replaces advisory guidance over the next 12–24 months.

- **Quantum-AI Convergence Risk to the Migration Itself:** Migration programs increasingly rely on AI-assisted tooling (code scanning, cryptographic inventory, agentic remediation). These tools inherit the dual-use and accountability risks described in Sections 6.4 and 7.3 — an AI agent misclassifying or mis-migrating a system is itself a migration risk, not just a downstream one.

10.3.2 Risk Mitigation Strategies

- **Implementation Risk** → Require independent, third-party cryptographic audits of every PQC implementation prior to production deployment, and re-audit after any library or configuration change. Prioritize NIST-validated reference implementations (CMVP-certified modules) over custom implementations wherever available.
- **Interoperability Risk** → Mandate hybrid PQ/T (post-quantum/traditional) configurations at every classical-to-PQC boundary during transition, with explicit testnet or staging validation before production cutover. Maintain a live compatibility matrix documenting which systems, counterparties, and vendors support which algorithm combinations.
- **Algorithm Risk** → Maintain cryptographic diversity by deploying at least one lattice-based and one hash-based or code-based algorithm in parallel for the highest-sensitivity use cases (e.g., ML-DSA paired with SLH-DSA), so a cryptanalytic break in one mathematical family doesn't compromise the whole system. Track NIST and ISO/IEC standardization of additional algorithm families (Section 9.3) as insurance against this risk.
- **Timeline Risk** → Establish a standing quarterly review — cross-referencing IBM, Google, and IQM hardware milestones (Section 2, Section 4) against the institution's migration roadmap — with pre-authorized triggers to accelerate migration velocity if hardware progress outpaces consensus estimates.
- **Budget and Resource Risk** → Build a multi-year cryptographic-talent pipeline combining internal training, university partnerships, and standing relationships with external quantum-security specialist firms, rather than sourcing expertise on a project-by-project basis. Budget migration as a recurring line item, not a one-time capital project, given the crypto-agility work required after initial PQC deployment.
- **Vendor and Supply Chain Risk** → Require standards-based proof of control and documented PQC roadmaps as a contractual condition of any critical vendor relationship (Section 9.1); build vendor PQC-readiness scoring into procurement and renewal decisions; identify single points of vendor dependency in the cryptographic inventory and prioritize diversification where concentration risk is highest.
- **Legacy and Embedded System Risk** → Complete a full cryptographic inventory (per NIST SP 1800-38B methodology, Section 9.3) before finalizing migration budgets, explicitly flagging systems that cannot be software-upgraded. Build hardware refresh cycles for these systems into capital planning now, since replacement lead times are typically longer than the remaining migration window.
- **Performance and Operational Impact Risk** → Benchmark PQC algorithm performance against latency- and throughput-sensitive systems before production rollout, and evaluate parameter-set tradeoffs (e.g., ML-KEM-512 vs. 768 vs. 1024) against actual operational requirements rather than defaulting to maximum security parameters everywhere.

- **Cryptographic Agility Debt Risk** → Require that all new PQC deployments use modular signature/key-exchange abstraction and versioned algorithm identifiers (Section 5.4) as a non-negotiable design standard, governed by the crypto-agility governance process described below — not as an optional architectural nicety.
- **Regulatory and Compliance Divergence Risk** → Assign ownership of regulatory tracking (US, EU, UK, and other G7 jurisdictions) to a named governance function with a mandate to flag divergence early, and build migration plans with modular compliance components that can absorb jurisdiction-specific requirements without a full redesign.
- **Quantum-AI Convergence Risk to the Migration Itself** → Apply the same human-in-the-loop review, provenance tracking, and reviewer-agent verification recommended in Section 7.3 to any AI-assisted migration tooling — treating the migration program itself as a system requiring quantum-AI risk controls, not just the end-state financial systems it produces.

11. Case Studies and Emerging Initiatives

The quantum-resilience transition is already underway in the financial sector. The following initiatives illustrate practical steps being taken and collaborative frameworks under development.

11.1 Central Bank Initiatives

- **European Central Bank (ECB):** Published quantum-risk assessments for TARGET2 and T2S payment and securities settlement systems; working with ENISA on PQC migration roadmaps for critical financial market infrastructure.
- **Bank of England:** Its 2023 Discussion Paper on AI in Financial Services flagged quantum computing as an emerging risk requiring supervisory attention; began internal PQC readiness assessments.
- **People's Bank of China (PBoC):** Piloting QKD for securing certain CBDC communications channels — a divergent national strategy that institutions with China operations must monitor.
- [PLACEHOLDER: Federal Reserve / Dallas Fed perspective — pending interview with former Governor.]

11.2 Industry Initiatives

- **SWIFT:** Published a quantum-computing threat assessment in 2022 and announced plans to test hybrid PQC implementations in its messaging infrastructure in December 2025. SWIFT's Customer Security Programme (CSP) is expected to add quantum-resilience requirements in future attestation cycles.
- **FS-ISAC:** Established a Quantum Working Group in 2023 developing threat intelligence sharing frameworks and coordinated response protocols for quantum-related financial cybersecurity incidents.
- **BIS Innovation Hub:** Project Leap, announced in announced 2024, is a proof-of-concept for quantum-resilient cross-border payment infrastructure, testing PQC integration in the mBridge multi-CBDC platform.
- [PLACEHOLDER: IBM case study — coordinate with John Medellin for IBM-approved details on financial sector quantum-resilience pilots.]

11.3 Blockchain and Digital Asset Initiatives

- **Ethereum Foundation:** Long-term roadmap includes quantum-resistance, with the 'Splurge' phase proposing EVM support for quantum-resistant signature schemes.
- **Hyperledger Foundation:** Published quantum-resilience guidance for enterprise blockchain implementations; Hyperledger Besu includes experimental support for PQC signature schemes.
- **IDAI Digital Governance & Security Center:** IDAI's Digital Trust & Cyber Resilience program is developing quantum-resilience frameworks for digital asset ecosystems — including tokenized real-world assets and DAO governance infrastructure.

- **GBA DAO Governance Working Group:** Developing governance frameworks that incorporate quantum-resilience requirements — addressing the specific challenge of maintaining decentralized governance integrity in a post-quantum environment.

12. Challenges and Barriers

For purposes of this report, challenges and barriers are distinguished from the risks enumerated in Section 10.3. Risks are potential adverse events or conditions — assessed by likelihood and impact — that could materialize during or after migration and cause harm if left unmitigated; a risk is contingent, and may or may not occur. Challenges and barriers, by contrast, are present-day structural, organizational, and market conditions that impede or slow the migration effort itself, independent of whether any specific adverse event occurs. A barrier does not need to "happen" to matter — it already exists and must be overcome for migration to proceed at all. This distinction also shapes how each is managed: risks are addressed through likelihood/impact scoring, ownership, and mitigation strategies (Section 10.3), while barriers are addressed through capacity-building, investment, advocacy, and cross-industry coordination — the categories described below.

Financial institutions' progress toward quantum resilience is constrained by a set of interlocking challenges that extend well beyond the availability of NIST-standardized algorithms. These barriers fall into four categories: organizational and human capital barriers rooted in awareness, culture, and skills; technical and infrastructure barriers rooted in the systems themselves; economic and investment barriers rooted in cost and financial justification; and external ecosystem and governance barriers that sit outside any single institution's control and require industry-wide or cross-border coordination to resolve. Distinguishing between barriers an institution can address unilaterally and those requiring external engagement is essential to sequencing a realistic migration strategy: internal barriers can be tackled through direct investment and governance, while external barriers demand advocacy, coordination, and participation in industry and regulatory forums. The table below maps each identified challenge to its category and locus of control.

Category	Barrier	Description	Locus of Control
Organizational and Human Capital	**Awareness and Urgency Gap**	Most financial institution boards and C-suites have not received formal briefings on quantum risk. The 5–15 year timeline creates a planning horizon that feels distant against quarterly earnings pressure.	Internal
Organizational and Human Capital	**Cryptographic Expertise Shortage**	The global supply of professionals with practical PQC implementation expertise is extremely limited — creating significant talent acquisition challenges for institutions beginning migration work.	Internal / External
Technical and Infrastructure	**Legacy System Complexity**	The financial sector's dependence on legacy infrastructure — some core banking systems date to the 1970s and 1980s — creates migration complexity that cannot be resolved through software updates alone.	Internal
Economic and Investment	**Cost and ROI Uncertainty**	Comprehensive PQC migration for a large financial institution has been estimated at USD$100 million to USD$500 million or more. The return on this investment is inherently difficult to quantify using traditional risk-adjusted return frameworks.	Internal
External Ecosystem and Governance	**Regulatory Uncertainty**	While NIST has provided clear technical standards, as of mid-2026, financial regulatory bodies have not yet issued specific quantum-resilience compliance timelines or examination criteria — reducing the urgency signal that drives compliance investment.	External
External Ecosystem and Governance	**Third-Party and Supply Chain Dependencies**	Financial institutions cannot achieve quantum resilience independently — they depend on the quantum readiness of payment networks, cloud providers, HSM manufacturers, and software vendors. Coordinating migration across this ecosystem requires industry-wide mechanisms that do not yet fully exist.	External / Shared
External Ecosystem and Governance	**International Coordination Gaps**	Quantum-resilience standards are advancing at different speeds across jurisdictions, creating compliance complexity and data sovereignty risks for institutions operating internationally.	External

13. Recommendations

Based on the analysis in this report, IDAI and the GBA Future of Money, Governance, & the Law Working Group offer the following recommendations organized by actor type and time horizon.

13.1 Government Decision Maker Priority Actions

Government decision makers are simultaneously exposed as operators of critical financial infrastructure AND empowered as regulators, standards setters, and procurement authorities. The following actions represent the highest-leverage interventions available to governments.

01

Issue a National Quantum-Resilience Directive for Financial Infrastructure

Establish clear compliance timelines — analogous to OMB M-23-02 for federal agencies — requiring all regulated financial institutions to complete cryptographic inventories and submit migration plans on a defined schedule. Target: within 12 months.

02

Mandate PQC Standards in All Public Financial System Procurements

Any new government payment system, CBDC infrastructure, central bank technology, or financial regulatory technology must meet NIST FIPS 203/204/205 standards as a condition of contract award. Do not build tomorrow's financial infrastructure on yesterday's cryptographic assumptions.

03

Establish a National Quantum-Security Center of Excellence for Financial Services

Centralize government expertise in PQC migration, provide technical assistance to smaller regulated institutions, and serve as the national coordination point for financial sector quantum intelligence and threat assessment.

04

Include Quantum Resilience in Financial Stability Monitoring

Central banks and treasury departments should incorporate quantum risk into financial stability reports, stress testing frameworks, and systemic risk monitoring — treating it as a macroprudential concern, not merely a cybersecurity matter.

05

Engage Internationally with Urgency

Convene quantum-resilience sessions at G7/G20 Finance Ministers' meetings. Direct the FSB and BIS to develop internationally binding quantum-resilience timelines for systemically important financial institutions (SIFIs). Establish bilateral intelligence-sharing agreements on quantum computing capability milestones.

13.2 Financial Institution Recommendations

- Treat quantum resilience as capital investment, not a cost center. Framing quantum migration as a cost center puts it in competition with every other IT expense. A 5-year PQC migration is not a one-year IT expense. The investment frame matches the actual financial reality.
- Complete a cryptographic inventory as soon as possible. Large complex Tier 1 banks and major insurers could take 24-36 months according to WEF and EY reports. Without a comprehensive map of vulnerable algorithm deployments, migration planning cannot be prioritized effectively.
- Identify and protect harvest-vulnerable data immediately. Any data with a sensitivity horizon of more than 5 years transmitted over quantum-vulnerable channels should be migrated to hybrid PQC channels as a near-term priority.
- Adopt a "quantum-hybrid first" policy for all new system procurement and major upgrades. Require PQC algorithm support as a minimum procurement criterion for all cryptographic infrastructure.
- Engage in industry coordination. Join FS-ISAC's Quantum Working Group, participate in SWIFT's quantum-resilience pilots, and contribute to financial sector-specific PQC implementation guidance.

13.3 Technology Providers and Standards Body Recommendations

- Accelerate PQC integration into financial technology products. HSM manufacturers, cloud providers, payment middleware vendors, and banking software platforms should publish PQC integration roadmaps with specific delivery timelines.
- Develop financial-sector-specific PQC implementation guidance. NIST, IETF, and ISO should produce sector-specific implementation guidance addressing the performance, interoperability, and legacy system constraints unique to financial infrastructure.
- Invest in PQC education and workforce development. The shortage of PQC implementation expertise is a systemic barrier. University curricula, professional certifications, and vendor training programs should be scaled to build the practitioner workforce needed for sector-wide migration.

13.4 Quantum Cyber-Ethics and Quantum Resilience as a Global Public Good

The transition to quantum-resilient financial infrastructure raises ethical dimensions that IDAI believes deserve explicit attention. Quantum cyber-ethics — the application of ethical principles to the development, deployment, and governance of quantum technologies — is an emerging discipline that financial services must engage with proactively.

- **Equity of Quantum Resilience:** The quantum threat does not discriminate by institution size, but the ability to mitigate it does. Smaller financial institutions and financial systems in developing nations may be unable to afford PQC migration, creating a quantum-security divide that perpetuates financial exclusion and systemic fragility.
- **Transparency of Quantum Capabilities:** Nation-state adversaries are unlikely to announce when they achieve cryptographically relevant quantum computing. The financial sector should advocate for international transparency agreements — requiring responsible disclosure of quantum computing milestones with systemic financial security implications.

- **Quantum Resilience as Financial Infrastructure:** Just as internet security and cybersecurity standards are treated as public goods warranting public investment and international cooperation, quantum resilience should be framed as a global financial stability issue requiring multilateral governance frameworks.
- **Ethical AI in Quantum-Era Financial Systems:** As quantum-enhanced AI capabilities expand, financial institutions must apply ethical AI principles — fairness, transparency, accountability, and non-discrimination — to quantum-accelerated AI decision systems. Quantum speed does not justify reduced ethical oversight.

14. Conclusion

The quantum computing transition represents the most significant cryptographic inflection point since the establishment of public-key cryptography in the 1970s. For the financial services sector — which depends on cryptographic integrity for every transaction, every identity, and every record — quantum resilience is not a future concern but a present strategic imperative.

The path forward is clear, even if the timeline is not. NIST has delivered the cryptographic standards. The migration methodology is understood. The risk of inaction — particularly through Harvest Now, Decrypt Later attacks occurring today — is quantifiable. What remains is the institutional will, investment, and coordination to execute at scale and pace.

IDAI and the GBA's FoMGL Working Group are independent nonprofits that provide financial institutions with quantum-resilient blockchain transition services and research. Their work spans standards development, policy advocacy, practitioner education, and cross-sector collaboration. Blockchain and distributed ledger technology — when designed for crypto-agility — can be a powerful enabler of quantum-resilient financial infrastructure rather than merely a victim of quantum vulnerability.

The window for orderly, planned migration is open today. The cost of waiting — measured in compromised transactions, forged identities, stolen financial data, and systemic fragility — will rise with every year of inaction.

Define the Standards. Build What's Next.

The FoMGL Working Group recommended actions:

- Financial institutions - begin cryptographic inventory today
- Regulators - Publish quantum-resilience guidance within 18 months
- Technology Providers - Accelerate PQC product integration
- International Community - Treat quantum resilience as a global financial stability priority requiring coordinated governance.

The era of quantum finance has begun. The question is whether we will be prepared for it.

Annex A: Risk Management Matrix

The following matrix provides a structured overview of key quantum risks for financial institutions. Adapt this to your specific risk profile after completing a cryptographic inventory and risk assessment.

Risk Category	Description	Likelihood	Impact	Priority	Mitigation
Harvest Now, Decrypt Later (HNDL)	Adversaries collecting encrypted financial data today for future quantum decryption	High	Critical	Immediate	Deploy hybrid PQC encryption for sensitive data in transit; classify harvest-vulnerable data
Loss of Digital Signature Integrity	Quantum-forged signatures on transactions or documents post-Q-Day	Medium	Critical	High	Migrate to NIST PQC signature standards (ML-DSA, SLH-DSA); implement crypto-agility
Blockchain Wallet Compromise	Quantum derivation of private keys from exposed on-chain public keys	Medium	High	High	Migrate institutional wallets to quantum-resistant addresses; implement PQC wallet standards
Payment Network Authentication Failure	Compromise of PKI-based authentication in SWIFT, card networks, real-time payment systems	Medium	Critical	High	Engage payment network operators on PQC migration timelines; implement hybrid auth
Legacy System Migration Failure	Core banking systems unable to support PQC algorithms within required timelines	High	High	High	Accelerate legacy system upgrade programs; implement PQC proxies for legacy interfaces
Vendor/Supply Chain Quantum Gap	Critical technology vendors not achieving PQC readiness in time	Medium	High	Medium	Include PQC readiness in vendor contracts; diversify vendor dependencies
Regulatory Non-Compliance	Failure to meet emerging quantum-resilience regulatory requirements	Medium	High	Medium	Engage regulators proactively; maintain migration documentation

Risk Category	Description	Likelihood	Impact	Priority	Mitigation
PQC Algorithm Vulnerability	Discovery of cryptanalytic weakness in a NIST-standard PQC algorithm	Low	Critical	Medium	Implement algorithm diversity; maintain crypto-agility; monitor NIST and academic research

Annex B: Glossary of Key Terms

AES	Advanced Encryption Standard — symmetric encryption for data at rest. Quantum-resilient at 256-bit key length.
CBDC	Central Bank Digital Currency — a digital form of central bank money issued by a central bank, typically on DLT infrastructure.
CRQC	Cryptographically Relevant Quantum Computer — a quantum computer able to run Shor's algorithm against real-world encryption. Does not yet exist.
DLT	Distributed Ledger Technology — decentralized record-keeping systems, of which blockchain is the most widely known.
ECC	Elliptic Curve Cryptography — public-key cryptography based on elliptic curves. Quantum-vulnerable via Shor's algorithm.
ECDSA	Elliptic Curve Digital Signature Algorithm — the ECC-based signature scheme used in Bitcoin, most blockchain networks, and many financial authentication systems.
FIPS	Federal Information Processing Standard — a standard published by NIST for U.S. federal and regulated financial system use.
Grover's Algorithm	A quantum algorithm providing quadratic speedup for unstructured search. Effectively halves the security strength of symmetric encryption keys.
HNDL	Harvest Now, Decrypt Later — collecting encrypted data now to decrypt with future quantum capability.
HSM	Hardware Security Module — a physical computing device that safeguards and manages cryptographic keys.
ML-KEM	Module-Lattice Key Encapsulation Mechanism (FIPS 203) — the NIST-standard post-quantum key exchange algorithm.
ML-DSA	Module-Lattice Digital Signature Algorithm (FIPS 204) — the NIST-standard post-quantum digital signature algorithm.
NISQ	Noisy Intermediate-Scale Quantum — current-generation quantum computers with significant error rates, insufficient for cryptographic attacks.
PQC	Post-Quantum Cryptography — cryptographic algorithms secure against both classical and quantum computers. Runs on classical hardware.

PKI	Public Key Infrastructure — the framework for creating, managing, distributing, and revoking digital certificates.
QKD	Quantum Key Distribution — a quantum communication method for securely exchanging cryptographic keys.
Q-Day	The moment a cryptographically relevant quantum computer first becomes operational.
RWA	Real-World Asset — a physical or traditional financial asset (real estate, bonds, commodities) represented as a digital token on a blockchain.
RSA	Rivest-Shamir-Adleman — the dominant public-key cryptographic algorithm for decades. Quantum-vulnerable via Shor's algorithm.
Shor's Algorithm	A quantum algorithm that efficiently factors large integers and solves discrete logarithm problems, breaking RSA and ECC encryption.
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (FIPS 205) — a NIST-standard post-quantum signature scheme based on SPHINCS+.
SWIFT	Society for Worldwide Interbank Financial Telecommunication — the messaging network used by 11,000+ financial institutions globally.
TLS	Transport Layer Security — the cryptographic protocol protecting data in transit across the internet and financial networks.
DAO	Decentralized Autonomous Organization — an organization governed by smart contracts and token-based voting on a blockchain.

Annex C: References

Preliminary reference list incorporating peer-reviewed literature from the working group's article review. Working group members are requested to review, supplement, and format final citations prior to publication.

Regulatory and Standards References

- National Institute of Standards and Technology. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). Module-Lattice-Based Digital Signature Standard. FIPS 204. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). Stateless Hash-Based Digital Signature Standard. FIPS 205. U.S. Department of Commerce.
- Office of Management and Budget. (2022). Migrating to Post-Quantum Cryptography. Memorandum M-23-02. Executive Office of the President.
- Bank for International Settlements. (2024). Quantum computing and financial stability. BIS Working Papers. Bank for International Settlements.
- European Union Agency for Cybersecurity (ENISA). (2021). Post-Quantum Cryptography: Current State and Quantum Mitigation. ENISA.

Foundational Research

- Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings, 35th Annual Symposium on Foundations of Computer Science, IEEE.
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on Theory of Computing.

Peer-Reviewed Literature — Quantum Cryptography and Security

- Rakhra, M., Kanday, R., Aggarwal, G., Ather, D., Kler, R., & Jairath, K. (2024). Quantum Cryptography: Enhancing Secure Communication in the Era of Quantum Computing. IEEE. [Covers QKD protocols BB84 and CV-QKD; demonstrates provable information-theoretic security; validates hybrid approaches for scalability. Relevance: §5.1, §5.3, §3.3]

Peer-Reviewed Literature — Quantum Computing and Finance

- Egger, D. J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., & Raymond, R. Quantum Computing for Finance: State-of-the-Art and Future Prospects. IEEE Transactions on Quantum Engineering, Volume 1. [IBM Research — demonstrates quantum algorithms for financial simulation, optimization, and ML on IBM Quantum backends; surveys computationally challenging financial problems for which quantum algorithms are promising. Relevance: §6.1, §6.2, §6.3, §11.2, §3.3]
- Aggarwal, A., Shrivastava, P., & Kler, R. (2025). A Comprehensive Review of the Convergence of Quantum Computing and Finance. 2025 2nd Global AI Summit — International Conference on Artificial Intelligence and Emerging Technology (AI Summit), IEEE. [Reviews quantum algorithms for financial modeling, optimization, quantum cryptography, and quantum ML; maps integration challenges and roadmap. Relevance: §6.1–6.3, §10]

- Chamma, E., McGee, A., Gillmann, A., McNallan, I., & Mahmoud, M. (2023). Feasible Applications of Quantum Computing in Varying Fields. 2023 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE. [Covers quantum applications in finance — portfolio optimization, risk management, algorithmic trading — alongside cybersecurity and cryptography risks; calls for PQC development. Relevance: §6.1–6.2]

Peer-Reviewed Literature — Quantum Digital Currency and Assets

- Broadbent, A., Kazmi, R. A., & Minwalla, C. (2024). A Quantum Vault Scheme for Digital Currency. 2024 IEEE International Conference on Quantum Computing and Engineering (QCE). [Proposes quantum vault architecture for digital currency — delegating quantum storage and processing to an intermediary, eliminating the need for consumer quantum hardware. Directly applicable to CBDC quantum security design. Relevance: §7.2, CBDC discussions throughout]
- Mishra, S., Ojha, A., Aggarwal, A., & Mehra, P. S. (2023). Quantum Money: Opportunities, Challenges and Open Issues. 2023 8th International Conference on Communication and Electronics Systems (ICCES), IEEE. [Reviews quantum money schemes and the no-cloning theorem as a physical impossibility (not just computational difficulty) for counterfeiting; covers security issues and future opportunities. Relevance: §7.2, digital asset design]

Peer-Reviewed Literature — Quantum and Blockchain

- Ren, X., Xu, M., Niyato, D., Kang, J., Xiong, Z., & Qiu, C. (2024). Building Resilient Web 3.0 Infrastructure With Quantum Information Technologies and Blockchain: An Ambilateral View. Proceedings of the IEEE, Volume 112, Issue 11, November 2024. [Provides comprehensive overview of quantum-blockchain convergence from both defensive (post-quantum migration) and offensive (quantum-enhanced performance) perspectives; covers DAOs, DeFi, digital identity, and asset management in Web 3.0 contexts. Relevance: §8.1–8.3, §7.2]

Industry and Working Group References

- Financial Services Information Sharing and Analysis Center (FS-ISAC). (2024). Quantum Computing and the Financial Sector: Threat Intelligence Summary. FS-ISAC.
- IBM Institute for Business Value. (2023). Cryptography in a post-quantum world. IBM Corporation.
- [PLACEHOLDER: John Medellin's Athens (2022) paper on crypto-agility — citation to be provided by author]
- [PLACEHOLDER: Additional references to be provided by working group members — particularly any 2025–2026 developments in quantum hardware timelines]

Crypto-Agility Literature

- Hohm, J., Heinemann, A., & Wiesmaier, A. (2022). Towards a Maturity Model for Crypto-Agility Assessment.
- Alnahawi, N., & Schmitt, N. (2023). On the State of Crypto-Agility.
- Santos, M. B., Ferrin, D., Kahat, R., & Lodder, M. (2026). Post-Quantum Blockchains with Agility in Mind.

Executive and Regulatory Actions (2025–2026)

- Office of Management and Budget. (2026). Execution of the Migration to Post-Quantum Cryptography. Memorandum M-26-15.
- Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (June 22, 2026).
- Executive Order 14413, Ushering in the Next Frontier of Quantum Innovation (June 22, 2026).
- G7 Cyber Expert Group. (2026). G7 CEG Quantum Roadmap.
- NIST IR 8547, Transition to Post-Quantum Cryptography Standards (finalized 2025).
- NIST SP 1800-38, Migration to Post-Quantum Cryptography (NCCoE practice guide, Vols. A–C).
- NIST SP 800-131A Rev. 3, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

International and Cross-Border Regulatory

- Digital Operational Resilience Act, Regulation (EU) 2022/2554.
- Commission Delegated Regulation (EU) 2024/1774 (RTS on ICT risk management/cryptographic controls).
- European Commission NIS2 amendment proposal (January 2026).
- UK Financial Conduct Authority research note on quantum computing in financial services.
- Monetary Authority of Singapore, QKD Sandbox Technical Report (September 2025).
- NSA, CNSA 2.0 (Commercial National Security Algorithm Suite).

Standards Bodies

- ISO/IEC 18033-2 (Classic McEliece — finalized July 15, 2026).
- ISO/IEC 14888-4 (stateful hash-based signature mechanisms, committee draft).
- ITU-T Y.3800-series standardization roadmap and 2025 supplement.
- ETSI Quantum-Safe Cryptography Working Group (including the Covercrypt KEM-AC standard).
- IETF, draft-ietf-tls-mlkem and draft-ietf-tls-ecdhe-mlkem.

Quantum Hardware and Error Correction Milestones

- Google Willow chip announcement (December 2024).
- IQM quantum error correction fault-tolerance milestone (June 2026).
- IBM Nighthawk and Loon processor announcements (IBM Newsroom, November 2025).
- Quantinuum Helios, QuEra, and Atom Computing logical-qubit demonstrations (2026).

Financial Sector Quantum Demonstrations

- HSBC and IBM, quantum-enabled algorithmic bond trading trial (September 2025).
- HSBC and Quantinuum, quantum-secured tokenized gold on the Orion platform.
- Coinbase Quantum Advisory Council, position paper on post-quantum migration and abandoned coins (June 2026).
- IBM Institute for Business Value, Quantum computing use cases for financial services.

- The Quantum Insider, "Top Global Banks Exploring Quantum Technologies in 2026" (March 2026).

Quantum Sensing and Communications

- Quantum Sensors Market Report 2025 (ResearchAndMarkets).
- World Economic Forum, "Banking in the quantum technologies era" (July 2025).
- EuroQCI (European Quantum Communication Infrastructure) initiative documentation.
- "Quantum-safe IPsec in the banking industry" (arXiv, 2026).

AI–Quantum Convergence

- HQNN-FSP: A Hybrid Classical-Quantum Neural Network for Financial Stock Market Prediction (arXiv).
- Quantum vs. Classical Machine Learning: A Benchmark Study for Financial Prediction (arXiv, 2026).
- Q-SYNTH: Hybrid Quantum-Classical Adversarial Augmentation for Fraud Detection (arXiv, 2026).
- Hybrid Classical-Quantum Generative Algorithms for Financial Modelling and Prediction (IEEE).

Quantum-AI Ethics

- "Envisioning responsible quantum software engineering and quantum artificial intelligence" (Springer, 2025).
- "Allocating Access to Quantum Computing: A Legal-Ethical Framework" (arXiv).
- UNESCO reporting on the global "quantum divide."
- "Why business adoption of quantum and AI technology must be ethical" (arXiv).

Agentic AI, Multi-Agent, Web3, and 6G Convergence Risk

- "AI Agents in Financial Markets: Architecture, Applications, and Systemic Implications" (arXiv).
- "AI POWER, GLOBAL RISK: Quantitative Systemic Risk Modeling for AI-Dominated Civilizational Infrastructure" (2026 Edition).
- KPMG, 2026 Cybersecurity Report (non-human identity findings).

HNDL Threat Intelligence

- Cyber Threat Alliance, "Approaching Quantum Dawn" (February 2026).
- GCHQ/NCSC assessment of active nation-state HNDL operations.
- FedTech Magazine, "Harvest Now, Decrypt Later: A Quantum Threat for Federal Agencies" (July 2026).

FS-ISAC (more specific document than what's currently cited)

- FS-ISAC, "Preparing for a Post-Quantum World by Managing Cryptographic Risk" (March 2023) — distinct from the 2024 threat intelligence summary already in Annex C.