Government Blockchain Association
Quantum Working Group

Report

THE IMPACT OF QUANTUM COMPUTING ON FINANCIAL SERVICES

September 29, 2026

Status: Draft
Version: Version 0.2

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 quantum 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, specifically RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), that would be rendered insecure by a sufficiently powerful quantum computer. While estimates for cryptographically-relevant quantum computers range from five to fifteen years, the "Harvest Now, Decrypt Later" (HNDL) attack strategy means the threat window has already opened: adversaries may be collecting encrypted financial data today to decrypt once quantum capabilities mature.

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

The path forward requires 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.

Key Findings for Government Decision Makers

1) The cryptographic foundations of digital banking, payment networks, and blockchain systems are vulnerable to quantum attack within a 5–15 year horizon. 2) "Harvest Now, Decrypt Later" attacks represent an immediate — not future — threat to financial data confidentiality. 3) NIST's PQC standards (FIPS 203, 204, 205) provide a viable migration pathway, but require significant institutional investment. 4) Quantum technologies also offer financial institutions material competitive advantages in optimization, simulation, and AI. 5) 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

1) Mandate cryptographic inventories for all government financial systems within 12 months. 2) Issue quantum-resilience compliance timelines for regulated financial institutions. 3) Require NIST PQC

standards in all new CBDC, government payment, and financial infrastructure procurements. 4) Fund quantum-security workforce development programs. 5) Engage internationally through FSB, BIS, and G7/G20 to harmonize global financial quantum-resilience standards.

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 problems that quantum computers 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.

Why Financial Services Is Uniquely Exposed

Unlike many sectors that can adopt new encryption standards in a relatively contained manner, financial services faces 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; and (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 is a family of related disciplines that exploit the behaviors of matter and energy at subatomic scales. 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.

3.1.1 Quantum Computing

Quantum computing uses superposition and entanglement to execute certain algorithms exponentially faster than classical computers. 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 security of 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 detection of tampering 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 ESG reporting, and complex derivatives pricing structures. For financial regulators, quantum simulation may enable stress testing at a scale and fidelity that current infrastructure 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 CBDC infrastructure.

3.2 Terms and Definitions

3.2.1 Quantum Threats — Key Terminology

Quantum Threat	Any capability enabled by quantum computing that undermines the security, integrity, or confidentiality of existing digital systems.
CRQC	Cryptographically Relevant Quantum Computer — a quantum computer able to execute Shor's algorithm against real-world encryption. Does not yet exist but is a credible near-term milestone.
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.
Grover's Algorithm	A quantum search algorithm providing quadratic speedup, effectively halving the security strength of symmetric encryption (e.g., AES-128 becomes AES-64 equivalent against a quantum adversary).
HNDL	Harvest Now, Decrypt Later — adversaries collect and store currently-encrypted data with the intent to decrypt it once a quantum computer becomes available. Also called "store now, decrypt later."
Q-Day	The moment at which a cryptographically relevant quantum computer first becomes operational marking the point at which current public-key cryptography is broken.

3.2.2 Quantum Risks — Key Terminology

Cryptographic Risk	The risk that quantum attacks compromise the confidentiality, integrity, or authenticity of encrypted financial data and communications.
Migration Risk	Operational and financial risk associated with transitioning legacy systems to quantum-resistant standards including compatibility failures, service disruption, and implementation errors.
Systemic Risk	The risk that quantum attacks on critical financial infrastructure such as payment rails, central bank systems, or clearing houses that trigger cascading failures across the financial system.
Regulatory Risk	The risk that financial institutions face penalties for failing to meet emerging quantum-security compliance requirements.
Vendor Risk	The risk that third-party technology providers will not achieve quantum readiness within required timeframes.

3.3 Recent Developments

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

- Google's Willow chip (2024) demonstrated quantum error correction below the threshold required for fault-tolerant operation — a critical milestone that accelerated timeline estimates across the research community.
- IBM's quantum roadmap projects utility-scale quantum computing by 2029, with consistent annual improvements in qubit count and error correction. IBM researchers have demonstrated quantum algorithms for financial simulation, optimization, and machine learning on IBM Quantum backends (Egger et al., IEEE Transactions on Quantum Engineering).
- NIST finalized its first three Post-Quantum Cryptography standards in August 2024: FIPS 203 (ML-KEM for key encapsulation), FIPS 204 (ML-DSA for digital signatures), and FIPS 205 (SLH-DSA, hash-based signatures).
- The U.S. OMB Memorandum M-23-02 requires federal agencies to inventory quantum-vulnerable systems and submit migration plans — establishing a compliance precedent that financial regulators are expected to follow.
- The Bank for International Settlements (BIS) published a 2024 working paper identifying quantum risk as a systemic financial stability concern, calling for coordinated international action.
- Peer-reviewed research confirms that hybrid classical+quantum cryptographic approaches are the most viable near-term transition strategy for financial institutions, with QKD protocols (BB84 and Continuous Variable QKD) providing provable information-theoretic security as a long-term complement to PQC for the highest-sensitivity channels (Rakhra et al., IEEE 2024).
- The convergence of quantum computing and blockchain is increasingly understood as bidirectional: quantum computing both threatens blockchain cryptographic security AND offers capabilities to enhance blockchain performance. This demans simultaneous defensive migration and offensive capability development (Ren et al., Proceedings of the IEEE, November 2024).

[DRAFT NOTE: John Medellin (IBM) — please review and supplement with 2025–2026 IBM quantum timeline updates. Egger et al. (IBM Research) may provide citable context for IBM's financial sector quantum demonstrations.]

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.

4. Quantum Risks to Financial Systems

The quantum threat to financial services operates on multiple timeframes, affects different systems in different ways, and varies in severity across domains. 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

"Immediate" in this 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 adversarial data collection is likely already underway.

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 Impact of Shor's Algorithm on RSA and ECC

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 break could be factored by a sufficiently powerful quantum computer in hours. ECC is increasingly preferred because it achieves equivalent security with shorter keys. It is equally vulnerable, as Shor's algorithm also solves the elliptic curve discrete logarithm problem that ECC relies upon.

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. A post-quantum adversary who had previously collected TLS-encrypted session traffic could retroactively decrypt account credentials, transaction histories, and personally identifiable information (PII). 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. Central Bank Digital Currencies (CBDCs) currently in development across 130+ countries are largely architected with ECC digital signatures, systems designed for multi-decade lifetimes that will outlive the cryptographic assumptions on which they are built if migration does not begin 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 — 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. Any government blockchain procurement decision made today should require quantum-resilience by design.

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. Nation-state adversaries with the capability and motivation to compromise long-term financial intelligence have strong incentives to collect encrypted data now.

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.

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.

[DRAFT NOTE: John Medellin (IBM) — please review this section. Jeff Crume's IBM research on HNDL may provide updated threat intelligence for inclusion.]

4.2 Long-Term Risks

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.

- 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.

4.3 Quantum Risk by Financial Services Domain

Quantum risk does not affect all financial services domains equally. The following assessment supports prioritization decisions for 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**
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, FX confirmation signing, exchange API security	HIGH	HIGH
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**
Capital Markets	Trade order authentication, settlement system integrity, FX confirmation signing	HIGH	HIGH
Investment & Asset Management	Portfolio data confidentiality, client communication encryption, advisor authentication	MEDIUM	HIGH
Insurance	Actuarial data confidentiality, claims signature authentication, reinsurance treaty signing	MEDIUM	MEDIUM
Lending & Credit	Loan origination documentation, credit bureau data transmission, syndicated loan communications	MEDIUM	HIGH
Regulatory, Risk & Compliance	Regulatory submission signing, audit trail integrity, AML/KYC record confidentiality	HIGH	HIGH

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

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against 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. 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 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 have larger key and signature sizes than classical counterparts, creating bandwidth and storage implications for high-frequency transaction systems.

- 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 PQC standards 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 classical+quantum 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 the BB84 and Continuous Variable QKD protocols — provides information-theoretic security that is provably unbreakable not just against quantum computers but against any future computational advancement. 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 — implementing 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 handling 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.

IDAI and the GBA are 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.

[DRAFT NOTE: John Medellin — your 2022 Athens paper on crypto-agility is directly relevant here. Please provide a citation and flag any portions superseded by recent developments.]

6. Quantum Opportunities in Financial Services

The quantum computing transition presents not only risk, but significant strategic opportunity for financial institutions and governments that invest early in quantum capability. Quantum technologies offer material advantages in optimization, simulation, and AI augmentation.

6.1 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).

6.2 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.

6.3 Synergies with Artificial Intelligence

Quantum Machine Learning (QML) explores whether quantum algorithms can accelerate AI model training and inference — with potential applications across fraud detection, credit scoring, and algorithmic trading. However, this convergence carries an important dual-use caution: AI also represents a new attack surface for quantum-era systems.

Quantum + AI: Guard and Attack

Quantum-enhanced AI can both defend and threaten financial systems. Quantum machine learning may dramatically improve anomaly detection and fraud prevention at transaction scale. At the same time, quantum-accelerated adversarial AI could generate synthetic transaction patterns defeating classical fraud models, or optimize social engineering attacks at speeds outpacing human response. Financial regulators must model both dimensions and treat AI system security as a component of quantum risk frameworks — not a separate concern.

[DRAFT NOTE: Ingrid Vasiliu-Feltes — please review the AI/quantum ethics dimensions in this section.]

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.

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). DAOs, 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.

Add Novel Risks Related to Convergence section here?

8. Implications for Blockchain Ecosystems

Blockchain and distributed ledger technology occupy a unique position in the quantum risk landscape. Blockchain systems are disproportionately exposed to quantum cryptographic attacks — 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 specific vulnerability is structurally more severe than traditional PKI: once a transaction is broadcast on-chain, the sender's public key is exposed. A quantum adversary with a CRQC could derive the private key from the public key and sign fraudulent transactions before the original transaction confirms — a race condition that becomes increasingly dangerous as quantum hardware improves.

Peer-reviewed research published in Proceedings of the IEEE (November 2024) frames this challenge through an "ambilateral" lens: quantum computing simultaneously (1) disrupts the original 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 bidirectional 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 — this 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 hardware improves, 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 Transition Strategies

- 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. 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: Conduct quantum-security audits of smart contracts implementing cryptographic operations natively, replacing vulnerable 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 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: decentralized autonomous organization governance mechanisms — often relying on on-chain ECC-signed ballots — must be made quantum-resistant without compromising decentralization principles.

9. Governance: Regulations, Standards, and Policy 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 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.

[DRAFT NOTE: Working group members should supplement with the latest ISO/IEC work program updates as of Q2 2026.]

9.2 NIST 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.

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 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.

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

10. Implementation Roadmap for Financial Institutions

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

[DRAFT NOTE: Addressed John Medellin's comment: a framework/model precedes the roadmap. Institutions should complete Phase 0 (assessment) before committing to Phase 1 timelines.]

10.1 Quantum Risk Assessment Framework

1. 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.
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. 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.
4. 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.
5. 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.

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) Change to 3+?

- 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

Add subheader “Risk Categories” ? 10.3.1

- 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.
- Other risks ?….

Add a new subheader Risk Mitigation Strategies 3.10.2?

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.

[DRAFT NOTE: John Medellin is exploring an interview with a former Federal Reserve Bank of Dallas Governor for this section. [PLACEHOLDER: Insert interview summary once conducted.]]

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 and announced plans to test hybrid PQC implementations in its messaging infrastructure. SWIFT's Customer Security Programme (CSP) is expected to add quantum-resilience requirements in future attestation cycles.
- FS-ISAC: Established a Quantum Working Group developing threat intelligence sharing frameworks and coordinated response protocols for quantum-related financial cybersecurity incidents.
- BIS Innovation Hub — Project Leap: 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

Despite the clear technical path forward, the financial sector faces structural, economic, and organizational barriers that could delay effective quantum-resilience migration. Understanding these barriers is essential for developing realistic transition plans and appropriate policy responses.

- Awareness and Urgency Gap: A significant minority of financial institution boards and C-suites have received formal briefings on quantum risk. The 5–15 year timeline creates a planning horizon that feels distant against quarterly earnings pressure.
- 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.
- 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.
- Regulatory Uncertainty: While NIST has provided clear technical standards, financial regulatory bodies have not yet issued specific quantum-resilience compliance timelines or examination criteria — reducing the urgency signal that drives compliance investment.
- 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.
- Cost and ROI Uncertainty: Comprehensive PQC migration for a large financial institution has been estimated at $100 million to $500 million or more. The return on this investment is inherently difficult to quantify using traditional risk-adjusted return frameworks.
- International Coordination Gaps: Different nations are advancing quantum-resilience standards at different speeds. Institutions operating across jurisdictions must navigate potentially conflicting migration requirements.

13. Recommendations

Based on the analysis in this report, IDAI and the GBA FoMGL Working Group offer the following recommendations organized by actor type and time horizon.

[DRAFT NOTE: Ingrid Vasiliu-Feltes's suggestion to include quantum cyber-ethics harmonization and quantum-resilience framing has been incorporated in Section 13.4.]

13.1 For Government Decision Makers — Priority Actions

Add short term urgent priority recommendations versus long term resilience recommendations?

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 government.

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 For Financial Institutions

1. Treat quantum resilience as a board-level risk management issue today. Establish executive accountability, integrate quantum risk into enterprise risk management frameworks, and include quantum-resilience status in board reporting.
1. Complete a cryptographic inventory within the next 12 months. Without a comprehensive map of vulnerable algorithm deployments, migration planning cannot be prioritized effectively.
2. 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.
3. 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.
4. 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 For Technology Providers and Standards Bodies

5. 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.
6. 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.
7. 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 Government Blockchain Association's FoMGL Working Group are committed to accelerating this transition through 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 calls on financial institutions to begin cryptographic inventory today; on regulators to publish quantum-resilience guidance within 18 months; on technology providers to accelerate PQC product integration; and on the international community to 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.

All separate working group documents should go under Annex for clarity; this document should be the corollary document offering a cohesive GBA opinion.

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

Risk Category	Description	Likelihood	Impact	Priority	Mitigation
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
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]