BANK & FINANCE
CONSULTING GROUP

Quantum Technology and the Future of Financial Security: Exploring the Disruptive Frontier of Computation, Cryptography, and Control

Bank & Finance
Consulting Group

November 2025

Preface

Technological revolutions often redefine the boundaries of what is possible—and, in doing so, they reshape the foundations of economic and financial stability. Quantum technology represents such a turning point. From quantum computing and communication to sensing and simulation, its rapid evolution holds the promise of unprecedented computational power, new materials, and more secure information systems. Yet it also introduces profound vulnerabilities: a single quantum-capable breakthrough could render today's cryptographic standards obsolete, undermining the trust on which modern finance depends.

This report explores the intersection between **quantum innovation and financial security**, assessing how quantum technologies could transform, strengthen, or disrupt the global financial ecosystem. It examines both the opportunities—enhanced optimization, ultra-secure communications, improved risk modelling—and the systemic risks that could emerge from asymmetric adoption, standards fragmentation, and exposure to quantum-enabled cyber threats.

As part of the **Bank & Finance Deep-Dive Series**, this study continues our effort to understand how technological, environmental, and geopolitical transformations interact across the five layers of the financial ecosystem: **Information, Infrastructure, Innovation, Integration, and Governance**. Each layer faces distinct quantum-related challenges—from cryptographic resilience and cloud migration to cross-border coordination and regulatory readiness. Together, they illustrate the need for an integrated, forward-looking approach to financial stability.

Our objective is to provide central banks, regulators, financial institutions, and technology leaders with a structured framework to assess quantum-related risks and design resilient transition strategies. The report draws on the latest international work by the BIS, IMF, FSB, NIST, ENISA, the European Commission, and the academic community, while building on Bank & Finance's proprietary ecosystem architecture and analytical methods.

This report follows previous deep dives on **Artificial Intelligence**, **Digital Currencies**, and **Cyber Resilience**, forming part of a broader sequence dedicated to the **technological frontier of finance**. Together, these studies examine how innovation simultaneously expands economic opportunity and introduces new forms of systemic exposure. By situating quantum technologies within this continuum, *Bank & Finance* seeks to anticipate the next phase of transformation shaping global finance—and to help institutions navigate it with foresight, integrity, and resilience.

Bank & Finance
November 2025

Table of Contents

List of Figures

List of Tables

List of Boxes

List of Acronyms

AI – Artificial Intelligence

AIML – Artificial Intelligence and Machine Learning

API – Application Programming Interface

BIS – Bank for International Settlements

BISIH – BIS Innovation Hub

BRICS – Brazil, Russia, India, China and South Africa

CBDC – Central Bank Digital Currency

CDS – Credit Default Swap

CLS – Continuous Linked Settlement

CPMI – Committee on Payments and Market Infrastructures

CRYSTALS – Cryptographic Suite for Algebraic Lattices

DORA – Digital Operational Resilience Act (European Union)

ECB – European Central Bank

ENISA – European Union Agency for Cybersecurity

ESA – European Space Agency

ESG – Environmental, Social and Governance

ETSI – European Telecommunications Standards Institute

EU – European Union

FMIs – Financial Market Infrastructures

FSAP – Financial Sector Assessment Program (IMF–World Bank)

FSB – Financial Stability Board

G20 – Group of Twenty

GFIN – Global Financial Innovation Network

IBM – International Business Machines Corporation

IMF – International Monetary Fund

IOSCO – International Organization of Securities Commissions

ISO – International Organization for Standardization

ITU – International Telecommunication Union

LWE – Learning With Errors (mathematical foundation of lattice-based PQC)

MAS – Monetary Authority of Singapore

MCTI – Ministry of Science, Technology and Innovation (Brazil)

ML – Machine Learning

MoST – Ministry of Science and Technology (China)

NIS2 – Network and Information Systems Directive 2 (European Union)

NISQ – Noisy Intermediate-Scale Quantum (current quantum-computing era)

NIST – National Institute of Standards and Technology (United States)

NQI – National Quantum Initiative (United States)

OECD – Organisation for Economic Co-operation and Development

PQC – Post-Quantum Cryptography

QAOA – Quantum Approximate Optimization Algorithm

QKD – Quantum Key Distribution

QML – Quantum Machine Learning

QRA – Quantum-Readiness Assessment

QRC – Quantum Readiness Council (proposed multilateral coordination forum)

QRFF – Quantum-Resilience Funding Facility

QRI – Quantum-Readiness Index

QRNG – Quantum Random Number Generator

RSA – Rivest–Shamir–Adleman (public-key encryption system)

RTGS – Real-Time Gross Settlement

SCO – Shanghai Cooperation Organisation

SPHINCS+ – Stateless Practical Hash-Based Incredibly Nice Cryptographic Signature (PQC algorithm)

SWIFT – Society for Worldwide Interbank Financial Telecommunication

VQE – Variational Quantum Eigensolver

WEF – World Economic Forum

WGQF – Working Group on Quantum Finance (proposed BIS–IMF coordination body)

Executive Summary

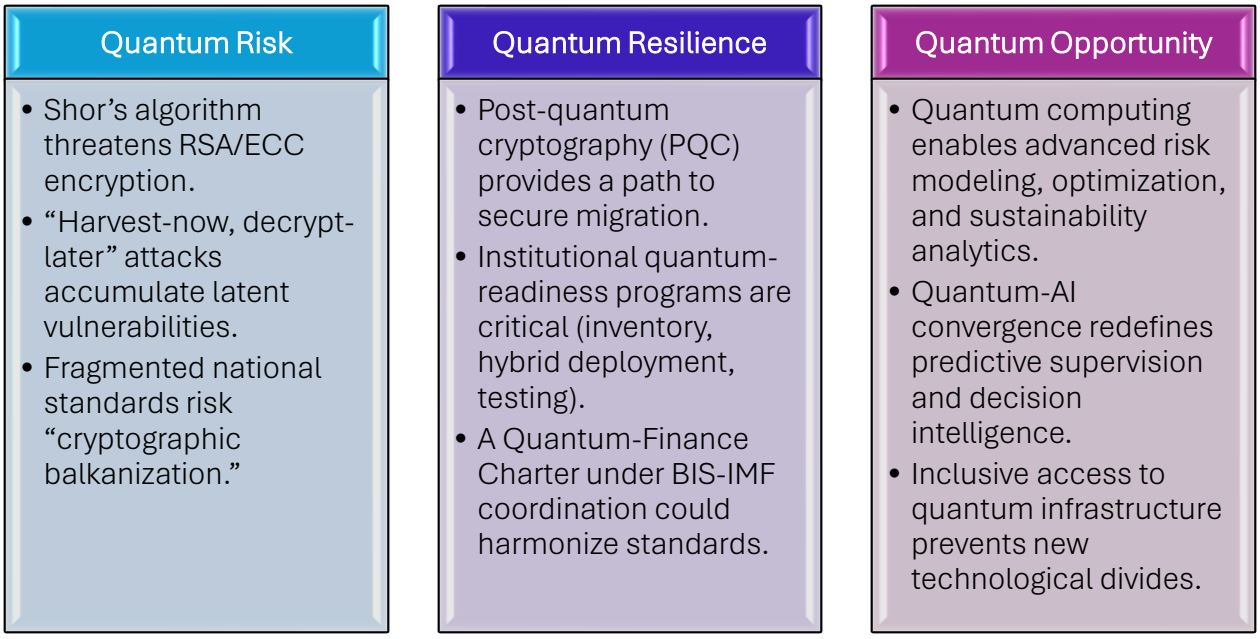
Quantum technology is transforming the foundations of global finance. Its development marks a paradigm shift comparable to the birth of digital computing or the rise of artificial intelligence—but with far deeper consequences for trust, the fundamental currency of the financial system.

Quantum computing threatens to break the cryptographic backbone that protects payments, identities, and digital assets. Yet it also offers new computational horizons that could revolutionize risk analysis, portfolio optimization, and sustainability modeling. The challenge is to manage this *quantum paradox*: defending today's system while building tomorrow's capabilities.

The report argues that quantum resilience must become the next frontier of prudential policy—complementing capital adequacy and cyber resilience—and that coordinated global action is essential to avoid a "quantum divide" between secure and insecure economies.

Figure 1 summarizes the report's key messages across three dimensions — *Risk*, *Resilience*, and *Opportunity* — distilling the main findings of the seven analytical sections.

Figure 1 – Key Highlights of the Report

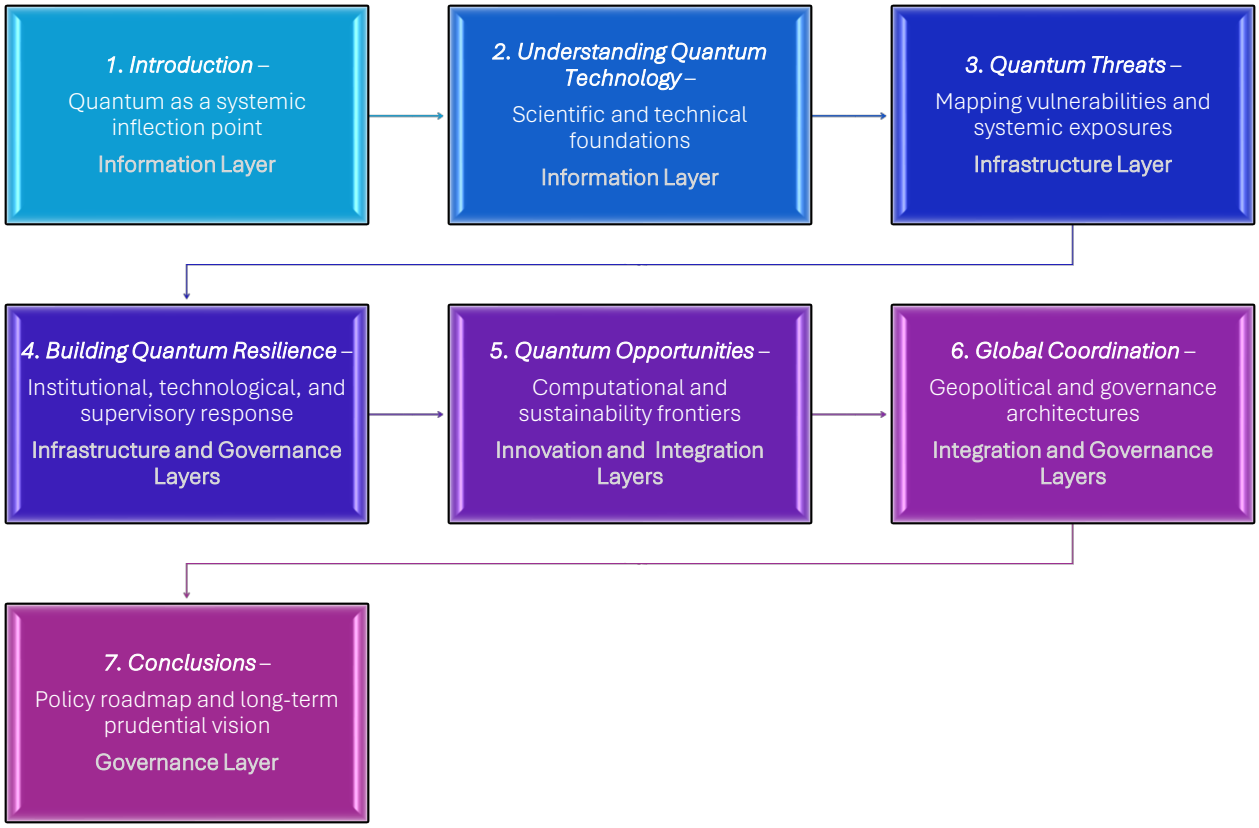


***Source**: Bank & Finance elaboration based on BIS (2024); FSB (2023); OECD (2025).*

Figure 1 captures the dual narrative of quantum transformation: existential risk and frontier opportunity. Finance stands at an inflection point—one that demands prudential imagination equal to that which created Basel III and the cyber-resilience frameworks of the 2010s.

Figure 2 outlines the structure and logic of this Deep-Dive Report, situating each section within the Five-Layer Financial Ecosystem framework.

Figure 2 – Report Roadmap



Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024).*

Figure 2 underscores the report's systemic architecture: risk and opportunity are not parallel narratives but interlocking dimensions of the same transformation. Quantum resilience must therefore be pursued as an ecosystem goal, connecting micro-institutional upgrades with macro-prudential governance.

The following synthesis highlights five dimensions of quantum transformation—Risk, Resilience, Opportunity, Coordination, and Policy—summarizing the central findings of the report.

Quantum Risk – The Collapse of Classical Cryptography. Quantum computing can break the mathematical backbone of today's financial encryption, exposing payments, identities, and digital assets to decryption once large-scale machines mature. The *harvest-now, decrypt-later* threat means sensitive data stolen today could be revealed tomorrow (ENISA, 2025). Unless migration begins early, a "cryptographic cliff edge" could emerge in the 2030s (BIS, 2024).

Quantum Resilience – Building the Next Layer of Trust. Resilience now depends on replacing vulnerable algorithms with Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) (NIST, 2024). Institutions should move through an inventory-to-integration roadmap coordinated by Quantum-Readiness Assessments (FSB, 2023). Cryptographic integrity must become a board-level and supervisory concern, not only an IT task (ECB, 2025).

Quantum Opportunity – Computing Beyond the Classical Frontier. Quantum algorithms such as QAOA and VQE could accelerate risk modeling, portfolio optimization, and sustainability analytics

by orders of magnitude (IBM Quantum, 2025). Their convergence with AI will enhance predictive supervision and climate-risk simulation, turning computation itself into a source of resilience rather than fragility (OECD, 2025; WEF, 2025).

Global Coordination – Avoiding a Quantum Divide. Readiness varies sharply across jurisdictions: the U.S. leads in standardization, the EU in regulation, China in infrastructure, and emerging markets in fintech adaptation (OECD, 2025). A BIS–IMF–G20 Quantum-Finance Charter could harmonize protocols, fund migration support, and embed ethical safeguards, preventing a new technological divide (IMF, 2024).

Policy Roadmap – From Awareness to Action. A phased timeline is proposed: 2025–27 for inventories and pilots; 2027–30 for hybrid encryption and testing; 2030–35 for full PQC migration and global reporting. Each phase builds capability and preserves interoperability, ensuring the financial system enters the quantum era with confidence rather than exposure.

Cross-Cutting Messages

Trust is the ultimate infrastructure. Quantum readiness is not a technical upgrade but a systemic imperative for maintaining confidence in money, payments, and data. Protecting cryptographic integrity is as essential as safeguarding capital or liquidity.

Coordination is competitiveness. Jurisdictions that standardize early will define the protocols, attract capital, and shape the norms of the quantum era. Fragmented adoption would turn innovation into vulnerability.

Inclusion determines legitimacy. Without funding, knowledge sharing, and capacity building, quantum security could deepen the digital divide. Shared infrastructure and cooperative standards are vital to make resilience a global public good.

Key Takeaways

1. **Quantum risk is systemic.** Encryption failure could undermine financial stability and digital trust worldwide.
2. **Quantum resilience is strategic.** Early migration to PQC, supported by sound governance, is cheaper—and safer—than crisis response.
3. **Quantum opportunity is transformative.** Harnessed responsibly, quantum computing can enhance analytical precision and sustainability.
4. **Global coordination is urgent.** Only collective action on standards, ethics, and inclusion can secure a trustworthy quantum-finance ecosystem.

Institutions that act now, investing in algorithms, governance, and collaboration, will not only preserve trust but lead the next wave of sustainable innovation.

The sections that follow expand each dimension in depth, tracing how quantum technology reshapes the information, infrastructure, innovation, integration, and governance layers of the financial ecosystem.

1. Introduction – A New Frontier for Financial Security

The rise of quantum technology represents one of the most profound transformations in the history of computation — comparable to the emergence of digital computing in the mid-20th century and the internet revolution that followed.

While its physics is esoteric, its consequences are tangible: quantum innovation could simultaneously **undermine the cryptographic foundations of modern finance** and **create unprecedented computational power** for analytics, security, and sustainability modeling.

For decades, financial systems have relied on the mathematical hardness of certain problems — prime factorization and discrete logarithms — to guarantee digital trust. The RSA and ECC encryption schemes that protect interbank messaging, digital identities, and blockchain ledgers are built on these assumptions. Yet, quantum computers capable of executing **Shor's algorithm** (Shor, 1994) can solve these problems exponentially faster than any classical computer, rendering today's cryptography obsolete.

This risk is not theoretical. The U.S. National Institute of Standards and Technology (NIST, 2024) has already launched a full post-quantum standardization process, while the Bank for International Settlements (BIS, 2024) and Financial Stability Board (FSB, 2023) have warned that "cryptographic fragility" could become a new source of systemic financial vulnerability. The issue therefore transcends cybersecurity: it strikes at the core of **financial stability and global trust**.

At the same time, quantum technology offers transformative potential. The same physical principles that threaten encryption — superposition, entanglement, and interference — could revolutionize portfolio optimization, derivative pricing, and macro-financial simulation (IBM Quantum, 2025). Quantum sensors could improve timing in payment systems, while quantum communication could make interbank networks unhackable.

This duality — existential risk and frontier opportunity — defines what this report calls the *quantum paradox of finance*. It demands both **prudential caution** and **strategic vision**: policymakers must protect financial systems from cryptographic collapse while positioning them to capture the advantages of quantum computation.

Bank & Finance situates this discussion within the **Five-Layer Financial Ecosystem Framework** developed across previous Deep-Dive reports (Bank & Finance 2025i). Quantum risk and opportunity intersect all layers:

- **Information Layer:** where truth and trust are encoded (see *Value of Truth*, Bank & Finance, 2025a).
- **Infrastructure Layer:** where systems settle and synchronize (*Future of Payments*, 2025c).

- **Innovation Layer:** where computational paradigms evolve (*Artificial Intelligence*, 2025f).
- **Integration Layer:** where standards and interoperability shape cross-border resilience (*Open Finance*, 2025e).
- **Governance Layer:** where geopolitical rivalry and global coordination converge (*Financial Geopolitics and Global Fragmentation*, 2025h).

Quantum thus acts as both an amplifier and a stress test of these interdependencies — the ultimate frontier of **digital trust and systemic coordination**.

Box 1 situates quantum resilience as a direct continuation of the cyber-resilience agenda, illustrating how lessons from digital defense can guide the post-quantum transition.

Box 1 – From Cyber Resilience to Quantum Resilience

Cyber resilience and quantum resilience share the same underlying logic: both redefine security as a *continuum of adaptation* rather than a static perimeter. Over the past decade, attacks such as the SWIFT heist (2016) and ICBC ransomware (2023) proved that digital vulnerabilities can escalate into systemic shocks. Supervisors responded by embedding resilience within prudential frameworks — transforming cybersecurity from a compliance function into a strategic capability.

Quantum computing introduces a similar inflection point, but with a fundamental difference: it attacks the *mathematical foundations* of trust rather than its operational layers. Traditional patching strategies will no longer suffice; institutions must redesign cryptographic cores.

The path toward quantum resilience involves:

1. Comprehensive cryptographic inventory and risk mapping;
2. Deployment of hybrid (classical + post-quantum) encryption;
3. Integration of quantum-safe standards into supervisory testing and systemic-resilience metrics.

Ultimately, quantum resilience will become the next prudential frontier — embedding encryption integrity within the architecture of financial stability.

Source: *Bank & Finance elaboration based on Bank & Finance (2025b); FSB (2023); BIS (2024); ENISA (2024); NIST (2024).*

The parallels between the cybersecurity transition of the 2010s and the quantum-security challenge of the 2020s are striking. When ransomware and cyberattacks became systemic, regulators realized that resilience could no longer be confined to IT departments; it had to be embedded into prudential supervision (FSB, 2023; ENISA, 2024). The same logic now applies

to quantum: the next decade will require embedding cryptographic integrity into **financial-stability oversight**.

Table 1 expands the analytical lens, mapping quantum technology across Bank & Finance's five-layer ecosystem — Information, Infrastructure, Innovation, Integration, and Governance.

Table 1 – Five Layers of Quantum Impact in the Financial Ecosystem

Ecosystem Layer	Quantum Impact Channel	Implications for Finance	Strategic Response
Information	Quantum computing breaks public-key encryption; quantum communication (QKD) enables unhackable links.	Threatens confidentiality and integrity of financial data; simultaneously opens secure-communication frontiers.	Begin PQC migration; pilot QKD for high-value infrastructures.
Infrastructure	Quantum sensors and clocks increase precision of settlement and timing systems.	Enhances synchronization and systemic reliability.	Integrate quantum timing into RTGS and satellite-based systems.
Innovation	Quantum algorithms accelerate portfolio optimization, valuation, and stress testing.	Expands analytical capabilities and model complexity.	Create regulatory sandboxes for quantum financial computing.
Integration	Uneven quantum capability risks regulatory and technological fragmentation.	Generates cross-border resilience gaps.	Coordinate global standards through BIS/IMF/FSB.
Governance	Quantum advantage amplifies geopolitical asymmetry.	Concentration of capability could reshape financial power dynamics.	Establish multilateral governance for equitable access and interoperability.

Source: *Bank & Finance elaboration based on Bank & Finance (2025i); BIS (2024); IMF (2024); OECD (2024); WEF (2025).*

The mapping in Table 1 reveals that quantum disruption is not linear but *ecosystemic*. For example, a compromise in the **Information Layer** — such as mass decryption of certificates — would cascade through the **Infrastructure Layer** (payments) and **Integration Layer** (cross-border systems), ultimately threatening the **Governance Layer** through geopolitical asymmetry. Conversely, quantum innovation in sensing or optimization could reinforce systemic reliability and accelerate sustainable finance (WEF, 2025; OECD, 2025).

The **timeline of technological vulnerability** helps explain why quantum preparedness is urgent. Public-key encryption was introduced in the 1970s (Diffie & Hellman, 1976) and has remained conceptually unchanged since. Meanwhile, Moore's Law doubled classical computing power roughly every 18 months. Quantum computation, however, follows a steeper exponential curve: from 5 qubits in 2016 (IBM) to over 1,000 qubits in 2025 prototypes, with error-corrected thresholds expected by early 2030 (Google Quantum AI, 2025).

Financial authorities thus face a **temporal asymmetry**: quantum capability may arrive faster than governance adaptation. In cyber resilience, regulatory alignment took nearly a decade (from early Basel guidance to the EU's DORA). A similar lag in quantum readiness would create what BIS (2024) calls a "cryptographic cliff edge" — a moment when financial infrastructures become simultaneously insecure and irreplaceable.

Furthermore, quantum risk is **non-local**. Unlike cyber incidents that propagate through identifiable network channels, quantum breaches could compromise information retroactively. Data stolen today could be decrypted years later — the so-called *harvest-now, decrypt-later* problem (ENISA, 2025). This latency transforms quantum from a technology risk into a **temporal policy challenge**, requiring forward-looking coordination and early migration to post-quantum cryptography.

For these reasons, Bank & Finance frames the quantum transition as a **prudential and geopolitical project**. It is not merely about algorithms but about sovereignty, cooperation, and trust. The institutions that succeed will be those that treat quantum readiness as integral to financial stability — much as capital adequacy once became a global standard after the 1980s crises.

In this sense, the transition to quantum resilience parallels the creation of the Basel framework itself: both represent efforts to harmonize responses to systemic, cross-border risk through shared principles and standards (Goodhart, 2011). The difference is that while Basel addressed the scarcity of capital, the quantum challenge addresses the scarcity of **trustworthy computation**.

The next section explains the scientific foundations of this new frontier — clarifying what quantum technology actually is, how it functions, and why it poses such asymmetric implications for finance.

2. Understanding Quantum Technology

Quantum technology is transforming the boundaries of computation, communication, and measurement. Unlike classical systems that store and process information in binary bits (0 or 1), **quantum systems use qubits** that can exist in superposition — simultaneously representing 0 and 1 until measured. Combined with *entanglement* (instantaneous correlation between particles) and *interference* (control of probability amplitudes), these features create

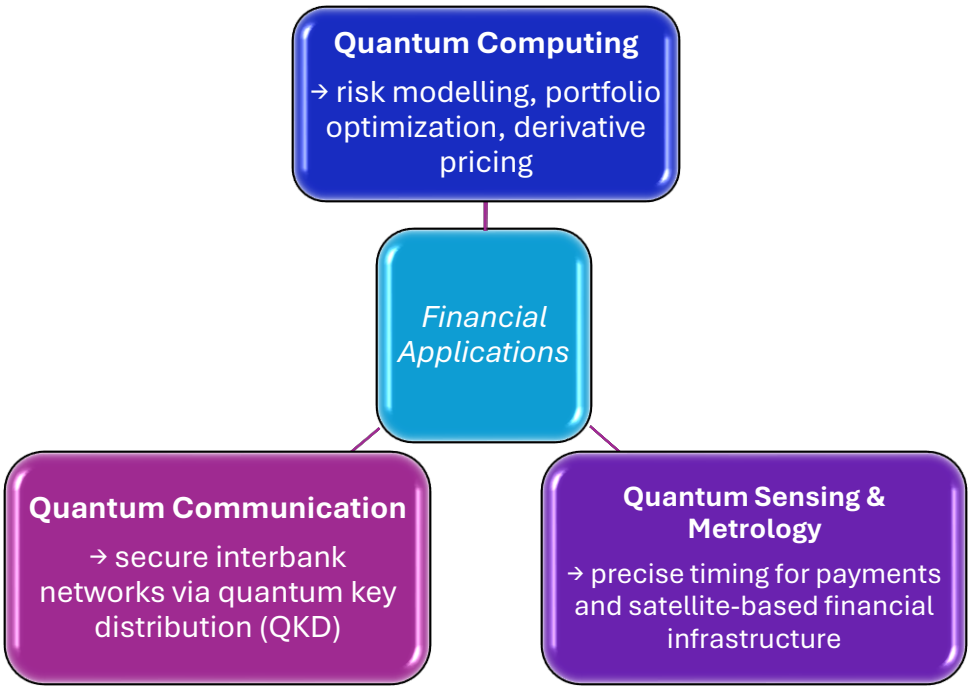
exponentially greater computational potential than classical architectures (Feynman, 1982; Arute et al., 2019).

In financial terms, quantum mechanics translates into an **entirely new information regime**: one capable of breaking the encryption that safeguards global data flows, but also of solving optimization and simulation problems previously deemed intractable. As BIS (2024) observes, this "computational discontinuity" could affect both sides of the financial-stability equation — *vulnerability and capability*.

This section explains the scientific and technical principles underlying quantum technology and their relevance to financial security. It distinguishes among three primary domains — computing, communication, and sensing — and situates their expected maturity timelines.

Figure 3 illustrates the three principal branches of quantum technology — computing, communication, and sensing — and the ways in which they intersect with financial infrastructures.

Figure 3 – The Quantum Technology Landscape



Source: *Bank & Finance elaboration based on BIS (2024); OECD (2024); WEF (2025); NIST (2024).*

Figure 3 illustrates that quantum technology is not monolithic. Each branch operates at a different level of maturity: while **quantum sensing** is already commercially deployed, **quantum communication** is in pilot stages, and **quantum computing** remains experimental but exponentially advancing. Financial systems will feel these impacts sequentially — sensing first (through timing systems), communication next (through secure data channels), and computing last (through cryptographic disruption and computational innovation).

Table 2 decomposes the three quantum domains into mechanisms, financial applications, and vulnerabilities, translating abstract physics into practical finance.

Table 2 – Core Quantum Technologies and Their Relevance to Finance

Quantum Domain	Underlying Principle	Potential Financial Applications	Key Risks / Limitations	Current Maturity (2025)
Quantum Computing	Superposition, entanglement, interference	Portfolio optimization, derivative valuation, systemic-risk simulation	Cryptographic obsolescence; decoherence; cost	Experimental (100–1 000 qubits)
Quantum Communication	Quantum key distribution (QKD)	Secure payments, digital-ID authentication, cross-border data sharing	Range limits; high deployment cost	Early deployment (EU, China, Japan)
Quantum Sensing & Metrology	Quantum-enhanced measurement and timing	Real-time settlement synchronization; anomaly detection in data centres	Integration and calibration challenges	Commercially viable in aerospace, energy sectors

Source: *Bank & Finance elaboration based on BIS (2024); OECD (2024); FSB (2023); ESA (2024).*

Table 2 confirms that financial implications differ sharply across domains. **Quantum computing** poses the greatest *threat*, whereas **quantum communication** and **sensing** offer near-term *resilience gains*. Central banks and market infrastructures should therefore adopt a **differentiated policy stance** — prioritizing defensive cryptography for computing risks while promoting pilot projects in sensing and communication for efficiency improvements (BIS, 2024; ECB, 2025).

Historical Perspective and Context

Quantum research has advanced through successive waves. The first (1980s–1990s) established the theoretical foundations with Feynman (1982) and Deutsch (1985). The second (2000s–2010s) demonstrated laboratory feasibility. The third, now underway, is marked by *commercial scaling* — the "Noisy Intermediate-Scale Quantum" (NISQ) era (Preskill, 2018). Financial institutions entered this landscape around 2018, when IBM and JP Morgan Chase executed the first quantum-algorithm pilot for option pricing (Pistoia et al., 2019).

Technological progress has been exponential: superconducting and trapped-ion platforms now achieve coherence times exceeding 200 microseconds, while hybrid algorithms allow cloud access to early quantum devices (Google Quantum AI, 2025). These milestones imply that the

window between proof-of-concept and commercial impact could be shorter than previous technological transitions — underscoring the need for anticipatory regulation.

Box 2 provides a conceptual bridge for readers unfamiliar with the physics underlying quantum technology, explaining the three foundational principles that define its behavior and potential.

Box 2 – Quantum Principles in Plain Language

1. Superposition: A classical bit is either 0 or 1. A quantum bit, or *qubit*, can exist as both simultaneously until measured. This allows parallel processing of an enormous number of possibilities. In financial terms, this translates into evaluating countless portfolio combinations or scenario simulations simultaneously.

2. Entanglement: When two qubits are entangled, the state of one instantly influences the other, even across distance. This property enables ultra-secure communications — any attempt at interception changes the state, revealing tampering — and allows for correlated computations in optimization problems.

3. Quantum Interference: Quantum systems rely on probability amplitudes, which can amplify correct outcomes and cancel incorrect ones. In financial modeling, this could dramatically accelerate convergence toward optimal solutions in risk assessment or pricing algorithms.

Together, these three features constitute the essence of quantum advantage: **performing certain computations exponentially faster or more securely than classical systems**. However, they also create new challenges in error correction, scalability, and energy efficiency — barriers that must be overcome before financial institutions can deploy quantum systems at scale.

Source: *Bank & Finance elaboration based on NIST (2024); IBM (2025); MIT (2024).*

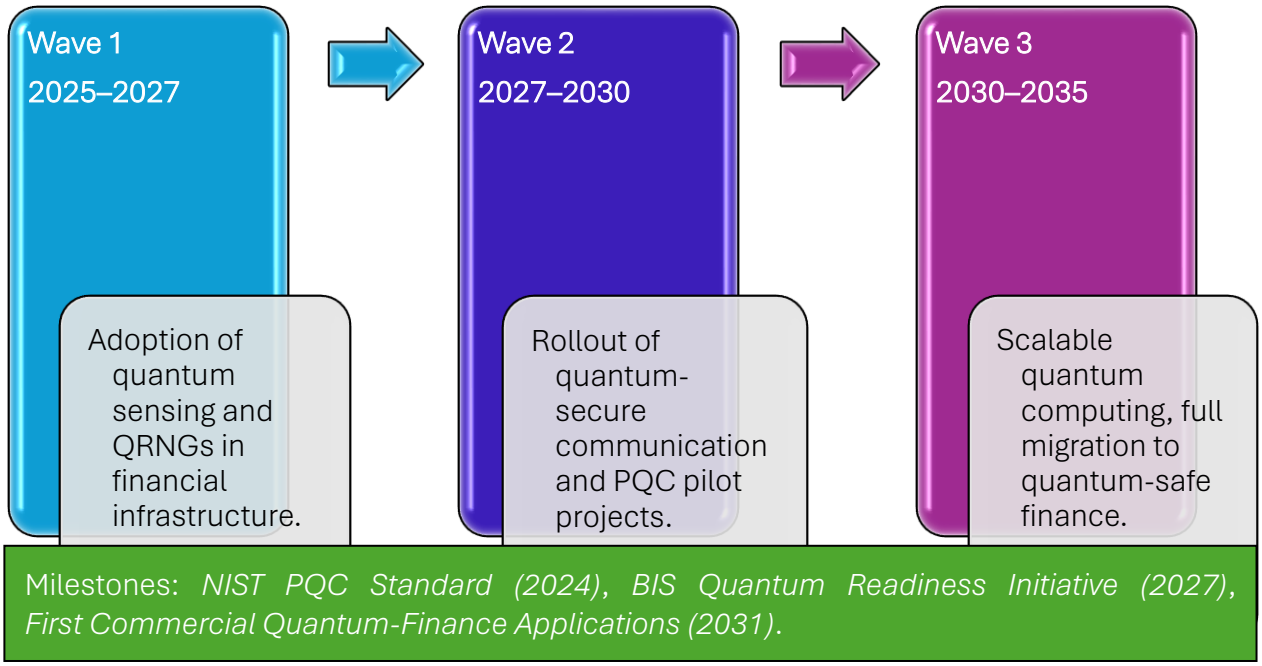
Box 2 demystifies quantum concepts for non-technical readers, linking them directly to financial functions. Understanding **superposition**, **entanglement**, and **interference** is crucial for appreciating both the vulnerability of existing cryptography and the potential of quantum-enabled analytics. These principles underpin *both the risk of decryption and the promise of innovation* (NIST, 2024; MIT, 2024).

Figure 4 situates technological milestones along a timeline of expected financial relevance, from sensing adoption to post-quantum cryptography (PQC) integration.

Figure 4 indicates that quantum impact will unfold gradually but inexorably. While sensing and communication deliver near-term benefits, the computing frontier introduces long-term systemic risk. Supervisors and market participants must therefore adopt a staggered readiness approach — protecting current systems today while investing in quantum innovation for tomorrow. Financial institutions must act in advance of Wave 3; waiting for full-scale quantum

computers would mean being overtaken by the risk curve. Proactive investment in hybrid PQC and talent development is therefore essential (BIS, 2024; OECD, 2025).

Figure 4 – Timeline of Quantum Readiness for Finance



Source: Bank & Finance elaboration based on NIST (2024); BIS (2024); OECD (2025); WEF (2025).

Box 3 highlights selected real-world examples of how financial institutions and central banks are already experimenting with quantum technologies.

Box 3 – Financial Institutions on the Quantum Frontier

BBVA and HSBC (Europe): Piloting quantum algorithms for portfolio optimization, achieving up to 20% efficiency improvements in computational speed for test portfolios.

JP Morgan Chase (U.S.): Developing quantum algorithms for derivative pricing and risk modeling in partnership with IBM Quantum.

Bank of Canada and BIS Innovation Hub: Testing quantum-safe encryption protocols for interbank data transfers and CBDC transaction integrity.

Singapore Monetary Authority (MAS): Integrating quantum random number generators into national digital-identity infrastructure to strengthen authentication mechanisms.

These initiatives remain largely experimental but signal an emerging shift from academic exploration to applied development. The main lesson is that institutional readiness is advancing unevenly: a few global leaders are moving ahead, while most of the system remains in early-awareness stages.

Source: Bank & Finance elaboration based on Bank & Finance (2025f); BIS Innovation Hub (2024); IBM Quantum (2025); JP Morgan (2024); MAS (2025).

The cases in Box 3 illustrate a pattern familiar from the AI revolution (Bank & Finance, 2025f): early movers gain *learning advantages* that compound over time. Financial institutions are beginning to operationalize use cases, often in collaboration with technology providers. Institutions like JP Morgan or BBVA are not merely experimenting with new computation; they are building organizational fluency that will become a source of competitive resilience once quantum technology matures (IBM Quantum, 2025). The next challenge is to ensure that these isolated pilots evolve into coordinated system-wide standards to prevent fragmentation and ensure interoperability.

From Physics to Policy

Quantum technology is not a single breakthrough but a **family of interrelated capabilities** progressing along distinct but converging trajectories. The financial relevance of quantum technology lies not in its underlying physics but in its **interaction with institutions of trust**. For finance, this means exposure on multiple fronts: data protection, infrastructure precision, and analytical computation. Payment systems, custodial networks, and data repositories all depend on reliable time stamps, encryption, and validation. Quantum technologies intervene directly in these mechanisms.

1. **Quantum Sensing** can deliver unprecedented precision to time-critical systems like RTGS settlement and satellite navigation (ESA, 2024). Even nanosecond errors in synchronization can distort valuations in high-frequency markets; quantum clocks mitigate such discrepancies.
2. **Quantum Communication** provides end-to-end data security by making interception physically detectable (Bennett & Brassard, 1984). For central-bank digital currencies (CBDCs), this could ensure *tamper-proof monetary messaging* across borders.
3. **Quantum Computing**, while threatening current cryptography, also enables modelling of interconnected risks — a "quantum twin" of the global financial system capable of stress-testing interdependencies in real time (BIS Innovation Hub, 2024).

Thus, understanding quantum technology is the first step toward building **quantum policy**. The next section examines the dark mirror of this potential: how quantum computing could compromise financial stability by breaking the mathematical backbone of digital security.

3. Quantum Threats to Financial Systems

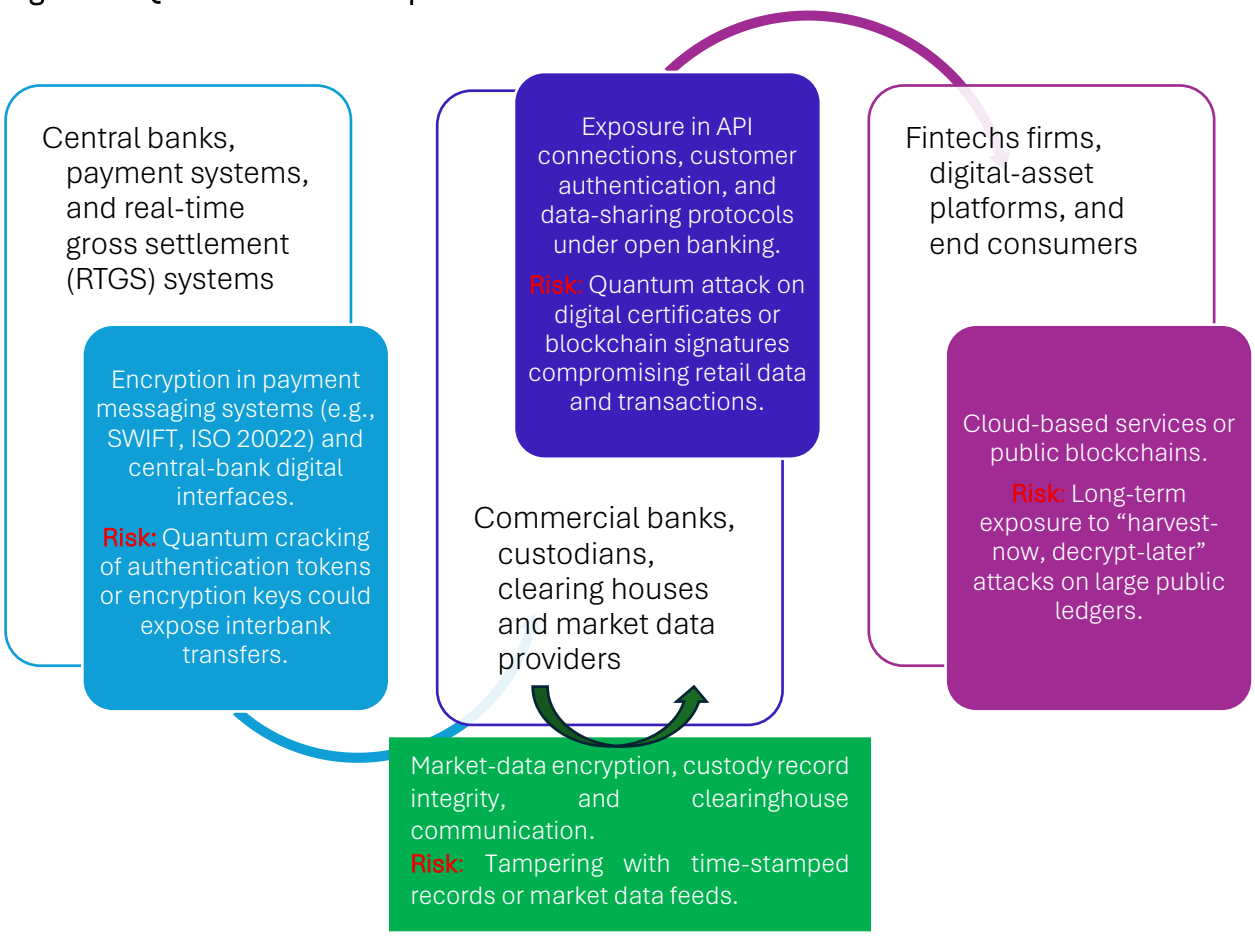
While the previous section explored how quantum technology functions, the present one examines its destabilizing potential for the global financial architecture. At the heart of the threat lies a paradox: the same mathematical elegance that powers encryption today — large-number factorization and elliptic-curve computations — is precisely what quantum computing renders tractable (Shor, 1994). Once scalable quantum machines exist, the confidentiality and authenticity of nearly every digital financial transaction could collapse.

Financial infrastructures were built on the assumption that decryption would remain computationally infeasible for centuries. That assumption no longer holds. As BIS (2024) warns, "quantum computing introduces the possibility of a systemic cryptographic shock." A single breakthrough could invalidate global standards such as RSA-2048 or ECC, compromising SWIFT messages, settlement instructions, and even central-bank digital-currency ledgers (NIST, 2024; FSB, 2023).

The danger extends beyond the future. Adversaries are already **harvesting encrypted data today** in anticipation of decrypting it later — a tactic known as *harvest-now, decrypt-later*. This creates a latent stock of compromised information whose risk increases over time (ENISA, 2025). Consequently, quantum risk is not a discrete event, but a cumulative exposure embedded in every dataset secured with vulnerable cryptography.

Figure 5 visualizes the channels through which quantum vulnerabilities permeate the financial ecosystem.

Figure 5 – Quantum Threat Map for Global Finance



Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); NIST (2024); ENISA (2025).*

The map illustrates that vulnerability is densest where trust is most concentrated — certificate authorities, custodians, and messaging networks. A compromise at any of these nodes could cascade through liquidity, confidence, and payment channels (BIS, 2024; OECD, 2025).

Table 3 classifies critical financial systems by encryption type, exposure, and estimated timeline to quantum compromise.

Table 3 – Financial Systems at Risk from Quantum Decryption

System / Application	Primary Encryption Standard Used	Quantum Vulnerability	Expected Impact	Estimated Risk Horizon*
Interbank payments (SWIFT, RTGS)	RSA-2048, TLS 1.3	High – keys can be factored by Shor's algorithm	Loss of confidentiality and authentication of messages	5–10 years
Central-bank reserves and CBDC ledgers	ECC-based digital signatures	High – discrete-logarithm problem vulnerable	Potential manipulation of digital-currency validation	7–12 years
Market-data networks & trading APIs	PKI certificates, RSA	Medium – session key compromise	Market manipulation, insider leakage	5–10 years
Blockchain-based assets (crypto, tokenized deposits)	ECDSA / Ed25519	Critical – all public keys exposed on-chain	Theft of digital assets, collapse of trust	3–8 years
Cloud services & data warehouses	Hybrid AES / RSA	Low-Medium – symmetric crypto relatively resistant but key-exchange vulnerable	Breach of stored customer data	8–15 years

**Risk horizon indicates estimated timeframe when scalable quantum computing (with error-correction > 10^6 logical qubits) could break current standards.*

Source: *Bank & Finance elaboration based on NIST (2024); NSA (2024); BIS (2024); OECD (2024).*

Two observations stand out. First, asymmetric cryptography — which secures authentication and signatures — is the weak link. Second, data longevity amplifies exposure: interbank archives and blockchain ledgers store information indefinitely, extending the window for future decryption (NIST, 2024; NSA, 2024). Hence, PQC migration should precede rather than follow quantum breakthroughs.

Box 4 explains one of the most misunderstood dimensions of quantum risk: the time lag between data theft and decryption.

Box 4 – Harvest Now, Decrypt Later: The Invisible Countdown

Cybercriminals and state actors increasingly archive vast troves of encrypted information — including bank transfers, emails, and certificates — under the assumption that quantum computers will eventually unlock them.

The process involves three stages:

1. **Acquisition:** Compromise or intercept encrypted data through standard breaches or mass scraping of communication backbones.
2. **Archival:** Store the encrypted data indefinitely; disk space is cheap and expanding.
3. **Decryption:** Once quantum resources become available, use algorithms such as Shor's or Grover's to break the original encryption keys.

This delayed-impact mechanism means that even data stolen innocuously in 2025 could be compromised in 2032 or later, long after institutions have changed systems or personnel. Sensitive categories include interbank payment archives, identity credentials, customer PII, and proprietary algorithms.

The "harvest-now, decrypt-later" dynamic transforms quantum risk from a *future* event into a *present* one. Every day that institutions continue to use non-quantum-safe encryption, they accumulate latent exposure. Regulators may need to treat cryptographic migration as part of operational-resilience supervision rather than optional innovation.

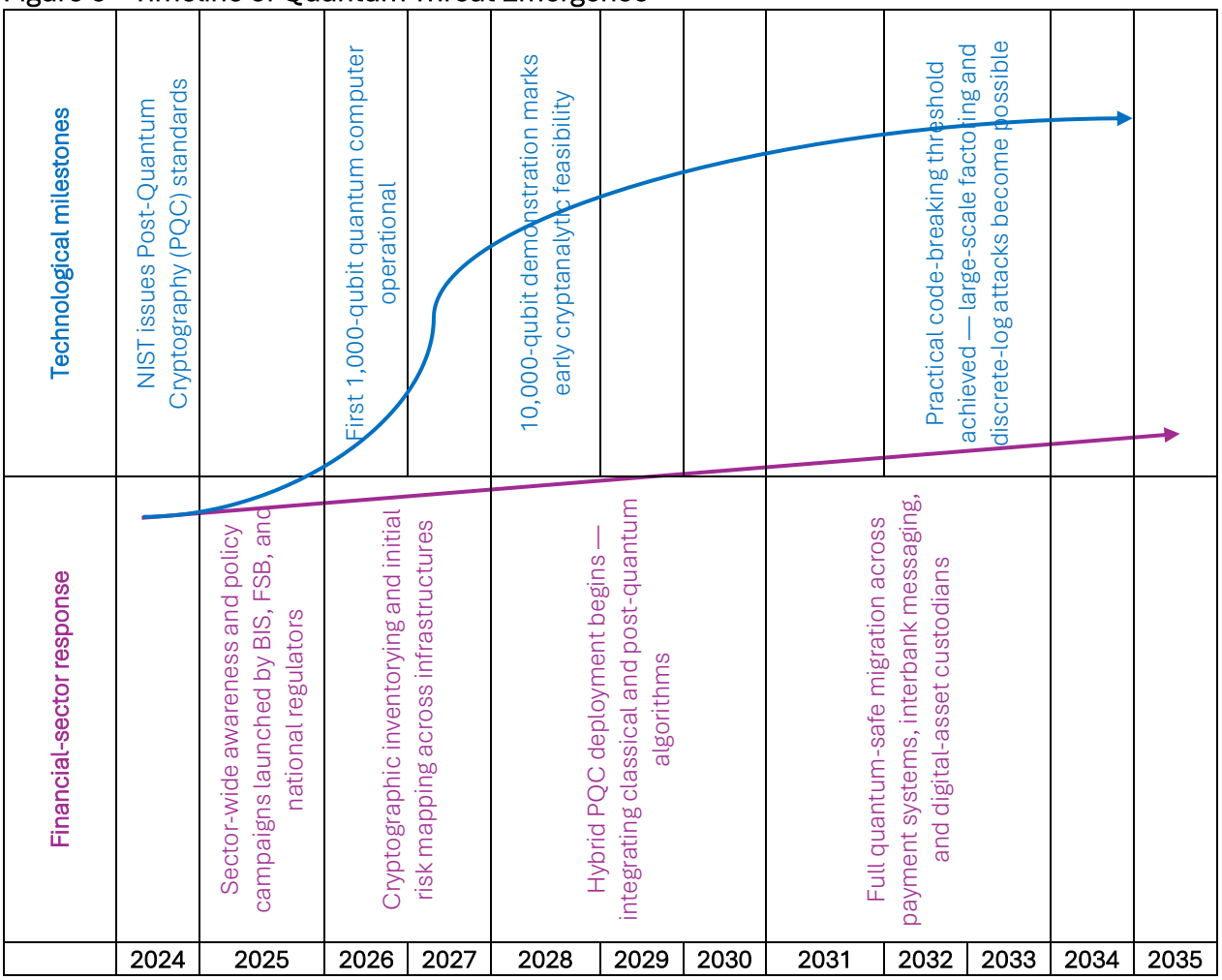
Source: *Bank & Finance elaboration based on ENISA (2025); NIST (2024); FSB (2023).*

This temporal lag transforms cryptography from a technical parameter into a **macroeconomic liability**. Institutions continue to accumulate "encryption debt" — future exposure resulting from today's algorithms. The only mitigation is early adoption of hybrid post-quantum solutions (ENISA, 2025; BIS, 2024).

Figure 6 projects the expected stages of quantum-related financial risk between 2024 and 2035, distinguishing between technological milestones and regulatory responses.

Figure 6 makes visible the *quantum readiness gap* — the period in which technological capability outpaces policy adaptation. Unless institutions initiate migration well before 2030, the financial system may face a cryptographic "cliff edge" — a moment when old standards fail faster than new ones are deployed (BIS, 2024; FSB, 2023).

Figure 6 – Timeline of Quantum Threat Emergence



Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); NIST (2024); OECD (2025); ENISA (2025).*

Box 5 adapts the systemic-risk logic from *Cyber Resilience in Finance* to show how a single cryptographic failure could propagate across the financial ecosystem. It illustrates why prudential oversight must extend beyond IT. If cryptographic integrity fails, capital and liquidity buffers offer little protection. Supervisors should therefore treat encryption integrity as a component of financial soundness — analogous to stress-testing or cyber-resilience assessments (BIS, 2024; ECB, 2025).

Box 5 – Quantum Risk Transmission Channels

Quantum vulnerabilities can propagate through at least four channels:

1. **Operational Channel:** Decryption of authentication keys leads to unauthorized access, payment manipulation, or transaction replay.
2. **Market Channel:** Breach of trading data or algorithms triggers insider advantages, liquidity distortions, and confidence loss.

3. **Reputational Channel:** Compromised encryption undermines public trust in digital banking, payment systems, and tokenized assets.
4. **Cross-Border Channel:** Fragmented adoption of quantum-safe standards creates interoperability failures between jurisdictions.

These channels mirror the contagion dynamics observed in cyber incidents but operate at a deeper layer — the *mathematical substrate of trust*. Unlike conventional operational shocks, quantum breaches would be nearly impossible to contain post-factum, as compromised data could be reused indefinitely.

Source: *Bank & Finance elaboration based on FSB (2023); BIS (2024); ECB (2025).*

Table 4 simulates a stylized crisis in which quantum actors decrypt archived payment credentials, demonstrating the potential for system-wide contagion.

Table 4 – Illustrative Stress Scenario: Quantum Breach of Global Payments

Event Sequence	Description	Immediate Effects	Systemic Spillovers
Day 0 – Compromise	Quantum actor decrypts archived SWIFT credentials of multiple correspondent banks.	Unauthorized payment instructions; liquidity mismatches.	Market uncertainty; short-term funding freeze.
Day 1–2 – Contagion	Central banks detect anomalies; cross-border settlements halted.	Payment-system downtime; surge in collateral demands.	Interbank markets seize; repo and FX spreads widen.
Week 1 – Confidence shock	Public announcement; trust erosion in digital-banking infrastructure.	Stock sell-offs in financial institutions; spike in CDS spreads.	Systemic funding stress; possible run on digital deposits.
Month 1 – Policy response	Coordinated central-bank backstop and emergency re-encryption of networks.	Stabilization but residual distrust in digital channels.	Long-term shift toward quantum-safe infrastructure.

Source: *Bank & Finance elaboration based on FSB (2023); IMF (2024); BIS (2024).*

The scenario mirrors the dynamic of previous systemic events: loss of confidence triggers liquidity stress, forcing central-bank intervention (IMF, 2024). But unlike 2008's credit crunch, a quantum breach undermines *trust in the infrastructure itself*. Recovery would require wholesale replacement of cryptographic systems rather than liquidity injections (BIS, 2024).

Integrating Prudential and Technological Perspectives

The quantitative horizon for cryptographic vulnerability remains debated. Optimistic estimates place practical quantum factoring a decade away (Mosca, 2022), but pessimistic projections

cite recent hardware acceleration and algorithmic refinements that could shorten this to five years (Gidney & Ekerå, 2021). Either way, policy inertia is costlier than premature action.

Central banks and regulators are therefore encouraged to establish **Quantum-Readiness Assessments (QRAs)**, mirroring the stress-testing approach used for liquidity and capital adequacy (BIS, 2024). QRAs would inventory cryptographic assets, evaluate vendor exposure, and set migration deadlines.

Furthermore, the private sector should embed quantum scenarios into existing **Operational-Resilience Frameworks** under the Basel Committee and DORA regimes. This integration would align quantum risk with established prudential language and supervisory cycles (FSB, 2023; ENISA, 2025).

Section Synthesis

Figures 5 and 6 and Tables 3 and 4 reveal a clear pattern: quantum risk is both technological and temporal. Its impact unfolds slowly but irreversibly through data exposure, and its resolution requires systemic migration rather than containment. Prudential policy must therefore move from reactive incident management to **pre-emptive architecture replacement**. The lesson for financial authorities is unequivocal: cryptography is the new capital — a resource that must be managed, tested, and replenished to sustain trust. The following section explores how this can be achieved through the design of a quantum-safe financial ecosystem and the emergence of global standards for **building quantum resilience**.

4. Building Quantum Resilience

The preceding section showed that the quantum threat is structural and cumulative; this section turns from diagnosis to design. **Quantum resilience** refers to the capacity of financial systems to preserve confidentiality, integrity, and operational continuity despite quantum-enabled disruption. It requires not only replacing vulnerable cryptography but also redesigning institutional governance, market coordination, and supervisory frameworks.

Historically, financial resilience has evolved through three eras:

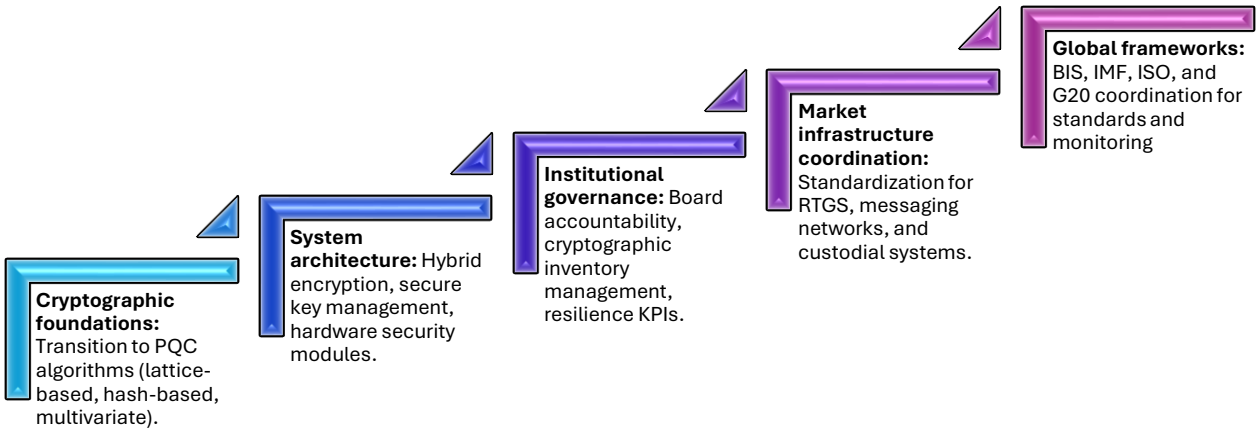
1. *Capital resilience* after the banking crises of the 1980s, institutionalized through the Basel Accords;
2. *Cyber resilience* after 2010, embedded through DORA, NIS2, and the FSB's operational-resilience principles (FSB, 2023); and now
3. *Quantum resilience* — a fusion of technical and prudential adaptation (BIS, 2024).

Unlike its predecessors, quantum resilience concerns the **mathematical foundations** of trust, not merely its operational expression. The challenge is to synchronize technological innovation

with institutional reform before quantum computing reaches cryptographically disruptive scale (NIST, 2024; OECD, 2025).

Figure 7 outlines a multi-layer defense model linking technical, institutional, and global coordination dimensions.

Figure 7 – Layers of Quantum Resilience in Finance



Source: Bank & Finance elaboration based on BIS (2024); NIST (2024); FSB (2023); OECD (2024).

Figure 7 mirrors the evolution of cyber resilience frameworks: from *technical hygiene* to *strategic governance*. Quantum resilience will only succeed if all layers operate coherently — technical upgrades must be embedded in governance, and governance must translate into global standards (BIS, 2024; FSB, 2023). A cryptographically upgraded payment system, for example, remains exposed if supervisory rules or inter-jurisdictional standards lag behind.

The Strategic Shift: From Cyber Hygiene to Cryptographic Architecture

Cyber resilience focused on *response and recovery*; quantum resilience focuses on *replacement and redesign*. Institutions can no longer rely on patching: once a quantum computer breaks RSA, all related credentials are compromised permanently. Therefore, the goal is **anticipatory migration** rather than reactive mitigation.

Three pillars define this shift (ENISA, 2025; BIS, 2024):

1. **Cryptographic inventory and risk mapping** — identify every system, vendor, and dataset that depends on vulnerable algorithms.
2. **Hybrid deployment** — combine classical and post-quantum cryptography (PQC) until standards mature.
3. **Supervisory integration** — embed quantum resilience into prudential oversight, stress-testing, and disclosure.

Box 6 outlines the main strategic milestones that financial institutions must meet between 2025 and 2035 to complete the transition toward post-quantum security.

Box 6 – From Awareness to Action: The Post-Quantum Imperative

1. 2025–2026 – Awareness and Inventory
   - Establish governance responsibility at board and CISO levels.
   - Conduct full inventory of cryptographic assets, dependencies, and lifespans (e.g., digital certificates, hardware tokens, APIs).
   - Engage with national quantum-readiness programs and NIST PQC algorithm adoption guidelines.

2. 2026–2028 – Experimentation and Hybrid Deployment
   - Pilot hybrid cryptographic schemes combining classical (RSA/ECC) and PQC algorithms for secure key exchange.
   - Integrate quantum-random-number generators (QRNGs) to enhance entropy and unpredictability.
   - Develop internal testing sandboxes for PQC implementation within payment and settlement systems.

3. 2028–2030 – Institutionalization
   - Embed quantum resilience into operational-risk frameworks, stress testing, and regulatory reporting.
   - Revise outsourcing and cloud-service contracts to include PQC compliance clauses.
   - Update digital-identity and KYC protocols to ensure quantum-safe authentication.

4. 2030–2035 – Global Convergence and Continuous Testing
   - Align national implementations with BIS and ISO quantum-security standards.
   - Participate in cross-border PQC interoperability tests.
   - Conduct periodic "quantum fire drills" simulating large-scale decryption scenarios.

Source: *Bank & Finance elaboration based on NIST (2024); FSB (2023); BIS (2024); ECB (2025).*

Box 6's four-phase roadmap illustrates that migration is a decade-long transformation rather than a single technological upgrade. The timeline underscores the urgency of early action: institutions that wait for regulatory mandates will face integration costs exponentially higher than early movers. Central banks and market infrastructures—should lead through pilots and sandboxes, building collective capacity as PQC matures (NIST, 2024; ECB, 2025).

Table 5 summarizes the main PQC algorithms recommended by NIST and ISO, highlighting their mechanisms, maturity, and suitability for different financial applications.

Table 5 – Post-Quantum Cryptography (PQC) Algorithms and Financial Suitability

Algorithm Family	Representative Algorithm (NIST Standard)	Mathematical Basis	Key Financial Applications	Advantages	Challenges / Limitations
Lattice-based	CRYSTALS-Kyber (key exchange), CRYSTALS-Dilithium (signatures)	Learning With Errors (LWE) problem	Payment authentication, SWIFT messaging, interbank settlement	High performance; scalable; strong security proofs	Larger key sizes; implementation complexity
Hash-based	SPHINCS+	Hash tree structures	Long-term archival and digital signatures	Proven security; stateless verification	Larger signatures; slower processing
Code-based	Classic McEliece	Error-correcting codes	Secure email, archival data	Long history of study; resistant to quantum and classical attacks	Very large public keys (hundreds of KB)
Multivariate	Rainbow (withdrawn), GeMSS (experimental)	Polynomial equations over finite fields	Specialized applications, not yet production-ready	Efficient key generation	Under review; potential weaknesses
Isogeny-based	SIKE (withdrawn due to attack, 2022)	Elliptic-curve isogenies	Experimental, research only	Compact keys	Currently insecure

Source: *Bank & Finance elaboration based on NIST (2024); ISO/IEC 14888-4 (2024); ETSI (2024).*

Table 5 illustrates that *no single PQC algorithm fits all use cases*. Financial institutions must adopt a portfolio approach, selecting algorithms according to latency, bandwidth, and regulatory constraints. The key insight is to **begin hybrid implementation early**—using classical and PQC algorithms in tandem—while standards mature. Lattice-based approaches (Kyber, Dilithium) currently offer the most balanced trade-off between performance and security. Hash-based methods (SPHINCS+) provide long-term archival protection but at the cost of larger signatures. Supervisors should encourage institutions to adopt **hybrid configurations**—for instance, combining RSA with Kyber for key exchange—while maintaining backward compatibility (NIST, 2024; ISO, 2025).

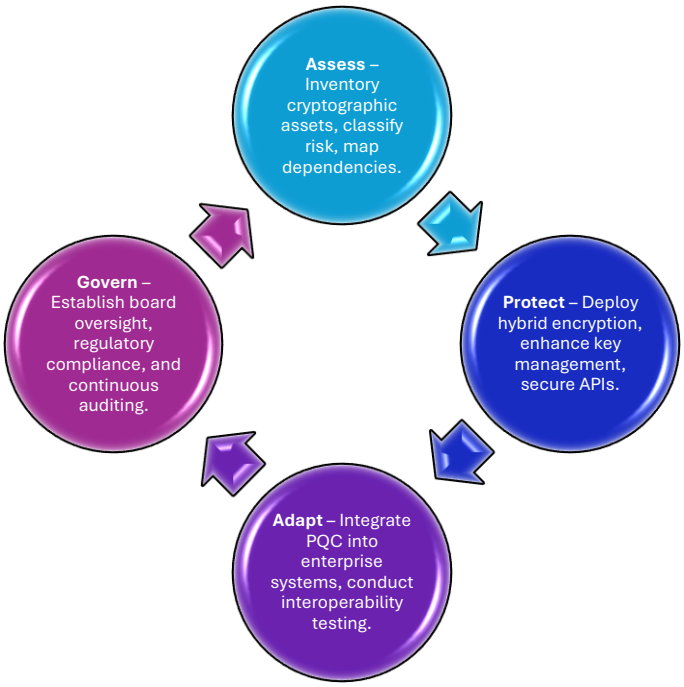
Implementation Dynamics

The migration to PQC will unfold unevenly. Large global banks and central banks have both the capability and incentive to move first; smaller institutions may depend on third-party vendors. This asymmetry requires regulatory coordination to avoid creating "cryptographic blind spots."

A BIS-led *Quantum Resilience Forum* could serve as the coordination hub, mirroring how the FSB harmonized cyber-resilience lexicons in the 2010s (BIS, 2024; FSB, 2023).

Figure 8 visualizes the sequential phases of the quantum-safe transition for financial institutions and supervisors.

Figure 8 – The Quantum-Safe Transition Framework



Source: Bank & Finance elaboration based on BIS (2024); IMF (2024); OECD (2025).

Figure 8 shows resilience as an iterative governance process—Assess → Protect → Adapt → Govern. This mirrors the risk-management cycles of DORA and the CPMI-IOSCO Principles, ensuring that quantum resilience becomes part of supervisory DNA rather than a separate compliance project. The figure reflects the practical architecture for implementation — iterative, auditable, and governance-driven. The goal is not immediate replacement but progressive hardening of financial infrastructures against quantum risk. Supervisors can use the same sequence to design national roadmaps and monitoring templates (ECB, 2025; OECD, 2025).

Box 7 showcases selected country initiatives leading the global shift toward quantum-safe finance, offering lessons for cross-border coordination. These national initiatives illustrate divergent but complementary strategies: the U.S. prioritizes standardization; the EU emphasizes regulation; China focuses on infrastructure sovereignty; and emerging markets integrate PQC into digital-currency modernization (MCTI-Brazil, 2024; ENISA, 2025). Coordination among them is essential to prevent a fragmented quantum geography.

Box 7 – Case Study: National Quantum-Safe Initiatives

- **United States:** The *Quantum Computing Cybersecurity Preparedness Act (2023)* mandates federal agencies to inventory and migrate cryptographic systems; NIST leads algorithm standardization.
- **European Union:** Under the *Digital Operational Resilience Act (DORA)*, the EU Commission and ENISA are preparing guidance on PQC integration within financial infrastructures.
- **China:** The *Beijing Quantum Information Highway* and *Micius Satellite* projects provide global leadership in quantum key distribution; several state banks are testing QKD for secure interbank communication.
- **Singapore and Japan:** Public-private partnerships fund quantum-safe payment pilots and talent programs.
- **Brazil:** The *National Quantum Strategy (2024)* links PQC adoption to digital-finance modernization under the Pix and Drex frameworks.

Source: *Bank & Finance elaboration based on NIST (2024); ENISA (2025); OECD (2025); MCTI-Brazil (2024); MAS (2025).*

Table 6 offers a self-assessment template enabling institutions to track their progress along six dimensions of resilience. This checklist converts abstract strategy into measurable practice. By 2030, financial institutions should achieve at least "hybrid readiness," meaning that 80 percent of mission-critical applications employ PQC or QKD protection. Supervisors could require annual attestation of these metrics, analogous to cyber-resilience maturity assessments (FSB, 2023; BIS, 2024).

Table 6 – Institutional Quantum Resilience Checklist

Dimension	Key Questions	Target Practice by 2030
Governance	Is board-level accountability for quantum risk established?	Yes – oversight embedded in risk committee mandates
Inventory	Has the institution catalogued all cryptographic assets and dependencies?	Comprehensive inventory updated annually
Technology	Are hybrid PQC schemes deployed for core systems?	≥80% of mission-critical applications quantum-safe
Testing	Are periodic penetration and decryption simulations performed?	Annual "quantum drills" with external auditors
Coordination	Are external vendors and counterparties aligned on PQC standards?	Contractual PQC clauses with key partners
Reporting	Is quantum resilience disclosed in operational-risk reporting?	Included in annual risk disclosures and stress-testing documentation

Source: *Bank & Finance elaboration based on FSB (2023); BIS (2024); NIST (2024).*

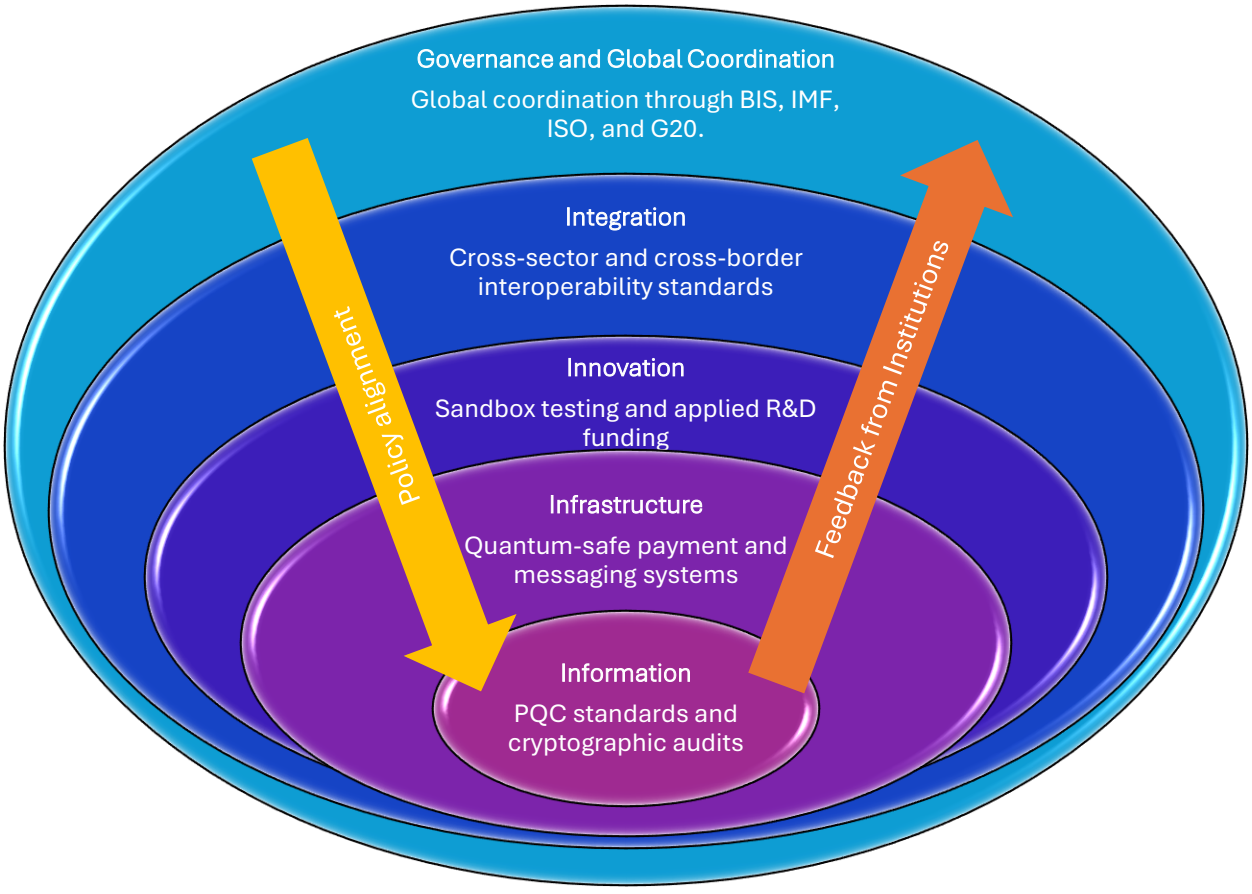
Institutional and Global Governance

Governance is the connective tissue of quantum resilience. Institutional accountability must reach board level: encryption is no longer purely a technical issue but a fiduciary duty linked to trust and reputation. At the macro level, global governance should rest on three pillars:

1. **Standardization:** harmonize PQC and QKD protocols through ISO/ETSI coordination.
2. **Supervision:** embed QRAs and resilience audits into BIS and IMF surveillance cycles.
3. **Solidarity:** create funding mechanisms such as the IMF's proposed *Quantum-Resilience Facility* to support emerging markets.

Figure 9 integrates quantum resilience into the broader *Five-Layer Financial Ecosystem* architecture, illustrating how responsibilities distribute across layers of coordination.

Figure 9 – Five-Layer Governance Framework for Quantum-Safe Finance



Source: *Bank & Finance elaboration based on Bank & Finance Ecosystem Framework (2025i); BIS (2024); IMF (2024).*

This figure visualizes governance coherence: technological hardening and institutional adoption (inner layers) must align with multilateral policy (outer layers). Without this vertical

integration, the world risks a “quantum divide” where some economies enjoy algorithmic sovereignty while others depend on foreign cryptographic infrastructure (OECD, 2025; IMF, 2024).

Operational and Cultural Challenges

Technological migration alone cannot secure financial trust. Human and organizational factors remain critical. Staff training, vendor management, and culture of proactive adaptation will determine success. Past crises show that resilience ultimately depends on institutional learning rather than hardware upgrades (Weick & Sutcliffe, 2011). Therefore, central banks and regulators should sponsor *Quantum Readiness Programs* combining education, simulation, and cross-sector collaboration.

Moreover, policymakers must guard against “security fatigue.” As in the early days of cybersecurity, institutions may perceive quantum threats as distant and intangible. Clear communication of timelines, standardized reporting templates, and integration into existing risk frameworks will help maintain momentum (ENISA, 2025).

Section Summary and Lessons

Section 4 reframes quantum security from technical challenge to **systemic capability**. Resilience requires sustained investment, cross-border cooperation, and new supervisory mandates. Figures 7–9 and Tables 5–6 demonstrate that building quantum resilience is feasible but demands early, coordinated action.

Three overarching lessons emerge:

1. **Anticipate rather than react**—the cost of early migration is lower than post-breach reconstruction.
2. **Governance is infrastructure**—without institutional accountability, technical defenses erode.
3. **Inclusion safeguards stability**—global coordination must prevent technological asymmetry from becoming financial fragmentation.

The next section explores the *positive frontier*—how quantum technologies, once secured, can drive innovation, analytics, and sustainable-finance transformation.

5. Quantum Opportunities in Finance

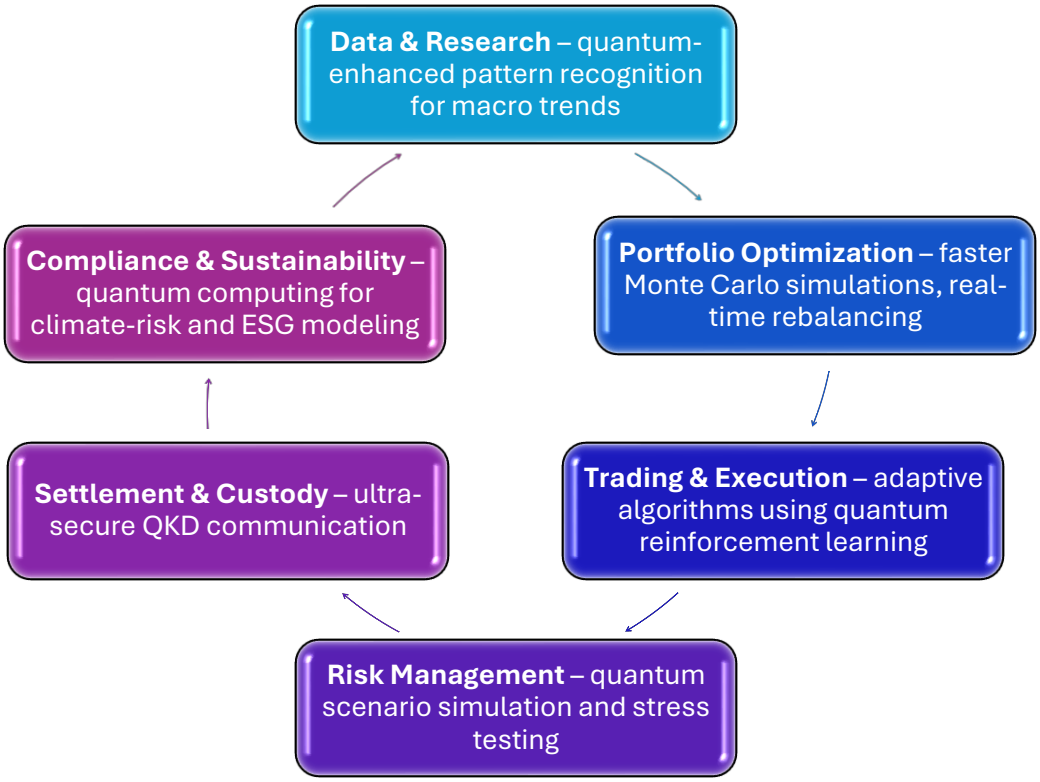
Quantum technology does not only threaten the financial system—it also holds the potential to **redefine its analytical, operational, and strategic frontiers**. Every historical leap in computation—from mechanical calculators to mainframes, then to digital and cloud

architectures—has expanded finance's ability to process complexity. Quantum computing extends that curve exponentially: by enabling parallel exploration of vast probability spaces, it promises to transform how institutions model uncertainty, allocate capital, and manage systemic risk (Arute et al., 2019; BIS, 2024).

This section explores how quantum technology can become a *competitive and public good*: improving efficiency, predictive accuracy, and sustainability. The shift from quantum risk to quantum opportunity is not just defensive adaptation; it is a **new phase in the evolution of financial intelligence**.

Figure 10 depicts how quantum technology permeates the financial value chain—from data acquisition to settlement and compliance—mirroring the multi-layer model of the broader financial ecosystem.

Figure 10 – Quantum Value Chain in Financial Services



Source: Bank & Finance elaboration based on BIS Innovation Hub (2025); IBM Quantum (2025); WEF (2025); OECD (2025).

Figure 10 illustrates that quantum impact spans the entire financial lifecycle with quantum's benefits compounding across stages. Gains in data precision and modeling efficiency enhance not only trading and risk management but also supervisory and sustainability analytics. In this sense, *quantum advantage* becomes a form of systemic efficiency. The challenge for institutions is to identify use cases that deliver **quantifiable advantage** before the technology matures at scale (OECD, 2025; WEF, 2025).

Table 7 enumerates concrete quantum applications across the Five-Layer Financial Ecosystem, distinguishing short-term pilots from long-term transformations.

Table 7 – Quantum Use Cases Across the Financial Ecosystem

Ecosystem Layer	Near-Term Applications (2025–2030)	Long-Term Opportunities (2030–2040)	Strategic Payoff
Information	Quantum random-number generators (QRNGs) for secure tokenization; improved data encryption.	Quantum-secured global data networks via satellite QKD.	Reinforced data integrity and digital-trust premium.
Infrastructure	Quantum sensing for time synchronization in payment systems; enhanced satellite navigation.	Quantum-optimized routing for global payment and logistics networks.	Higher system reliability and reduced latency.
Innovation	Quantum algorithms for portfolio optimization and risk modeling; hybrid quantum–AI analytics.	Full quantum financial simulators integrating macro-financial feedback loops.	Superior decision-making and predictive capability.
Integration	Quantum computing partnerships between banks, fintechs, and research labs.	Cross-sector quantum-cloud ecosystems with financial APIs.	Economies of scale, shared innovation costs.
Governance	Policy simulations using quantum computation for systemic stress testing.	Quantum-enhanced ESG and climate-risk assessment tools for regulation.	Informed, evidence-based policymaking.

Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024); IBM Quantum (2025); McKinsey (2025).*

These cases demonstrate that quantum technology is both a **defensive tool** (through encryption and timing) and an **offensive capability** (through analytics and optimization). Early experimentation — even on limited quantum hardware — will be critical for capacity building and human-capital development across the financial ecosystem. The applications cluster into three horizons.

1. **Operational security** (2025–2030): QRNGs, QKD, and PQC protect digital trust.
2. **Analytical advantage** (2028–2035): hybrid quantum-AI systems enhance forecasting, stress testing, and portfolio construction.
3. **Policy intelligence** (post-2035): full-scale simulation enables macro-prudential design under deep uncertainty (BIS Innovation Hub, 2025).

The policy implication is to integrate quantum experimentation into innovation frameworks such as the *FSB SupTech and RegTech Roadmaps* (FSB, 2024).

Box 8 examines how quantum algorithms are already being tested in financial modeling and portfolio optimization.

Box 8 – Quantum Computing in Financial Modeling

Financial modeling involves solving high-dimensional problems — from pricing exotic derivatives to optimizing portfolios under uncertainty. Quantum computers excel in these domains because they can evaluate multiple outcomes simultaneously.

Key prototypes include:

- **Portfolio Optimization:** Institutions like **BBVA** and **Goldman Sachs** have tested quantum algorithms based on the *Quantum Approximate Optimization Algorithm (QAOA)* to find optimal asset allocations under complex constraints. Results show potential speed-ups of 10–100× relative to classical heuristics.
- **Derivative Pricing:** Quantum amplitude estimation can reduce the computational complexity of Monte Carlo simulations from $O(1/\varepsilon^2)$ to $O(1/\varepsilon)$, drastically accelerating valuation of path-dependent instruments.
- **Risk Aggregation:** Quantum simulators can model correlated shocks across thousands of risk factors simultaneously, supporting systemic-risk forecasting and stress testing.

Source: *Bank & Finance elaboration based on IBM Quantum (2025); BIS Innovation Hub (2024); BBVA (2024); Goldman Sachs (2024).*

Quantum computing is unlikely to replace traditional analytics soon, but it will **redefine the efficiency frontier**. Institutions that integrate quantum pilots into their R&D, will accumulate algorithmic and human-capital advantages that compound over time. Quantum algorithms such as **Quantum Approximate Optimization Algorithm (QAOA)** and **Variational Quantum Eigensolver (VQE)** exploit the same physics that threatens encryption—superposition and interference—to evaluate millions of portfolio combinations simultaneously (Farhi et al., 2014). Their adoption could compress hours of risk simulation into seconds, transforming regulatory stress testing and asset allocation (BBVA, 2024; IBM Quantum, 2025).

From Computational Scarcity to Quantum Abundance

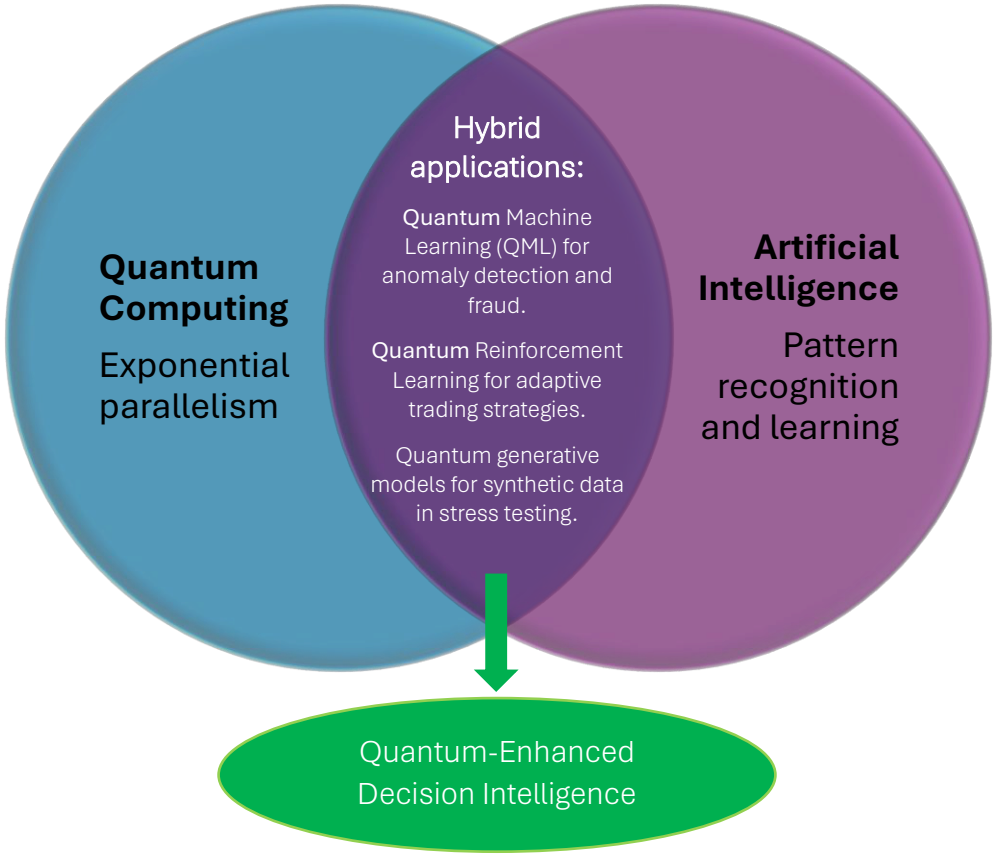
Traditional finance operates under computational scarcity: models simplify reality to remain tractable. Quantum computing removes much of that constraint, allowing *direct simulation of interdependence*. Monte Carlo simulations—currently limited by sequential sampling—could be replaced by **amplitude estimation**, offering quadratic speed-ups (Montanaro, 2016). For systemic-risk analysis, this means running full-network contagion models across thousands of institutions in real time (BIS, 2024).

At the same time, quantum technology reshapes the **cost structure of precision**: what was once computationally prohibitive—multi-factor scenario modeling or high-resolution climate data integration—becomes routine. This will blur the distinction between micro-prudential risk modeling and macro-financial forecasting, enabling *continuous prudential simulation*.

Figure 11 illustrates the emerging convergence between quantum computing and artificial intelligence — a development already reshaping predictive analytics.

This figure captures the synergy between two transformative forces. AI amplifies insights from data; quantum amplifies the *speed and depth* of those insights. The combination could enable predictive stress tests, dynamic hedging, and even real-time systemic-risk monitoring — functions that classical computing cannot perform efficiently. Early research suggests that **quantum machine learning (QML)** could outperform classical ML for pattern recognition in high-dimensional data, such as fraud detection or ESG analytics (Huang et al., 2021). For regulators, this convergence implies a new era of **predictive supervision**, where systemic anomalies are detected before they escalate (BIS, 2024).

Figure 11 – Quantum-AI Convergence: The Next Frontier



Source: Bank & Finance elaboration based on BIS (2025); IBM (2025); MIT (2025); WEF (2025).

Table 8 summarizes benchmark comparisons between classical and quantum approaches in key financial tasks, highlighting potential efficiency gains. It quantifies efficiency gains that could reshape competitive advantage. Even moderate quantum advantage — say, a 10× speed-up — could translate into major competitive leverage for institutions processing millions of transactions per day. Impacts pricing and optimization equating to significant cost savings and faster liquidity adjustment. Yet, realizing this advantage depends on *hybrid architecture*:

classical front-ends orchestrating quantum back-ends through APIs (IBM Quantum, 2025; McKinsey, 2025).

Table 8 – Comparative Performance: Classical vs Quantum Algorithms

Use Case	Classical Algorithm (Complexity)	Quantum Algorithm (Complexity)	Potential Speed-Up	Estimated Maturity
Monte Carlo Simulation	$O(1/\varepsilon^2)$	$O(1/\varepsilon)$ via Amplitude Estimation	100×	2028–2030
Portfolio Optimization	NP-hard heuristic (minutes–hours)	QAOA or VQE (seconds–minutes)	10–100×	2027–2029
Credit-Risk Modeling	Gradient boosting / deep neural networks	Quantum support-vector machines	5–20×	2030+
Option Pricing	Binomial / PDE methods	Quantum path integration	10×	2030+
Fraud Detection	ML anomaly detection	Quantum kernel methods	Qualitative improvement	2028–2032

Source: *Bank & Finance elaboration based on BIS Innovation Hub (2024); IBM (2025); OECD (2025).*

Box 9 extends the analysis beyond efficiency and profitability, showing how quantum capabilities can support sustainability and climate-related financial analysis.

Box 9 – Quantum Applications in Sustainable and Climate Finance

Climate and biodiversity risks involve vast, non-linear systems that are computationally intensive. Quantum algorithms can simulate molecular, atmospheric, and network dynamics with far greater accuracy and speed.

Applications include:

- **Energy-system optimization:** Quantum algorithms for grid balancing and renewable-energy dispatch.
- **Carbon-market modeling:** Simulating carbon-credit pricing under complex regulatory and behavioral interactions.
- **Climate-risk assessment:** Integrating satellite data and climate scenarios into portfolio stress tests using quantum machine learning.

Financial institutions could use these models to price sustainability risk more accurately and channel capital toward resilient, low-carbon assets.

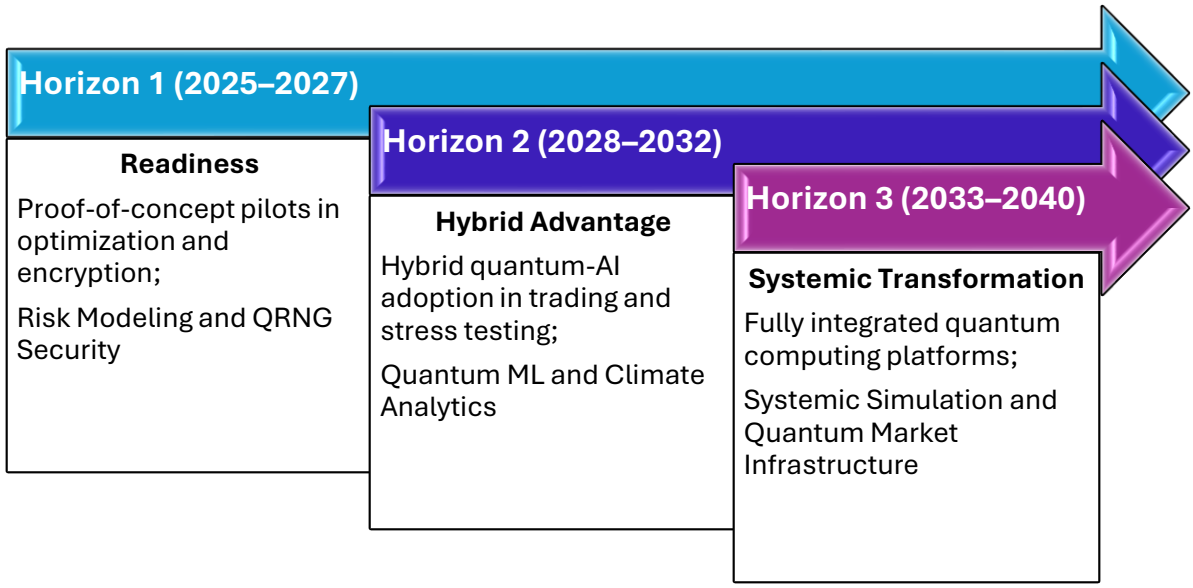
Source: *Bank & Finance elaboration based on Bank & Finance (2025g); WEF (2025); OECD (2025); BIS (2024); IBM Quantum (2025).*

Box 9 highlights how quantum innovation intersects with *climate and biodiversity finance* serving public interest. By simulating molecular and atmospheric systems, quantum computing can refine climate-risk metrics and carbon-pricing mechanisms (OECD, 2025; WEF, 2025). Beyond technical progress, this alignment reinforces a narrative of **sustainable**

competitiveness — where technological leadership and environmental stewardship converge. Financial institutions integrating these tools will move from compliance-driven ESG analysis to *physics-informed sustainability forecasting*.

Figure 12 integrates the preceding analysis into a single visualization of short-, medium-, and long-term opportunity horizons for financial institutions.

Figure 12 – Quantum Opportunity Horizon for Finance



Source: *Bank & Finance elaboration based on BIS (2024); IBM (2025); OECD (2025).*

Figure 12 shows that quantum finance will mature in waves. Early gains will come from hybrid computing and security upgrades; deeper transformation will occur when full quantum advantage emerges in the 2030s. Institutions that invest early in capacity, partnerships, and data architecture will be best positioned to lead each horizon (BIS, 2024; IBM Quantum, 2025).

Table 9 provides a step-by-step roadmap linking technology maturity to concrete institutional actions.

Table 9 – Strategic Roadmap for Quantum Adoption in Finance

Phase	Timeframe	Key Actions for Financial Institutions	Expected Outcomes
1. Exploration	2025–2027	Identify use cases; form partnerships with quantum providers; train staff; allocate R&D budgets.	Awareness and talent readiness.
2. Experimentation	2027–2029	Run pilot projects in risk modeling, optimization, and encryption; establish internal quantum labs.	Proof of concept; early performance gains.

3. Integration	2029–2033	Deploy hybrid quantum-classical solutions in production systems; develop governance standards.	Operational efficiency; risk-reduction synergy.
4. Transformation	2033–2040	Full-scale quantum computing for portfolio, market, and systemic simulation.	Strategic differentiation and competitive advantage.

Source: *Bank & Finance elaboration based on BIS (2025); OECD (2025); IBM Quantum (2025); WEF (2025).*

It shows how to transform opportunity into institutional roadmap. The sequencing—Exploration → Experimentation → Integration → Transformation—mirrors how financial institutions internalized digital and AI revolutions. Institutions that reach phase 3 before peers will define the next generation of financial leadership — where quantum capability becomes a new dimension of market competitiveness.

Central banks can catalyze progress by embedding quantum readiness into their innovation hubs, ensuring prudential benefits accompany private-sector experimentation (IMF, 2024; OECD, 2025).

Integrating Opportunity and Stability

Harnessing quantum technology for finance requires **balanced innovation governance**. Excessive caution risks technological dependency on foreign providers; reckless experimentation risks new systemic vulnerabilities. A "quantum-safe innovation framework" should therefore rest on four pillars (BIS, 2024; OECD, 2025):

1. **Security first** – all quantum applications must comply with PQC standards.
2. **Transparency** – algorithms and datasets should be auditable for bias and robustness.
3. **Collaboration** – public-private consortia should pool costs of experimentation.
4. **Sustainability** – quantum computing should prioritize energy-efficient architectures and green data centers.

Section Summary and Lessons

Section 5 reframes quantum technology as a source of systemic improvement rather than purely systemic risk. Figures 10–12, Tables 7–9, and Boxes 8–9 show that quantum capabilities can reinforce resilience by enhancing forecasting, optimization, and sustainable finance.

Three strategic messages emerge:

1. **Hybrid now, quantum later:** the decisive advantage will come from institutions mastering hybrid quantum-classical workflows before full quantum maturity.
2. **Human capital is the new frontier:** without quantum-literate analysts and supervisors, technological leadership is hollow.

3. **Public purpose and competitiveness can align:** quantum computing can power not only profit but also planetary stewardship through better climate-risk modeling.

The next section will broaden the focus from institutional strategy to global coordination, examining how **policy, regulation, and standardization** can ensure that the quantum revolution strengthens — rather than fragments — the financial system.

6. Global Coordination and Strategic Policy

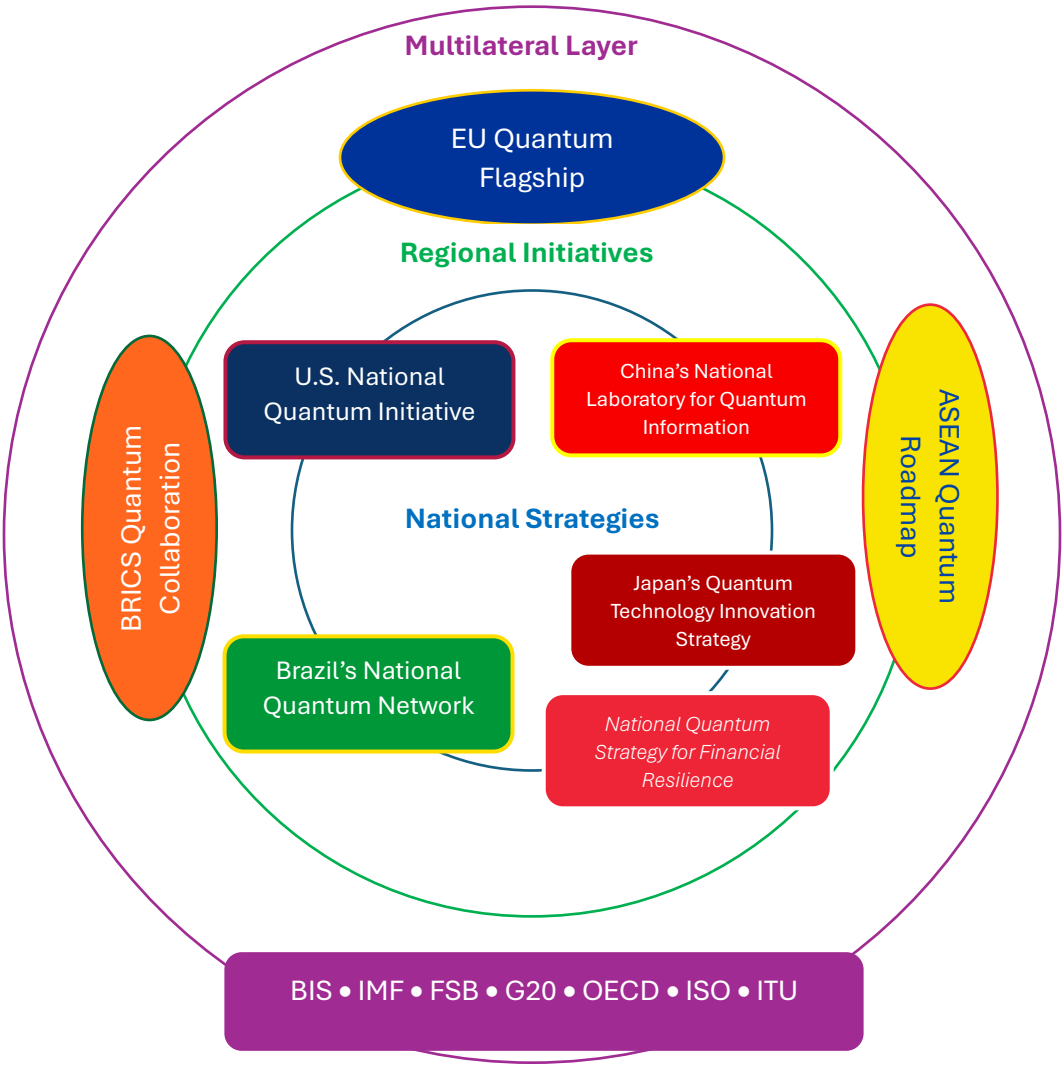
Quantum technology is rapidly becoming the **new frontier of financial geopolitics**. What began as a scientific race for computational power has evolved into a contest for **digital sovereignty**, with direct implications for global stability.

Because quantum computing threatens the encryption that underpins payments, reserves, and digital assets, its governance cannot remain confined to laboratories — it must be embedded within the multilateral financial architecture (BIS, 2024; IMF, 2024; OECD, 2025).

This section examines how global policy frameworks are adapting to quantum disruption. It maps the institutional landscape, compares national strategies, and outlines mechanisms for cooperation that could prevent a fragmented "quantum cold war" in finance.

Figure 13 situates the principal actors shaping the emerging quantum order — from multilateral bodies to regional initiatives and national strategies. It shows that quantum policy is simultaneously globalized and fragmented. There is a striking asymmetry: coordination at the scientific (regional and multilateral) level coexists with rivalry at the strategic (national) level. While scientific cooperation exists, security concerns increasingly drive technological protectionism. BIS and OECD advocate openness and standards convergence, while several major powers are developing proprietary cryptographic systems. For global finance, this raises the risk of *cryptographic balkanization* — incompatible security standards fragmenting cross-border payment networks (FSB, 2023; OECD, 2025).

Figure 13 – The Global Quantum Governance Landscape



Source: *Bank & Finance elaboration based on BIS (2024); OECD (2024); EU Commission (2025); U.S. DOE (2024).*

Table 10 compares the quantum strategies of leading economies, focusing on policy orientation, investment, and financial-sector engagement. It reveals asymmetric readiness. China and the U.S. dominate hardware and algorithmic capacity; Europe leads in regulatory harmonization; emerging economies innovate through digital-currency integration. Without convergence, these differences could translate into **regulatory fragmentation** and security asymmetry across the global financial system.

Table 10 – National Quantum Strategies and Financial Readiness

Jurisdiction	Strategic Orientation	Public Investment (2020–2025)	Financial-Sector Focus	Regulatory Coordination	Readiness Rating
United States	Security and innovation leadership	≈ USD 3 billion via NQI & NSF	PQC standardization, quantum cloud partnerships (IBM, Google, AWS)	NIST-led with Treasury and Fed oversight	★★★★☆
European Union	Standardization and resilience	≈ EUR 1.2 billion (Quantum Flagship, DORA extension)	QKD network pilots, ENISA guidelines for finance	ENISA + ECB coordination	★★★★☆
China	Strategic sovereignty and industrial dominance	> USD 10 billion	National quantum network, satellite QKD, state-bank pilots	Centralized under Ministry of Science & Technology	★★★★★
Japan	Public-private innovation ecosystem	≈ USD 1 billion	Quantum finance research consortia, fintech sandboxes	FSA + METI	★★★☆☆
Singapore	Regional hub model	≈ USD 250 million	Quantum-safe payments, MAS innovation lab	MAS-led cross-agency steering	★★★☆☆
Brazil	Emerging-market integration strategy	≈ USD 120 million	PQC integration in PIX / Drex digital-currency frameworks	MCTI + BCB	★★★☆☆

Source: *Bank & Finance elaboration based on OECD (2025); BIS (2024); EU Quantum Flagship (2025); MAS (2025); MCTI-Brazil (2024).*

Therefore, three models emerge.

1. **Security-driven leadership** — exemplified by the United States, integrating PQC standardization (via NIST) with federal R&D investment.
2. **Regulatory harmonization** — the European Union's approach, emphasizing cross-sector resilience under DORA and ENISA guidance.

3. **Technological sovereignty** — China's state-led model, prioritizing domestic production and satellite-based QKD networks (OECD, 2025; EU Commission, 2025).

Emerging economies such as Brazil and Singapore illustrate a **developmental adaptation model**, linking quantum readiness to fintech and digital-currency modernization (MCTI-Brazil, 2024; MAS, 2025).

Box 10 analyzes the geopolitical dynamics underlying quantum development and their implications for financial sovereignty.

Box 10 – The Geopolitics of Quantum Dominance

Quantum technology has become a strategic frontier comparable to nuclear energy in the mid-20th century.

Three dynamics define this emerging order:

1. **Technological Concentration:** Fewer than ten countries control 95% of global quantum-computing patents and 90% of quantum-communication infrastructure.
2. **Dual-Use Dilemma:** The same hardware that enables secure communication can also break encryption elsewhere, creating a security paradox.
3. **Financial Sovereignty:** States with domestic quantum capacity can guarantee the confidentiality of monetary operations and data flows, while others remain dependent on foreign cryptographic providers.

These dynamics are redefining alliances: quantum cooperation increasingly follows security blocs — U.S.–EU–Japan on one side; China–Russia and emerging BRICS+ on another. For the financial sector, this means that **quantum capability equals strategic autonomy**.

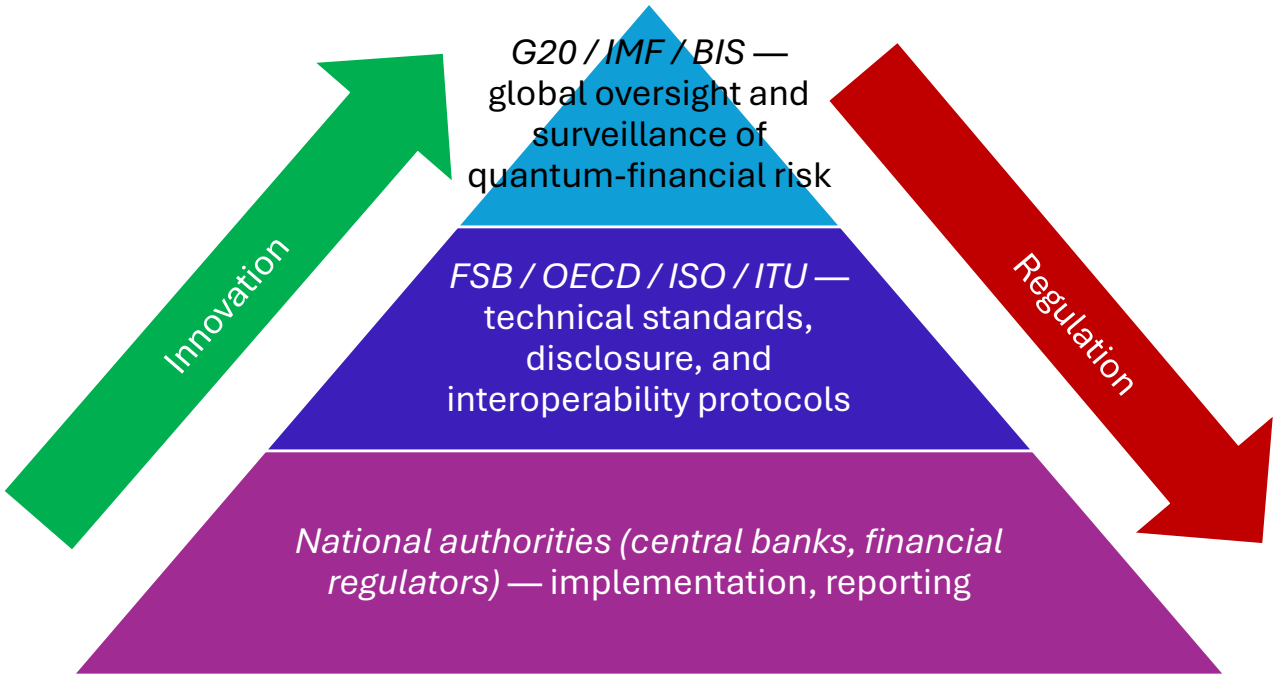
Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024); WEF (2025); OECD (2025).*

Box 10 underscores that **financial resilience and technological autonomy are converging**. Quantum capability now determines not only who sets standards, but who controls the infrastructure of global trust. Cross-border capital flows, payment networks, and CBDCs will all require quantum-safe interoperability to prevent fragmentation of global liquidity. The parallels with nuclear deterrence are imperfect but instructive: both involve dual-use technologies whose governance requires transparency and mutual restraint (Allison, 1971; BIS, 2024).

Figure 14 presents a proposed architecture for global coordination among standard-setting and financial-stability bodies. It proposes a vertical integration of governance, from technical standardization to prudential oversight. This "pyramid of coordination" ensures that algorithmic standards (bottom) align with macro-financial policy (top)) — *technologists* set the standards, *regulators* enforce them, and *international bodies* ensure consistency. Without such alignment,

local PQC choices could impede interoperability, much as divergent accounting standards once obstructed capital flows (IMF, 2024; BIS, 2024).

Figure 14 – Quantum Policy Coordination Architecture



Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); OECD (2025).*

The Multilateral Coordination Challenge

The global financial system faces a dilemma: the incentives for national innovation conflict with the collective need for interoperability. The BIS Innovation Hub, OECD Working Party on Quantum Policy, and IMF's Digital Advisory Group have begun exploratory coordination, yet no unified governance framework exists.

Historically, international financial stability has advanced through **crisis-induced cooperation**—the Basel process (1980s), the FSB (2009), the Network for Greening the Financial System (2017). The quantum era demands *pre-emptive coordination before crisis* (BIS, 2024). This would entail shared metrics (Quantum Readiness Index), synchronized standards (ISO/ETSI/NIST), and transparent peer review (Quantum-Finance Charter).

Table 11 summarizes the principal tools and policy instruments emerging from international discussions to manage quantum risk and adoption.

Table 11 – Emerging Quantum-Policy Instruments

Instrument	Objective	Responsible Institutions	Status / Examples
Quantum-Readiness Assessments (QRAs)	Evaluate national financial-system preparedness.	BIS / IMF / FSB	Under design; pilot 2026.
Global PQC Standard (ISO / ETSI)	Harmonize algorithmic standards and certification.	ISO / ETSI / NIST	Draft ISO 23837-1 expected 2026.
Quantum-Safe Financial-Messaging Protocol (QS-SWIFT)	Replace legacy RSA encryption in interbank messaging.	SWIFT / BIS Innovation Hub	Prototype 2027.
Quantum Security Disclosure Framework (QSDF)	Require public reporting of cryptographic resilience.	FSB / IOSCO / Basel Committee	Concept note 2028.
Quantum-Resilience Funding Facility (QRFF)	Support low-income economies in PQC transition.	IMF / World Bank	Proposed for 2029.

Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); IMF (2024); OECD (2025).*

Table 11 shows that quantum policy is rapidly institutionalizing. These instruments mirror the evolution of climate-finance frameworks: information disclosure, capacity-building funds, and standardized metrics. The **Quantum-Resilience Funding Facility (QRFF)**, for instance, would parallel the Green Climate Fund—addressing global public-good asymmetry by financing PQC migration in developing economies (IMF, 2024; OECD, 2025).

Box 11 outlines a conceptual proposal for a *Global Quantum-Finance Charter* that could anchor international cooperation.

Box 11 – Toward a Global Quantum-Finance Charter

A Charter could rest on five pillars:

1. **Recognition of Quantum Security as a Public Good:** Financial encryption and PQC migration to be treated as shared global-stability priorities.
2. **Commitment to Interoperability:** Signatories adopt common PQC standards and participate in cross-border testing.
3. **Transparency and Disclosure:** Regular publication of quantum-readiness metrics by financial authorities.
4. **Equitable Access:** Creation of funding windows for developing economies to access quantum infrastructure.
5. **Ethical Use and Non-Weaponization:** Prohibition of offensive use of quantum computing against global financial infrastructures.

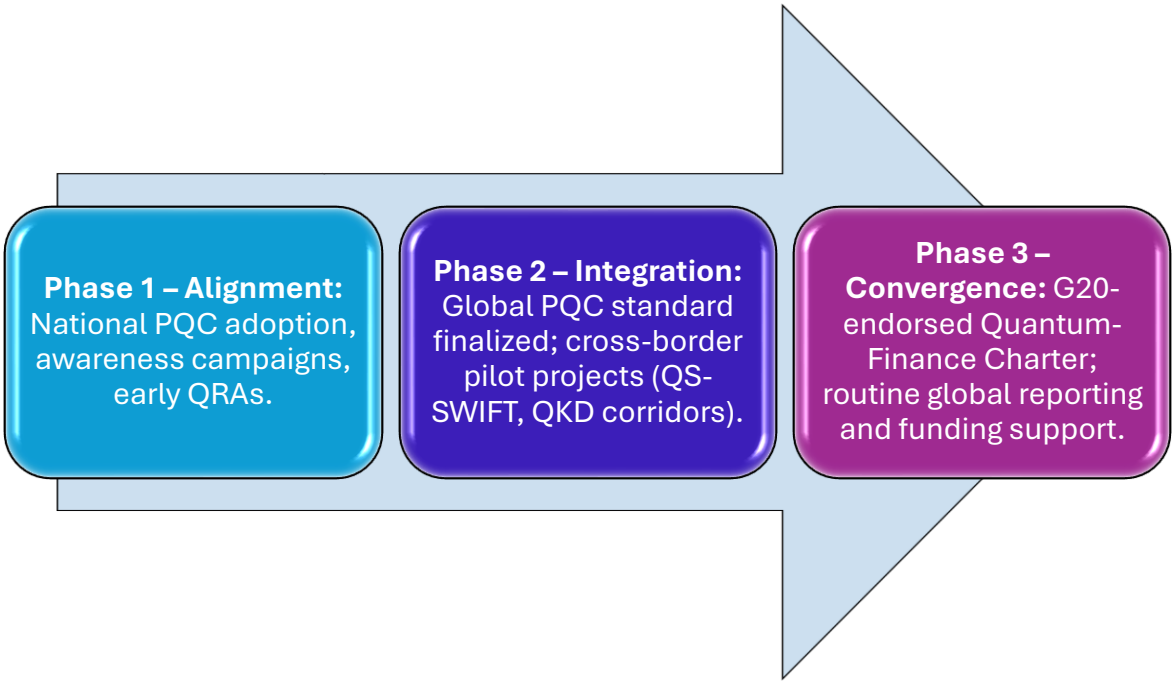
Such a charter could be ratified under the G20 or IMF framework and monitored by a *Quantum-Finance Coordination Council (QFCC)* linking central banks, supervisors, and technology agencies.

Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024); OECD (2025).*

Box 11 captures the normative dimension of quantum coordination: **financial trust must be preserved as a global commons**. A *Quantum-Finance Charter* would transform voluntary coordination into formal commitment, establishing transparency and ethical constraints. It could be annexed to the G20 agenda under the IMF's Financial Stability Mandate. Such a charter would codify quantum trust as a **shared global asset**, akin to monetary stability (BIS, 2024; IMF, 2024).

Figure 15 integrates the policy and coordination measures into a single roadmap toward a globally quantum-safe financial system.

Figure 15 – Pathways to Quantum-Safe Global Finance



Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024); OECD (2025); WEF (2025).*

The roadmap emphasizes that coordination unfolds in three phases—*Alignment*, *Integration*, and *Convergence*. This sequencing parallels the Basel Accords: initial recognition, harmonization, and then continuous peer review. The proposed *Quantum-Finance Charter* could institutionalize this cycle, establishing a permanent forum for global monitoring of algorithmic resilience (BIS, 2024; IMF, 2024).

Integrating Geopolitics, Regulation, and Market Incentives

The interplay between national security and global finance requires careful governance. Without safeguards, quantum capability could become a tool of economic coercion. Hence, coordination must integrate **geopolitical transparency mechanisms**—for instance, reciprocal audits of PQC implementations or joint simulations of quantum-decryption risk, analogous to nuclear "confidence-building measures" (Allison, 1971).

Market incentives also matter. If regulators embed quantum-readiness criteria into credit ratings or bank disclosures, private capital will align with public resilience goals. The result could be a **quantum-resilience premium**—where quantum-secure institutions enjoy lower funding costs due to superior trustworthiness (FSB, 2023; OECD, 2025).

Section Summary and Lessons

Section 6 situates the quantum transition within the broader architecture of global financial governance. Figures 13–15, Tables 10–11, and Boxes 10–11 together depict a global ecosystem that is technically dynamic but institutionally lagging.

Three strategic imperatives emerge:

1. **Synchronize innovation and supervision:** International coordination must evolve in tandem with quantum R&D to avoid fragmentation.
2. **Institutionalize cooperation:** The Quantum-Finance Charter and Quantum Readiness Assessments could become the backbone of global trust governance.
3. **Preserve inclusivity:** Developing economies need technical and financial assistance to avoid exclusion from the next cryptographic standard.

In essence, the world faces a race between **quantum progress and regulatory coherence**. If coordination prevails, quantum technology can reinforce stability; if rivalry dominates, it may fragment it.

The next section synthesizes these findings into **actionable policy recommendations**, outlining how regulators, central banks, and financial institutions can translate these insights into a coherent implementation roadmap for quantum-safe global finance.

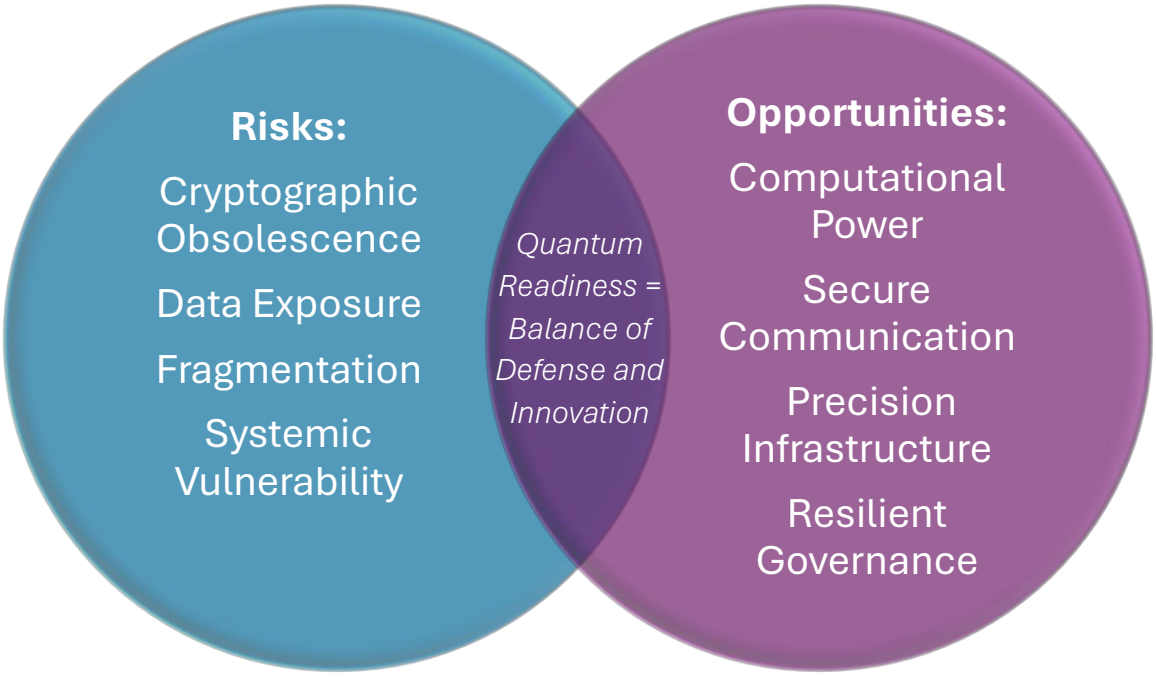
7. Conclusions and Policy Recommendations: From Quantum Threat to Quantum Readiness

Quantum technology will reshape the foundations of financial stability and trust. Its rise completes a technological trilogy—after digitalization and artificial intelligence—pushing finance into an era where **computation itself becomes a source of systemic risk and resilience**. The challenge is not whether quantum disruption will arrive, but whether financial authorities can guide its arrival in a way that strengthens, rather than fragments, global stability (BIS, 2024; IMF, 2024).

This section synthesizes the report's core findings, translating them into a sequence of policy actions for central banks, regulators, and financial institutions. It also articulates the long-term vision: a *quantum-safe global financial ecosystem* that balances innovation, inclusion, and security.

Figure 16 encapsulates the report's overarching message—quantum technology is both the sharpest threat and the greatest opportunity in finance's modern history. It highlights the essence of the quantum challenge: *the same algorithms that endanger financial security can also enhance it*. The policy priority is therefore not to resist quantum development but to **govern its trajectory**, ensuring that quantum capability strengthens rather than destabilizes the financial system.

Figure 16 – The Dual Nature of Quantum Technology in Finance



Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); OECD (2025).*

Quantum's duality resembles that of nuclear energy: a technology capable of destruction or progress depending on governance. In financial terms, this means the same algorithms that can break encryption can also model and mitigate systemic risk. The key variable is **institutional readiness**—the ability to manage technological power through coordination, prudence, and foresight (OECD, 2025; BIS, 2024).

Table 12 consolidates the cross-layer findings of the report, linking risks, opportunities, and policy levers within the Bank & Finance Five-Layer Ecosystem Framework. The table shows that quantum disruption traverses all ecosystem layers. The **Information Layer** demands PQC migration; the **Infrastructure Layer** calls for quantum-secure payments; the **Innovation Layer** invites hybrid quantum-AI modeling; the **Integration Layer** requires interoperability standards; and the **Governance Layer** must embed coordination within the BIS–IMF–G20 nexus. Resilience therefore depends on synchronizing micro-level upgrades with macro-level oversight—a challenge analogous to aligning prudential capital reforms across borders after Basel III (Goodhart, 2011).

Table 12 – Summary of Key Findings Across Layers

Ecosystem Layer	Quantum Risk	Quantum Opportunity	Policy Response
Information	Cryptographic collapse, data exposure	Quantum-secure communication (QKD), PQC	Mandatory PQC migration plans; encryption audits.
Infrastructure	Payment-system vulnerability, time desynchronization	Quantum sensing for timing accuracy	Integrate quantum timing into RTGS and satellite systems.
Innovation	Competitive asymmetry, algorithmic opacity	Quantum-AI integration for analytics	Create regulatory sandboxes for quantum financial computing.
Integration	Cross-border fragmentation	Global PQC standards, interoperability frameworks	BIS/FSB-led Quantum-Readiness Assessments.
Governance	Technological divide, geopolitical risk	Global coordination and equitable access	Establish a Quantum-Finance Charter under G20/IMF.

Source: *Bank & Finance elaboration based on BIS (2024); IMF (2024); OECD (2025).*

Box 12 distills the guiding principles that should anchor regulatory and institutional responses to quantum disruption. It translates analysis into normative guidance. These six principles—precaution, proportionality, transparency, collaboration, equity, and learning—should form the backbone of emerging *quantum-prudential policy*. They mirror the logic that underpinned earlier transformations: capital adequacy in the 1980s, cyber resilience in the 2010s, and now cryptographic integrity in the 2030s (FSB, 2023; BIS, 2024).

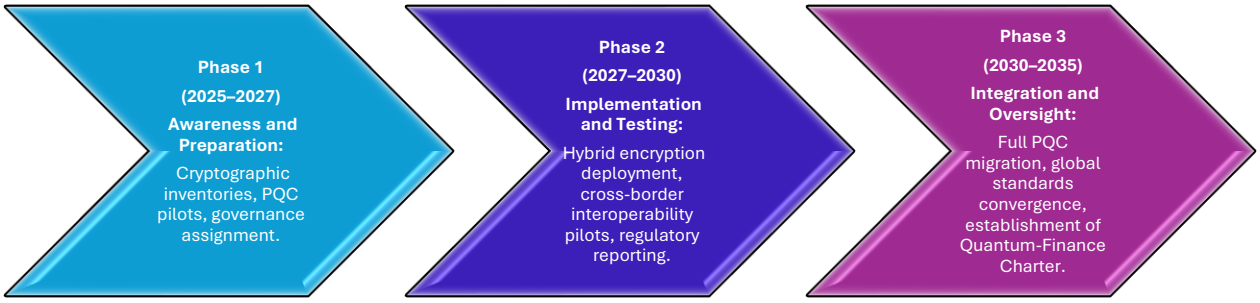
Box 12 – Core Policy Principles for a Quantum-Safe Financial System

1. **Precautionary Preparedness:** Begin PQC migration before quantum computers reach decryption capability; treat cryptographic risk as a prudential concern.
2. **Proportional Adaptation:** Tailor requirements to systemic importance — higher standards for systemically important banks, FMIs, and central-bank infrastructures.
3. **Transparency and Accountability:** Mandate public disclosure of quantum-readiness metrics within operational-risk reporting.
4. **Collaboration and Standardization:** Promote interoperability through ISO, ETSI, and BIS frameworks; establish shared testing environments.
5. **Equitable Access:** Support emerging economies with funding and technical assistance for PQC adoption.
6. **Continuous Learning:** Institutionalize quantum drills, research partnerships, and adaptive supervision as part of an evolving resilience culture.

Source: *Bank & Finance elaboration based on BIS (2024); FSB (2023); IMF (2024).*

Figure 17 outlines the sequential roadmap guiding the quantum transition from initial risk identification to mature governance coordination.

Figure 17 – Roadmap for Quantum Transition in Global Finance



Source: Bank & Finance elaboration based on BIS (2024); IMF (2024); OECD (2025).

Figure 17 visualizes the decadal horizon of transformation: *Phase 1 (2025–2027)*—Awareness and Inventory; *Phase 2 (2027–2030)*—Implementation and Testing; *Phase 3 (2030–2035)*—Integration and Oversight. The roadmap implies that quantum readiness must become part of **national financial-stability strategies** and IMF Article IV surveillance by the early 2030s (IMF, 2024). Delay risks creating a "cryptographic sudden stop"—a discontinuity in digital trust akin to liquidity freezes in past crises (BIS, 2024).

Table 13 details actionable recommendations tailored to the four primary stakeholder groups in the financial ecosystem.

Table 13 – Policy Recommendations by Stakeholder

Stakeholder	Recommended Actions	Expected Outcome
Central Banks & Regulators	Conduct Quantum-Readiness Assessments (QRAs); integrate cryptographic integrity into financial-stability monitoring; establish PQC compliance deadlines.	Strengthened systemic resilience and supervisory foresight.
Financial Market Infrastructures (FMIs)	Transition messaging and settlement systems to hybrid PQC; coordinate with SWIFT and ISO 20022 updates.	Secure and interoperable payment ecosystems.
Commercial Banks & Institutions	Implement hybrid PQC solutions; train staff; disclose readiness metrics; engage in joint R&D consortia.	Reduced operational risk; improved investor confidence.
International Organizations	Develop global PQC and QKD standards; fund emerging-market adoption via IMF/WB facilities.	Harmonized global framework and inclusive participation.

Source: Bank & Finance elaboration based on BIS (2024); FSB (2023); OECD (2025).

Table 13 provides the operational bridge between principle and practice by distinguishing responsibilities across the ecosystem. Each actor has distinct but complementary responsibilities: supervisors ensure discipline; infrastructures implement safeguards; and multilateral institutions guarantee cohesion. This distributed model ensures redundancy—if one tier lags, others maintain systemic resilience (OECD, 2025; FSB, 2023). The key success factor is feedback: continuous peer review through *Quantum-Readiness Assessments (QRAs)*.

Box 13 draws historical parallels with the previous decade's cyber-resilience transformation to extract lessons for the quantum era.

Box 13 – Lessons from the Cyber-Resilience Transition

The transition from IT security to cyber resilience (2015–2025) offers valuable precedents:

- **From Awareness to Regulation:** Cybersecurity moved from technical departments to supervisory frameworks (e.g., DORA, NIS2, CPMI-IOSCO guidance).
- **From Fragmentation to Harmonization:** Global coordination through the FSB Cyber Lexicon and resilience testing reduced inconsistencies.
- **From Compliance to Capability:** Institutions learned that resilience depends on culture, not only controls.

Applying these lessons to quantum:

- Start coordination early to prevent "patchwork protection."
- Embed quantum risk within prudential oversight before crises occur.
- Invest in capacity building and information-sharing communities.

Source: *Bank & Finance elaboration based on FSB (2023); ENISA (2024); BIS (2024).*

The cyber-resilience experience proves that **institutional learning is cumulative**. It took a decade for cybersecurity to evolve from IT to boardroom priority; the quantum era must compress that learning into half the time. Joint drills, cross-border exercises, and harmonized reporting templates can accelerate this institutional diffusion (ENISA, 2025; ECB, 2025).

As illustrated earlier in **Figure 9**, quantum resilience rests on a layered and interdependent architecture. At its foundation lies **information integrity** — the deployment of post-quantum cryptography (PQC) standards, quantum-key distribution (QKD), and continuous cryptographic auditing to secure the raw fabric of trust. Surrounding this is **infrastructural security**, where quantum-timing synchronization, secure payment networks, and resilient messaging systems preserve the precision and reliability of settlement. The **innovation layer** harnesses Quantum-AI convergence, regulatory sandboxes, and applied R&D funding to turn computational breakthroughs into supervisory strength rather than systemic risk. **Integration through standards** ensures that advances remain interoperable across sectors and borders, preventing regulatory and technological fragmentation. Finally, **governance through coordination** —

anchored in BIS, IMF, FSB, G20, and ISO frameworks — binds these layers into a coherent global system.

Stability in the quantum era will depend on the **coherence of this architecture**: each layer must reinforce the others in a self-supporting continuum of trust. Fragmentation at any level — technical, institutional, or geopolitical — would propagate fragility through the entire structure. Technological hardening and institutional adaptation must therefore progress in tandem with multilateral policy alignment. Without this vertical integration, the world risks a new **quantum divide**, in which a few economies achieve algorithmic sovereignty while others remain dependent on foreign cryptographic infrastructure (BIS, 2024; IMF, 2024; OECD, 2025). The next decade will determine whether quantum power becomes a foundation for shared resilience or a frontier of financial inequality.

Toward a Quantum-Safe Financial Order

The transition to quantum-safe finance is both a **technological imperative and a moral responsibility**. Trust—the currency of financial systems—can no longer rely on the obsolescence of mathematical attacks; it must rest on continual renewal of cryptographic and institutional design.

To operationalize this transition, Bank & Finance proposes three integrated policy tracks:

1. Prudential Integration
    a. Treat quantum risk as a financial-stability concern.
    b. Mandate PQC migration plans within Basel III operational-risk frameworks.
    c. Include encryption-integrity indicators in IMF FSAPs.

2. Global Standardization
    a. Institutionalize common PQC and QKD protocols.
    b. Formalize the *Quantum-Finance Charter* under the G20/IMF.
    c. Create an ISO 23837-based certification for financial infrastructures.

3. Inclusive Capacity Building
    a. Ensure all jurisdictions can afford the transition.
    b. Operationalize the *Quantum-Resilience Funding Facility (QRFF)*.
    c. Launch a *Quantum Readiness Fellowship* for supervisors and technologists from developing economies.

From Capital to Cryptography

Financial history shows that every era of innovation demands a new prudential paradigm. The 1980s addressed **capital adequacy**; the 2010s focused on **cyber resilience**; the 2020s must now secure **cryptographic integrity**. The common lesson is that stability hinges on institutional

cooperation, not technical perfection (Goodhart & Schoenmaker, 2016). Quantum technology will not eliminate uncertainty—but it can help model and manage it, provided governance keeps pace.

Section Summary and Final Takeaways

Section 7 closes the analytical loop: quantum technology is not an external shock but an endogenous phase of financial evolution. Managing it requires a paradigm shift from *defensive risk control* to *strategic trust architecture*.

Key takeaways:

1. Quantum risk is systemic and time-sensitive — delay increases exposure geometrically.
2. Quantum resilience is multi-layered — aligning technology, governance, and global policy.
3. Quantum opportunity is transformative — enabling new frontiers of predictive analytics and sustainable finance.
4. Global coordination is indispensable — digital trust is a collective good that no nation can secure alone.

The next frontier is implementation: embedding quantum resilience into supervisory frameworks, stress-testing tools, and educational curricula. As Bank & Finance concludes, **quantum readiness will become the defining prudential capability of the 2030s**—the cornerstone of a financial system built not only on capital and code, but on collective foresight.

8. References

Allison, G. (1971) *Essence of Decision: Explaining the Cuban Missile Crisis.* Boston: Little, Brown.

Arute, F. et al. (2019) "Quantum Supremacy Using a Programmable Superconducting Processor." *Nature*, 574(7779).

Bank & Finance (2025a). *The Value of Truth: Information Integrity in Global Finance.* Bank & Finance Deep-Dive Series Report No. 1.

Bank & Finance (2025b). *Cyber Resilience in Finance: From Risk Mitigation to Competitive Advantage.* Bank & Finance Deep-Dive Series Report No. 3.

Bank & Finance (2025c). *The Future of Payments and Cross-Border Finance: Navigating Transformation Amid Risk and Opportunity.* Bank & Finance Deep-Dive Series Report No. 6.

Bank & Finance (2025d). *Unveiling the Future of Digital Currency Infrastructure: Navigating the Transformation of Finance in a Tokenized World.* Bank & Finance Deep-Dive Series Report No. 7.

Bank & Finance (2025e). *Open Finance: Unleashing the Next Wave of Financial Innovation.* Bank & Finance Deep-Dive Series Report No. 10.

Bank & Finance (2025f). *Artificial Intelligence: Investment Implications and Strategic Outlook 2025–2030*. Bank & Finance Deep-Dive Series Report No. 11.

Bank & Finance (2025g). *Climate Change and Financial Risks: Navigating the Transition and Managing Physical Exposure*. Bank & Finance Deep-Dive Series Report No. 13.

Bank & Finance (2025h). *Financial Geopolitics and Global Fragmentation*. Bank & Finance Deep-Dive Series Report No. 17.

Bank & Finance (2025i). *Navigating the Global Financial Ecosystem: Risks, Opportunities, and a Five-Layer Architecture*. Bank & Finance Deep-Dive Series Report No. 20.

Bank for International Settlements (BIS) (2024) *Quantum Technologies and the Future of Financial Stability*. Basel.

Bank for International Settlements – Innovation Hub (BISIH) (2024) *Quantum Readiness for Financial Systems*. Basel.

Bank for International Settlements – Innovation Hub (BISIH) (2025) *Quantum-Safe Payment Messaging Prototype*. Basel.

Bennett, C.H. & Brassard, G. (1984) "Quantum Cryptography: Public-Key Distribution and Coin Tossing." *Proceedings of the IEEE Conference on Computers, Systems and Signal Processing*, Bangalore.

BBVA (2024) *Quantum Algorithms for Portfolio Optimization*. Madrid.

European Central Bank (ECB) (2025) *Quantum Technologies in Financial Infrastructure*. Frankfurt.

European Commission (2025) *EU Quantum Flagship Progress Report*. Brussels.

European Space Agency (ESA) (2024) *Quantum Communications and Satellite Security*. Paris.

European Union Agency for Cybersecurity (ENISA) (2024) *Cybersecurity Guidance for Financial Services under DORA*. Athens.

European Union Agency for Cybersecurity (ENISA) (2025) *Guidelines for Quantum-Safe Financial Systems under DORA*. Athens.

ETSI (2024) *GS QSC 010/011: Quantum-Safe Cryptography—Implementation Guidance*. Sophia Antipolis.

Farhi, E., Goldstone, J. & Gutmann, S. (2014) "A Quantum Approximate Optimization Algorithm." *arXiv:1411.4028*.

Feynman, R. (1982) "Simulating Physics with Computers." *International Journal of Theoretical Physics*, 21(6/7), 467–488.

Financial Stability Board (FSB) (2023) *Enhancing Cyber and Quantum Resilience in the Financial Sector*. Basel.

Gidney, C. & Ekerå, M. (2021) "How to Factor 2048-bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits." *Quantum*, 5, 433.

Goldman Sachs (2024) *Quantum Computing for Derivatives and Risk—Pilot Findings*. New York.

Goodhart, C. (2011) *The Basel Committee on Banking Supervision: A History of the Early Years 1974–1997*. Cambridge University Press.

Goodhart, C. & Schoenmaker, D. (2016) *The Boundaries of the Banking System*. Financial Markets Group, LSE.

Google Quantum AI (2025) *Quantum Computing Applications in Finance*. Mountain View, CA.

IBM Quantum (2025) *Quantum Advantage in Financial Services*. Armonk, NY.

International Monetary Fund (IMF) (2024) *Quantum Readiness and Financial Stability: Emerging Issues*. Washington, DC.

International Organization for Standardization (ISO) (2024) *ISO/IEC 14888-4: Information Security—Digital Signatures with Appendix*. Geneva.

International Organization for Standardization (ISO) (2025) *ISO/IEC 23837 (Draft): Quantum-Resistant Cryptography—Implementation Guidelines*. Geneva.

International Telecommunication Union (ITU) (2024) *ITU-T X.QKD Series: Quantum Key Distribution Networks and Interoperability*. Geneva.

J.P. Morgan (2024) *Exploring Quantum Computing for Risk and Portfolio Optimization*. New York.

Massachusetts Institute of Technology (MIT) (2024) *Quantum Information Science and Financial Applications*. Cambridge, MA.

Monetary Authority of Singapore (MAS) (2025) *National Quantum Strategy for Financial Resilience*. Singapore.

Ministry of Science, Technology and Innovation of Brazil (MCTI) (2024) *National Quantum Strategy*. Brasília.

McKinsey & Company (2025) *Quantum Computing in Financial Services*. New York.

Mosca, M. (2022) "Timeframes for Quantum Threats to Cryptographic Systems." *Communications of the ACM*, 65(11).

National Institute of Standards and Technology (NIST) (2024) *Post-Quantum Cryptography Standards (NISTIR 8413)*. Gaithersburg, MD.

National Security Agency (NSA) (2024) *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) and PQC Guidance*. Fort Meade, MD.

Organisation for Economic Co-operation and Development (OECD) (2024) *Quantum Technologies and Economic Security*. Paris.

Organisation for Economic Co-operation and Development (OECD) (2025) *Quantum Technology Governance and Global Standards*. Paris.

Preskill, J. (2018) "Quantum Computing in the NISQ Era and Beyond." *Quantum*, 2, 79.

Shor, P.W. (1994) "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*.

U.S. Department of Energy (DOE) (2024) *Quantum Information Science and Technology Programs—Roadmap Update*. Washington, DC.

Weick, K. & Sutcliffe, K. (2011) *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Jossey-Bass, San Francisco.

World Economic Forum (WEF) (2025) *Quantum Economy 2030: Governance and Inclusion*. Geneva.

9. Appendices

Appendix A – Glossary of Quantum and Cryptographic Terms

This glossary summarizes the technical and institutional concepts used throughout the report, serving as a reference for policymakers, supervisors, and financial practitioners unfamiliar with quantum terminology.

Term	Definition and Financial Relevance
Amplitude Estimation	Quantum algorithm that accelerates Monte Carlo simulations by estimating probabilities quadratically faster than classical methods — used in risk modeling and option pricing.
BB84 Protocol	The first practical quantum key distribution (QKD) protocol (Bennett & Brassard, 1984), enabling provably secure communication; basis for quantum-safe payments.
CRYSTALS-Kyber / CRYSTALS-Dilithium	Post-quantum cryptographic algorithms standardized by NIST (2024) for key exchange and digital signatures; recommended replacements for RSA/ECC in financial systems.
Entanglement	Quantum phenomenon linking particles such that their states remain correlated; foundation of quantum communication and sensing.
Grover's Algorithm	Quantum algorithm offering quadratic speed-up for unstructured search problems — may accelerate financial data mining and fraud detection.
Hybrid Encryption	Security architecture combining classical and post-quantum algorithms; ensures backward compatibility during PQC transition.
Learning With Errors (LWE)	Hard mathematical problem underlying most lattice-based PQC schemes; foundation for CRYSTALS-Kyber and Dilithium.
Quantum Advantage	Demonstrated performance edge where a quantum computer solves a problem faster than the best classical algorithm — key benchmark for financial innovation.
Quantum Key Distribution (QKD)	Technique using quantum mechanics to securely exchange encryption keys; interception is detectable, making it ideal for central-bank and cross-border data links.
Quantum Random Number Generator (QRNG)	Device that uses quantum phenomena to produce truly random numbers; enhances security in financial authentication and tokenization.
Quantum Supremacy	Milestone demonstrating that a quantum processor can perform a computation infeasible for any classical computer (Arute et al., 2019).
Shor's Algorithm	Quantum algorithm capable of factoring large numbers exponentially faster than classical algorithms — the principal threat to RSA/ECC encryption (Shor, 1994).
Superposition	Property of qubits allowing simultaneous representation of 0 and 1; foundation of quantum parallelism and computational power.
Variational Quantum Algorithms (VQE/QAOA)	Hybrid algorithms leveraging quantum circuits for optimization and simulation; used in portfolio optimization and derivative pricing pilots.

Source: *Bank & Finance elaboration based on NIST (2024); BIS (2024); OECD (2025); IBM Quantum (2025).*

Appendix B – Key Standards and Protocols for Quantum Security

This appendix consolidates the emerging technical and institutional frameworks guiding the post-quantum transition.

Table A1 – Key Quantum-Security Standards and Protocols

Standard / Framework	Issuing Body	Scope and Relevance for Finance	Status (as of 2025)
NIST PQC Suite (CRYSTALS-Kyber, Dilithium, SPHINCS+)	U.S. National Institute of Standards and Technology	Defines official post-quantum algorithms for government and commercial use; de facto benchmark for global PQC migration.	Finalized (2024)
ISO/IEC 23837 Series – PQC Implementation Guidelines	International Organization for Standardization	Specifies conformity and testing for quantum-resistant algorithms; crucial for interoperability across borders.	Draft (expected 2026)
ETSI GS QSC 010/011	European Telecommunications Standards Institute	Technical guidelines for hybrid encryption and key management in critical infrastructure, including finance.	Released (2024)
BIS-FSB Quantum-Readiness Framework	Bank for International Settlements & Financial Stability Board	Establishes supervisory expectations for PQC migration and stress-testing integration.	Consultation draft (2025)
ENISA Quantum Security Guidance under DORA	European Union Agency for Cybersecurity	Operational guidance for integrating PQC into financial infrastructures and digital-identity systems.	Published (2025)
ITU-T X.QKD Series	International Telecommunication Union	Standards for QKD networks and interoperability; essential for cross-border payment channels.	Released (2024)
IMF Quantum-Readiness Index (QRI)	International Monetary Fund	Composite metric for assessing national financial preparedness for quantum transition.	Pilot phase (2026)

Sources: *Bank & Finance elaboration based on BIS (2024); NIST (2024); ISO (2025); ETSI (2024); IMF (2024); OECD (2025).*

These frameworks collectively define the emerging **"quantum regulatory perimeter."** Financial authorities should align domestic rules with NIST, ISO, and BIS standards to maintain cross-border trust and interoperability.

The alignment of these frameworks will determine the coherence of global quantum security. Financial authorities should prioritize participation in **NIST, ISO, ETSI, BIS, and IMF processes** to ensure interoperability between domestic standards and multilateral initiatives.

Appendix C – Country Quantum-Readiness Matrix

The Quantum-Readiness Matrix assesses governance, R&D capacity, financial-sector integration, and international coordination. Ratings (1–5) are based on publicly available strategies, institutional capacity, and engagement in global standards (BIS, 2024; OECD, 2025).

Table A2 – Country Quantum-Readiness Matrix

Country / Region	Governance Framework	R&D Capacity	Financial-Sector Integration	International Coordination	Readiness (1–5)
United States	NQI Act, NIST PQC Program	Very High	Advanced pilots (Fed, JPM, Goldman)	Strong (BIS, OECD, ISO)	5
European Union	DORA, ENISA, ECB coordination	High	Early QKD and PQC testing	Strong (EU Quantum Flagship)	4
China	MoST-led centralized policy	Very High	Active QKD pilots in state banks	Moderate (BRICS, SCO)	5
Japan	FSA–METI joint strategy	High	Fintech consortium pilots	High	4
Singapore	MAS Quantum Initiative	Medium–High	PQC in payment systems	High (ASEAN)	4
Brazil	MCTI–BCB coordination	Moderate	PQC in Pix/Drex projects	Medium	3
India	National Mission on Quantum Tech	Moderate	Bank pilots in research phase	Medium	3
Africa (select economies)	Nascent frameworks	Low	Limited pilots	Low	2

Sources: *BIS (2024); OECD (2025); IMF (2024); ENISA (2025); MCTI-Brazil (2024).*

Quantum capability and governance remain concentrated in advanced economies. Emerging markets demonstrate creativity but lack resources. Without targeted support through IMF and World Bank programs, a "quantum readiness divide" may widen global digital inequality. Bridging this gap requires technical assistance and financial support mechanisms, such as the proposed *Quantum-Resilience Funding Facility (QRFF)*.

Appendix D – Quantum Stress-Testing Template for Financial Institutions

This appendix provides a template for integrating quantum-related vulnerabilities into institutional and system-wide stress tests. It is intended as a practical starting point for central banks, supervisory authorities, and FMIs.

Table A3 – Quantum Stress-Testing Template

Stress-Test Dimension	Scenario Description	Key Metrics	Data Sources	Time Horizon	Supervisory Relevance
Cryptographic Exposure	Compromise of RSA/ECC algorithms before PQC migration completion.	% of systems using legacy encryption; data archived under risk.	IT and vendor inventories.	Short term (1–3 yrs)	Prioritize PQC adoption plans.
Operational Disruption	Quantum decryption of interbank credentials causes message spoofing and payment halts.	Failed transaction ratio; recovery time.	RTGS data; payment logs.	Immediate (days–weeks)	Test crisis-response and redundancy.
Market Confidence Shock	Revelation of large-scale quantum breach leads to liquidity flight.	CDS spreads; equity declines; digital-outflow ratios.	Market and sentiment data.	Medium term (weeks–months)	Gauge systemic contagion risk.
Cross-Border Fragmentation	Asynchronous PQC adoption disrupts settlement interoperability.	Settlement lag times; failed cross-border payments.	SWIFT, CLS, ISO 20022 data.	Medium–long term (1–5 yrs)	Coordinate international standardization.

Sources: *BIS (2024); FSB (2023); IMF (2024).*

Stress-Test Dimension	Scenario Description	Key Metrics	Data Sources	Time Horizon	Supervisory Relevance
Cryptographic Exposure	Compromise of RSA/ECC algorithms before PQC migration completion.	% of systems using legacy encryption; data archived under risk.	IT and vendor inventories.	Short term (1–3 yrs)	Prioritize PQC adoption plans.
Operational Disruption	Quantum decryption of interbank credentials causes message spoofing and payment halts.	Failed transaction ratio; recovery time.	RTGS data; payment logs.	Immediate (days–weeks)	Test crisis-response and redundancy.
Market Confidence Shock	Revelation of large-scale quantum breach leads to liquidity flight.	CDS spreads; equity declines; digital-outflow ratios.	Market and sentiment data.	Medium term (weeks–months)	Gauge systemic contagion risk.
Cross-Border Fragmentation	Asynchronous PQC adoption disrupts settlement interoperability.	Settlement lag times; failed cross-border payments.	SWIFT, CLS, ISO 20022 data.	Medium–long term (1–5 yrs)	Coordinate international standardization.

This template operationalizes *quantum macroprudential testing*. It allows supervisors to assess systemic exposure and cross-jurisdictional contagion, supporting inclusion in the BIS–IMF Financial Sector Assessment Program (FSAP) cycle by 2027.

Appendix E. Source–Exhibit Matrix

This appendix provides a consolidated mapping of all figures, tables, and boxes in the report to their primary sources.

I. Figures

No.	Figure Title	Primary Sources
1	Key Highlights of the Report	BIS (2024); FSB (2023); OECD (2025)
2	Report Roadmap	BIS (2024); IMF (2024)
3	The Quantum Technology Landscape	BIS (2024); OECD (2024); WEF (2025); NIST (2024)
4	Timeline of Quantum Readiness for Finance	NIST (2024); BIS (2024); OECD (2025); WEF (2025)

5	Quantum Threat Map for Global Finance	BIS (2024); FSB (2023); NIST (2024); ENISA (2025)
6	Timeline of Quantum Threat Emergence	BIS (2024); FSB (2023); NIST (2024); OECD (2025); ENISA (2025)
7	Layers of Quantum Resilience in Finance	BIS (2024); NIST (2024); FSB (2023); OECD (2024)
8	The Quantum-Safe Transition Framework	BIS (2024); IMF (2024); OECD (2025)
9	Five-Layer Governance Framework for Quantum-Safe Finance	Bank & Finance (2025i); BIS (2024); IMF (2024)
10	Quantum Value Chain in Financial Services	BIS Innovation Hub (2025); IBM Quantum (2025); WEF (2025); OECD (2025)
11	Quantum-AI Convergence: The Next Frontier	BIS (2025); IBM (2025); MIT (2025); WEF (2025)
12	Quantum Opportunity Horizon for Finance	BIS (2024); IBM (2025); OECD (2025)
13	The Global Quantum Governance Landscape	BIS (2024); OECD (2024); EU Commission (2025); U.S. DOE (2024)
14	Quantum Policy Coordination Architecture	BIS (2024); FSB (2023); OECD (2025)
15	Pathways to Quantum-Safe Global Finance	BIS (2024); IMF (2024); OECD (2025); WEF (2025)
16	The Dual Nature of Quantum Technology in Finance	BIS (2024); FSB (2023); OECD (2025)
17	Roadmap for Quantum Transition in Global Finance	BIS (2024); IMF (2024); OECD (2025)

II. Tables

No.	Table Title	Primary Sources
1	Five Layers of Quantum Impact in the Financial Ecosystem	Bank & Finance (2025i); BIS (2024); IMF (2024); OECD (2024); WEF (2025)
2	Core Quantum Technologies and Their Relevance to Finance	BIS (2024); OECD (2024); FSB (2023); ESA (2024)
3	Financial Systems at Risk from Quantum Decryption	NIST (2024); NSA (2024); BIS (2024); OECD (2024)
4	Illustrative Stress Scenario: Quantum Breach of Global Payments	FSB (2023); IMF (2024); BIS (2024)
5	Post-Quantum Cryptography (PQC) Algorithms and Financial Suitability	NIST (2024); ISO/IEC 14888-4 (2024); ETSI (2024)
6	Institutional Quantum Resilience Checklist	FSB (2023); BIS (2024); NIST (2024)
7	Quantum Use Cases Across the Financial Ecosystem	BIS (2024); IMF (2024); IBM Quantum (2025); McKinsey (2025)
8	Comparative Performance: Classical vs Quantum Algorithms	BIS Innovation Hub (2024); IBM (2025); OECD (2025)

9	Strategic Roadmap for Quantum Adoption in Finance	BIS (2025); OECD (2025); IBM Quantum (2025); WEF (2025)
10	National Quantum Strategies and Financial Readiness	OECD (2025); BIS (2024); EU Quantum Flagship (2025); MAS (2025); MCTI-Brazil (2024)
11	Emerging Quantum-Policy Instruments	BIS (2024); FSB (2023); IMF (2024); OECD (2025)
12	Summary of Key Findings Across Layers	BIS (2024); IMF (2024); OECD (2025)
13	Policy Recommendations by Stakeholder	BIS (2024); FSB (2023); OECD (2025)
A1	Key Quantum-Security Standards and Protocols	BIS (2024); NIST (2024); ISO (2025); ETSI (2024); IMF (2024); OECD (2025)
A2	Country Quantum-Readiness Matrix	BIS (2024); OECD (2025)

III. Boxes

No.	Box Title	Primary Sources
1	From Cyber Resilience to Quantum Resilience	Bank & Finance (2025b); FSB (2023); BIS (2024); ENISA (2024); NIST (2024)
2	Quantum Principles in Plain Language	NIST (2024); IBM (2025); MIT (2024)
3	Financial Institutions on the Quantum Frontier	Bank & Finance (2025f); BIS Innovation Hub (2024); IBM Quantum (2025); JP Morgan (2024); MAS (2025)
4	Harvest Now, Decrypt Later: The Invisible Countdown	ENISA (2025); NIST (2024); FSB (2023)
5	Quantum Risk Transmission Channels	FSB (2023); BIS (2024); ECB (2025)
6	From Awareness to Action: The Post-Quantum Imperative	NIST (2024); FSB (2023); BIS (2024); ECB (2025)
7	Case Study: National Quantum-Safe Initiatives	NIST (2024); ENISA (2025); OECD (2025); MCTI-Brazil (2024); MAS (2025)
8	Quantum Computing in Financial Modeling	IBM Quantum (2025); BIS Innovation Hub (2024); BBVA (2024); Goldman Sachs (2024)
9	Quantum Applications in Sustainable and Climate Finance	Bank & Finance (2025g); WEF (2025); OECD (2025); BIS (2024); IBM Quantum (2025)
10	The Geopolitics of Quantum Dominance	BIS (2024); IMF (2024); WEF (2025); OECD (2025)
11	Toward a Global Quantum-Finance Charter	BIS (2024); IMF (2024); OECD (2025)
12	Core Policy Principles for a Quantum-Safe Financial System	BIS (2024); FSB (2023); IMF (2024)
13	Lessons from the Cyber-Resilience Transition	FSB (2023); ENISA (2024); BIS (2024)