OXFORD JOURNAL
OF STUDENT
SCHOLARSHIP

Role of Quantum Cryptography in the Financial Sector: How is the World Preparing for a New Era of Computing?

Hamsini Mopuru
hamsinimopuru@gmail.com

ABSTRACT

Quantum computing is advancing rapidly and is expected to reshape the cybersecurity foundations of the financial sector. Modern financial systems rely heavily on classical public-key cryptography such as Rivest-Shamir-Adleman (RSA) and elliptic-curve cryptography (ECC), which are vulnerable to quantum algorithms capable of breaking current encryption schemes. As these technologies mature, financial institutions face growing pressure to transition toward quantum-resistant security frameworks that can preserve the confidentiality and integrity of financial data.

This paper reviews the role of quantum cryptography in finance and describes how governments, regulators, and financial institutions are preparing for the transition to quantum-resilient security systems. Drawing on academic literature, institutional reports, and organizational case studies, the analysis explores the technical, regulatory, and economic factors shaping the adoption of post-quantum security measures across global financial networks. Particular attention is given to hybrid security strategies that combine post-quantum cryptography (PQC) with quantum key distribution (QKD), which are emerging as practical solutions for strengthening communication security while maintaining operational performance.

The findings highlight substantial disparities in national and institutional readiness, with higher-income countries and large financial organizations leading pilot programs and infrastructure investments while lower-capacity systems remain dependent on legacy encryption. These differences create uneven levels of protection across interconnected financial networks and increase the risk of systemic vulnerability. The paper concludes that coordinated standards, phased implementation strategies, and sustained investment in technical capacity will be essential for maintaining secure and stable financial systems in the quantum era.

1. INTRODUCTION

Quantum cryptography is a method of securing communication by using the principles of quantum mechanics, rather than relying on classical computing systems based on mathematical hardness assumptions. As quantum computing capabilities advance, this topic has become increasingly relevant for sectors that depend on durable confidentiality, including financial services.

Unlike classical encryption, which can theoretically be broken given enough computational power, quantum cryptography derives its security from quantum-mechanical principles that can make eavesdropping detectable under ideal protocol assumptions. This distinction between classical and quantum security has significant implications for financial systems [1]. Financial models depend on the reliability and confidentiality of data flows that drive trading algorithms, pricing strategies, and real-time risk assessments. If classical encryption is compromised by quantum computing, the integrity of these models could be undermined, leading to both financial loss and systemic instability. By deriving security from fundamental quantum-mechanical principles, quantum cryptography can help strengthen long-term protection for the key exchange used to secure market data and transactions, even against future computational breakthroughs. This ensures secure communication channels and supports the reliability of financial models by protecting data integrity and preventing adversarial interference, which in turn contributes to more stable and trustworthy predictive outcomes [2, 3].

A key reason this shift matters, across various applications, including finance, is that current security infrastructures still depend heavily on public-key encryption methods such as Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC). These schemes derive their security from mathematical problems that are difficult for classical computers, but they become vulnerable under sufficiently capable quantum computation. As an example, a quantum algorithm known as Shor's algorithm poses a major risk because it can efficiently factor large integers and compute discrete logarithms, which are the core assumptions that underpin RSA and ECC, respectively.

These potential impacts of quantum cryptography on the financial sector highlight why long-term, quantum-based security has become increasingly valuable. As quantum computers advance, the appeal of quantum cryptography has grown, especially for applications that demand long-term confidentiality and resistance to future attacks [3, 4].

This review synthesizes the literature on financial applications in quantum cryptography, direct reports from financial organizations, and documents from (inter)governmental organizations to frame quantum-era cybersecurity as both a technical migration problem and a coordination problem. It links specific failure modes in current financial cryptography to the main remedies now discussed as feasible near- and mid-term responses. This includes standardization efforts that rely on what is known as post-quantum cryptography (PQC, described in Section 4.1.) and hybrid approaches that use a method known as quantum key distribution (QKD, described in Section 4.1.) for key exchange while retaining classical systems for scalable encryption. It then uses national readiness disparities to show why "quantum resilience" is unevenly distributed, with early-moving jurisdictions and central banks piloting

quantum-safe channels while lower-capacity systems remain exposed through legacy infrastructure and limited regulatory guidance. Next, the report situates these choices in a global standards environment where interoperability incentives pull many G7/NATO actors toward National Institute of Standards and Technology (NIST)-aligned PQC and European Telecommunications Standards Institute/International Telecommunication Union (ETSI/ITU) efforts, while BRICS priorities (notably China's infrastructure-led approach) point toward more sovereign, potentially divergent QKD trajectories that could complicate cross-border financial connectivity. Finally, company case studies later in the paper provide applied evidence of how this transition is unfolding in practice, contrasting live QKD/PQC pilots and crypto-agile backbones (e.g., JPMorgan and HSBC) with institutions emphasizing planning, internal testing, and advisory-led readiness pathways. Overall, the report evaluates quantum security in finance as an emerging transition in which technical feasibility, institutional readiness, and geopolitical standard-setting jointly shape adoption outcomes.

2. QUANTUM FINANCE

Quantum computing is relevant to finance because it creates cybersecurity risks while also offering potential applications in portfolio optimization, stock prediction, derivatives pricing, and risk analysis [1]. These applications help explain why financial institutions are preparing for quantum technologies on two fronts: adopting potential computational benefits and protecting cryptographic systems from quantum-enabled attacks. Because quantum computers could, in principle, be exceptional at factoring large numbers and certain complex mathematical computations, quantum systems are highly relevant in finance; some future prospects extend to quantum cryptography, blockchain, and quantum money. Nevertheless, any early applications are expected in noisy intermediate-scale quantum (NISQ) devices before fault-tolerant quantum computers become available [5]. In practice, this means that near-term quantum applications in finance are likely to focus on exploratory, hybrid quantum–classical use cases on NISQ devices, rather than transformative breakthroughs, until fault-tolerant quantum computers with stable error correction become available [5].

Quantum computing shows promise in portfolio optimization, risk modeling, fraud detection, and pricing strategies through methods such as quantum annealing, quantum machine learning, and amplitude estimation [5]. One example of this is portfolio optimization framed as a quantum annealing problem, where the portfolio objective is encoded so that the best allocation corresponds to the lowest-energy solution. Orús and colleagues (2019) point to demonstrations on D-Wave Systems that incorporate expected returns, risk terms, transaction costs, and constraints in a single optimization [5]. Another example is the use of Principal Component Analysis (PCA), which can be implemented classically, and its quantum analogue, quantum PCA, to extract dominant factors from large covariance or correlation matrices; while classical PCA is sufficient for many applications, quantum PCA is theoretically advantageous in handling extremely high-dimensional datasets by leveraging quantum state preparation and logarithmic scaling in matrix size, thereby accelerating factor extraction in settings where classical computation becomes prohibitive.

Despite the promising capabilities, the maturity of quantum hardware remains limited, requiring hybrid strategies and cautious implementation. These applications often rely on early-stage quantum systems and hybrid approaches that combine quantum hardware with classical computing. Most financial institutions remain in the conceptual stage of quantum adoption, conducting small-scale pilots in risk modeling, portfolio optimization, and fraud detection [6]. In response to these early-stage limitations, frameworks such as the Responsible Quantum Readiness Levels (RQRL) emphasize ethical and sustainable quantum integration. Institutions like the International Monetary Fund (IMF) and central banks (France, Germany, Singapore, Italy, Brazil, and Canada) are experimenting with quantum-safe pilots, recognizing that uncoordinated readiness across borders could create systemic risks [3, 7].

This creates a central tension for financial institutions: the same quantum capabilities that may improve financial decision-making for one organization can also strengthen the potential cyberattack capabilities of an adversary. For example, a bank could benefit from quantum optimization by using quantum or hybrid quantum-classical methods to test portfolio-allocation models, derivatives-pricing routines, or large-scale risk simulations more efficiently [5]. However, those gains would arrive alongside new security pressures because sufficiently powerful quantum computers could use algorithms such as Shor's algorithm to undermine RSA- or ECC-based authentication and encryption. As a result, the institution may gain computational advantages in modeling and optimization, while also needing to prepare for the possibility that the broader quantum transition could expose customer data, transaction records, and interbank communications secured under vulnerable public-key systems [3, 4]. A similar pattern appeared after the 2016 Bangladesh Bank cyberattack, when attackers exploited weaknesses in the bank's payment environment to send fraudulent SWIFT transfer requests, showing how faster digital financial infrastructure can also create new cybersecurity risks [8]. In this sense, quantum finance creates both an innovation opportunity and a security transition, requiring firms to modernize their cryptographic infrastructure while exploring quantum-enabled financial applications.

3. EFFECT OF QUANTUM TECHNOLOGY ON THE FINANCIAL SECTOR

The intersection of quantum cryptography and finance lies in this tension: quantum technologies offer tools to advance financial systems, but also pose serious threats to the cryptographic foundations that those systems rely on. Since digital finance expands across borders, securing sensitive information has become a global concern for banks, governments, and individuals alike. Thus, the financial sector is highly exposed to quantum-enabled decryption risks due to the sensitivity of financial data and the vulnerability of some current encryption techniques. From mobile banking to interbank transfers, modern finance is built on cryptographic systems that were not designed to withstand quantum attacks. As quantum computers grow more powerful, the encryption used in banking, digital payments, and financial data storage may no longer be secure. This raises the possibility that encrypted data being transmitted or stored today could be intercepted and later decrypted once quantum machines are powerful enough.

This risk should be understood as primarily prospective rather than immediate. Most current financial systems are not facing a near-term collapse of encryption from quantum computers, since large-scale fault-tolerant machines capable of breaking widely deployed public-key systems have not yet arrived. The

more pressing concern is long-term exposure through "harvest now, decrypt later" attacks, where adversaries collect encrypted financial records, payment data, or confidential communications today and wait until future quantum capabilities make decryption possible [3]. This risk is already reflected in intelligence practice, as declassified NSA procedures allow certain encrypted communications collected under Section 702 to be retained for as long as they remain useful for cryptanalysis or deciphering, showing that encrypted data can be stored even before it is readable [9].

This long-term risk is especially relevant for asymmetric encryption systems such as RSA and ECC. Shor's algorithm can, in principle, efficiently factor integers and solve discrete logarithms, undermining the hardness assumptions that secure these schemes; a point discussed further in the Shor's Algorithm section [3, 4]. To combat this issue, many regulatory frameworks, such as the EU's Digital Operational Resilience Act (DORA), are initiating programs to encourage the early adoption of post-quantum cryptography (PQC) even before fully mature quantum computers exist [7]. These programs typically involve assessing cryptographic dependencies, piloting quantum-resilient algorithms, and developing phased transition roadmaps to ensure interoperability. Accordingly, financial resilience depends on technological innovation, anticipatory regulation, and early preparation by governments and financial institutions.

In response to these emerging challenges, financial institutions and regulators are beginning to adapt their security strategies and plan for quantum-resistant protections.

4. QUANTUM CRYPTOGRAPHY: CURRENT WEAKNESSES AND SOLUTIONS

As quantum technologies move from theory toward deployment, cryptographic security is increasingly shaped by the tension between mathematical guarantees and real-world implementation limits. Quantum cryptography emerges in this context as both a response to future computational threats and a framework constrained by present-day infrastructure, cost, and scalability. Understanding its role therefore requires examining how quantum protocols behave under practical conditions, how they interact with classical systems already embedded in financial networks, and how emerging quantum algorithms reshape the threat landscape. Taken together, these considerations frame quantum cryptography not as a singular solution, but as part of a layered transition toward security models capable of withstanding long-term quantum risks.

4.1 Integrating QKD with Classical Encryption Methods: Advanced Encryption Standard

Within this response landscape, the most widely studied approach in quantum cryptography is quantum key distribution (QKD). Table 1 presents several properties of QKD, which relates its application to practical scenarios.

Features	Quantum Key Distribution (QKD)	Post-Quantum Cryptography (PQC)
Quantum Vulnerability	Secure Key Exchange (Resistant under ideal protocol assumptions)	Designed to be resistant
Security Basis	Physics-based (quantum mechanics)	Math-based (hard, quantum-resistant problems)
Hardware	Specialized quantum	Classical computers/networks
Key Functionality	Secure key exchange (primarily)	Encryption, signatures, key exchange
Authentication Provided	Requires external authentication	Yes (via Public Key Infrastructure/Signatures)
Security Guarantee	Information-Theoretic Security (Key Exchange)	Computational Security
Implementation	Requires special hardware	Usually software-only
Communications Media	Typically requires optical fiber or free-space optical links	Compatible with any type of communications media
Cost	Higher cost (hardware)	Lower cost (software)
Repeater Compatibility	Possible with quantum-specific processing (quantum-to-classical-to-quantum; which creates interception risk)	Compatible with current classical repeater technology
Mobile Device Compatibility	Very limited; could only be used with line-of-sight nodes	Compatible with existing classical communications networks
Digital Signature Compatibility	Not suited for digital signatures; requires separate classical/PQC signature for authentication	Supports quantum-safe digital signatures; NIST-selected schemes already standardized
Primary Use	Secure key exchange between two parties	Replace classical public key encryption/signatures
Infrastructure Needs	Fiber optic or satellite links for quantum signal transport	Standard IT networks (no new physical infrastructure)
Deployment Scalability	Limited to point-to-point links	More scalable across networks

Features	Quantum Key Distribution (QKD)	Post-Quantum Cryptography (PQC)
Quantum Vulnerability	Secure Key Exchange (Resistant under ideal protocol assumptions)	Designed to be resistant
Security Basis	Physics-based (quantum mechanics)	Math-based (hard, quantum-resistant problems)
Maturity Level	Emerging (proven in pilots, but not yet fully deployed)	Standardized, with deployment still ongoing
Ideal Applications	Military, national defense, financial clearinghouses	General enterprise, cloud, communications, IoT
Time to Deploy	Over 3-7 years for full infrastructure	About 1-3 years for phased rollout

Table 1. Comparative characteristics of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) across security, infrastructure, cost, scalability, and deployment factors.

QKD enables two parties to share a secret encryption key in a way that makes eavesdropping detectable. Some common eavesdropping strategies include: intercept-resend, in which attackers measure the quantum signal and then transmit a replacement to the receiver; beamsplitter attacks, where they use a beamsplitter to divert part of the signal while allowing the remainder to pass undetected; trojan horse attacks, in which hidden light is sent into the system to extract information about secret settings or keys; and multiphoton attacks, where they exploit pulses containing multiple photons by capturing one photon and letting the others proceed without interference [10].

The comparison in Table 1 shows that PQC and QKD are complementary rather than interchangeable. PQC is designed to replace vulnerable public-key algorithms used for encryption, signatures, and key exchange, while QKD mainly provides a secure method for distributing symmetric keys. Because QKD does not independently solve authentication, financial institutions would still need classical or post-quantum authentication methods to verify the communicating parties. These differences suggest that PQC is likely to become the scalable baseline for quantum-safe financial security because it can be phased into existing software, protocols, and classical network infrastructure. QKD, by contrast, is better suited for high-value links, such as interbank, central-bank, or data center connections, where the additional requirements for implementation can be justified. Even where QKD strengthens key exchange, large-scale adoption remains difficult in financial systems that require speed, interoperability, and broad network coverage [10].

Despite the implied robustness of QKD in detecting eavesdropping, real-world systems can still be vulnerable to implementation flaws and side-channel attacks. QKD systems are also vulnerable to other

types of attacks that do not currently exist with classical computing. This makes the practical value of QKD an area of ongoing debate.

One key QKD protocol, BB84, demonstrates how quantum states of light can be used to securely exchange cryptographic keys, making it a foundational element of quantum-secure communication systems. Another core protocol is Eckert's entanglement-based scheme (E91) that uses entangled photon pairs to generate a secure encryption key, with its security guaranteed by the laws of quantum mechanics that make any eavesdropping attempt detectable by disturbing the photons' correlations [10]. Despite theoretical security, practical implementations face issues such as photon loss, imperfect detectors, and multiphoton vulnerabilities. Experimental QKD systems rely on weak laser pulses or entangled photon pairs transmitted through optical fibers or free-space channels, but they remain limited in distance and cost efficiency. Quantum principles like the no-cloning theorem make eavesdropping detectable, though real-world implementations still face challenges.

Studies on online banking security have shown that the combination of QKD and Advanced Encryption Standard (AES) can protect against common threats such as phishing, man-in-the-middle, and replay attacks [11]. By using QKD to establish encryption keys through quantum channels and AES for high-speed data encryption, this hybrid model leverages the strengths of both technologies: the theoretically strong security of quantum key exchange under ideal assumptions and the efficiency of classical symmetric encryption. This layered approach can strengthen the key distribution phase by making certain forms of interception detectable under ideal QKD assumptions, while AES continues to provide fast and scalable protection for financial transactions. Such hybrid systems are particularly valuable in banking, where security must not compromise speed, reliability, or compliance requirements, making them a realistic transitional solution as the industry prepares for the post-quantum era.

The integration method has been tested primarily in controlled or central-bank pilot environments, suggesting that widespread adoption would require substantial investment in communication infrastructure and regulatory alignment.

For the financial sector, hybrid systems like QKD+AES offer a path to quantum-safe communication without entirely abandoning the classical cryptographic frameworks.

4.2. Shor's and Grover's Algorithms

The most direct threats to current cryptographic systems come from two quantum algorithms: Shor's and Grover's. Shor's algorithm, developed in the 1990s, allows quantum computers to factor large integers exponentially faster than classical computers, effectively breaking public-key systems such as RSA and ECC. The workflow shown in Figure 1 illustrates how the algorithm alternates between classical computation and a quantum period-finding routine before returning to classical verification steps to determine the prime factors of the input number.

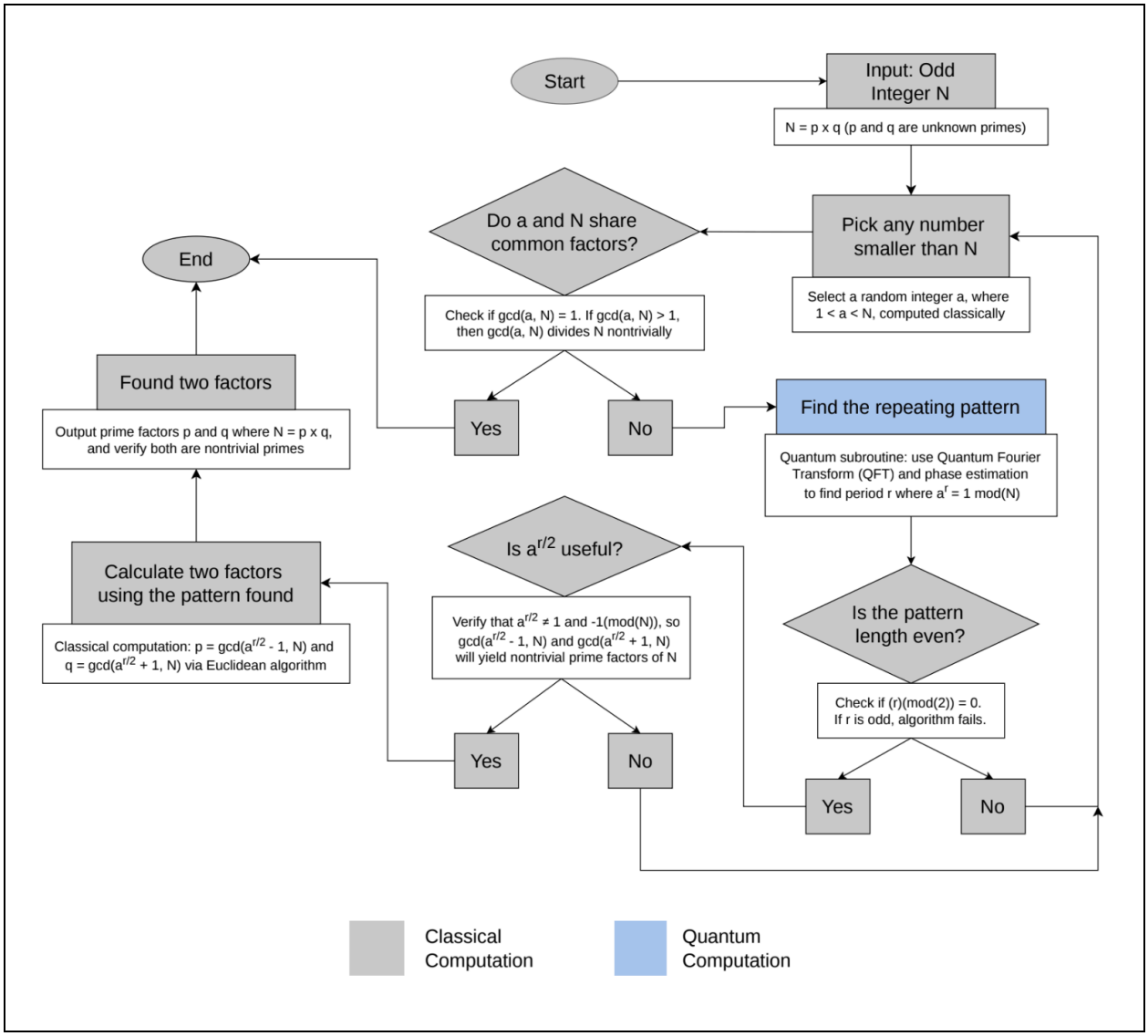

Figure 1. Workflow of Shor's algorithm for integer factorization. The diagram illustrates the hybrid computational structure of the algorithm, combining classical preprocessing with a quantum period-finding routine to efficiently determine the prime factors of large integers [12].

Grover's algorithm, while less powerful, can still weaken symmetric encryption by providing a quadratic speedup in brute-force searches. Figure 2 depicts the iterative structure of the algorithm, where repeated cycles of oracle evaluation and probability amplification increase the likelihood of identifying the target item before measurement.

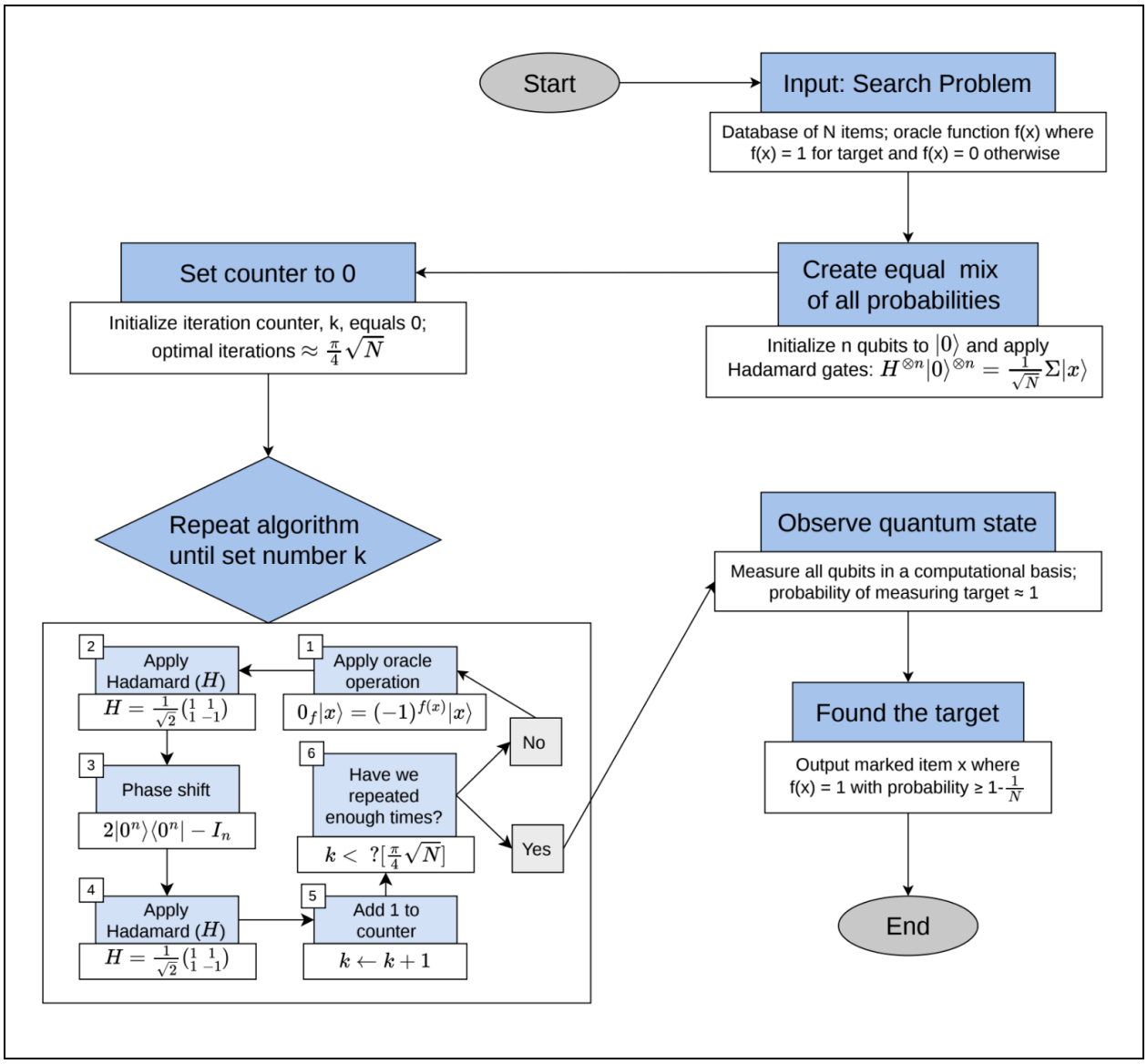

Figure 2. Iterative search process of Grover's algorithm demonstrating amplitude amplification used to identify a target item within an unsorted dataset [13].

From a design standpoint, the cryptographic impact of these algorithms stems from their ability to change computational complexity rather than exploit implementation flaws. Shor's algorithm directly compromises the mathematical foundations of public-key encryption, whereas Grover's algorithm reduces the effective security margin of symmetric systems without eliminating their viability. This difference arises from their underlying architectures: Shor's use of quantum period-finding and interference enables exponential speedup for structured mathematical problems, while Grover's amplitude amplification provides only a quadratic improvement for unstructured searches. As a result, the design of each algorithm determines the scale of disruption it poses to existing cryptographic systems. While Grover's algorithm provides a quadratic speedup, effectively reducing an n-bit system key to about n/2 bits of

security, Shor's algorithm threatens widely used public-key systems such as RSA and ECC. In response, Post-Quantum Cryptography (PQC, Table 1) seeks to replace existing cryptographic primitives with mainly lattice-based, code-based, hash-based, or multivariate systems; each designed to resist known quantum attacks. Although symmetric encryption can be reinforced by doubling key sizes, asymmetric systems will need complete replacement once practical quantum computers are available, marking one of the most significant cryptographic transitions in modern digital history. For financial institutions, this transition carries systemic implications because the security of payment systems, infrastructure, regulatory reporting, and cross-border trust frameworks depends on the replacement of quantum-vulnerable cryptography.

However, a robust cybersecurity strategy might have to rely on the complementary strengths of PQC and QKD. As gathered from Table 1, PQC is software-based, easy to deploy across networks, and could be suitable for broad enterprise use. By comparison, QKD provides physics-based security for key exchange by making eavesdropping detectable, but it also requires specialized quantum hardware, optical communications channels, and significant infrastructure investment.

4.3. Vulnerabilities and Systemic Exposure in Financial Cryptography

Mobile and online banking represent some of the most exposed components of the financial ecosystem, largely because they rely on cryptographic mechanisms that were not designed to withstand quantum-enabled attacks. Many current systems depend on RSA- or ECC-based authentication, while passwords and one-time passcodes remain vulnerable to phishing, credential theft, and implementation weaknesses. These weaknesses are not isolated to user-facing applications, but extend across the broader financial infrastructure that supports digital transactions, data storage, and interbank communication.

Quantum threats significantly amplify these existing vulnerabilities. Future quantum machines could undermine the encryption protocols that currently secure financial interactions, particularly through the use of algorithms such as Shor's, which directly target public-key cryptography. One of the most serious risks is the possibility that adversaries can intercept encrypted financial data today and decrypt it later once sufficiently powerful quantum computers become available. This "harvest now, decrypt later" strategy poses a substantial threat to the financial sector because much of its data, including transaction histories, settlement records, and contractual agreements, retains long-term value and sensitivity [2, 3]. As a result, communications that are considered secure under current standards could be exposed years after transmission, creating lasting consequences for financial stability and trust.

These risks are further compounded by the interconnected structure of modern financial systems. Banks, payment processors, clearinghouses, cloud providers, and cross-border messaging networks often depend on shared authentication, encryption, and data-exchange protocols. Research by Poledna and colleagues shows that indirect exposures through overlapping portfolios can transmit systemic risk across financial institutions, and that measuring only direct interbank connections may underestimate total systemic risk by as much as 50% [14]. In a cryptographic context, this means that a weakness in one part of the network could affect confidence in other connected institutions, even if the initial vulnerability is limited. For example, if a financial institution continues to rely on quantum-vulnerable public-key systems for

archived transaction records or interbank communications, adversaries may have incentives to collect encrypted data now and attempt to decrypt it later when quantum capabilities improve [2, 3]. The concern is therefore less that quantum attacks would automatically cause financial instability, and more that widely used vulnerable cryptography could increase systemic risk over time if migration to quantum-resistant protections remains uneven across the sector.

As mentioned earlier, from a solutions perspective, research suggests that hybrid quantum-classical approaches, such as combining quantum key distribution with classical authentication and encryption methods, could mitigate some of these risks by strengthening key exchange and improving detection of interception attempts [2, 11]. However, implementation remains limited, often restricted to well-funded or central-bank institutions with access to specialized infrastructure. This uneven readiness highlights a growing divide between financial systems that are preparing for quantum-secure cryptography and those that may struggle to adapt.

Within the context of quantum cryptography, these vulnerabilities underscore the need for proactive security measures that address both immediate infrastructural weaknesses and long-term quantum threats. Safeguarding the financial system in the quantum era will therefore require coordinated policy efforts and international alignment to ensure that quantum-resistant solutions are adopted consistently across global financial networks.

5. GLOBAL IMPLICATIONS OF QUANTUM FINANCE

5.1. Disparities in Post-Quantum Cryptography Implementation

While technological innovation in quantum computing continues to accelerate, the global readiness to implement post-quantum cryptography (PQC) remains highly uneven, as suggested by nations' investments in quantum technology (Figure 3A). This disparity in preparedness has significant implications for international finance, as asymmetric adoption of PQC creates weak links that can compromise even the most secure networks.

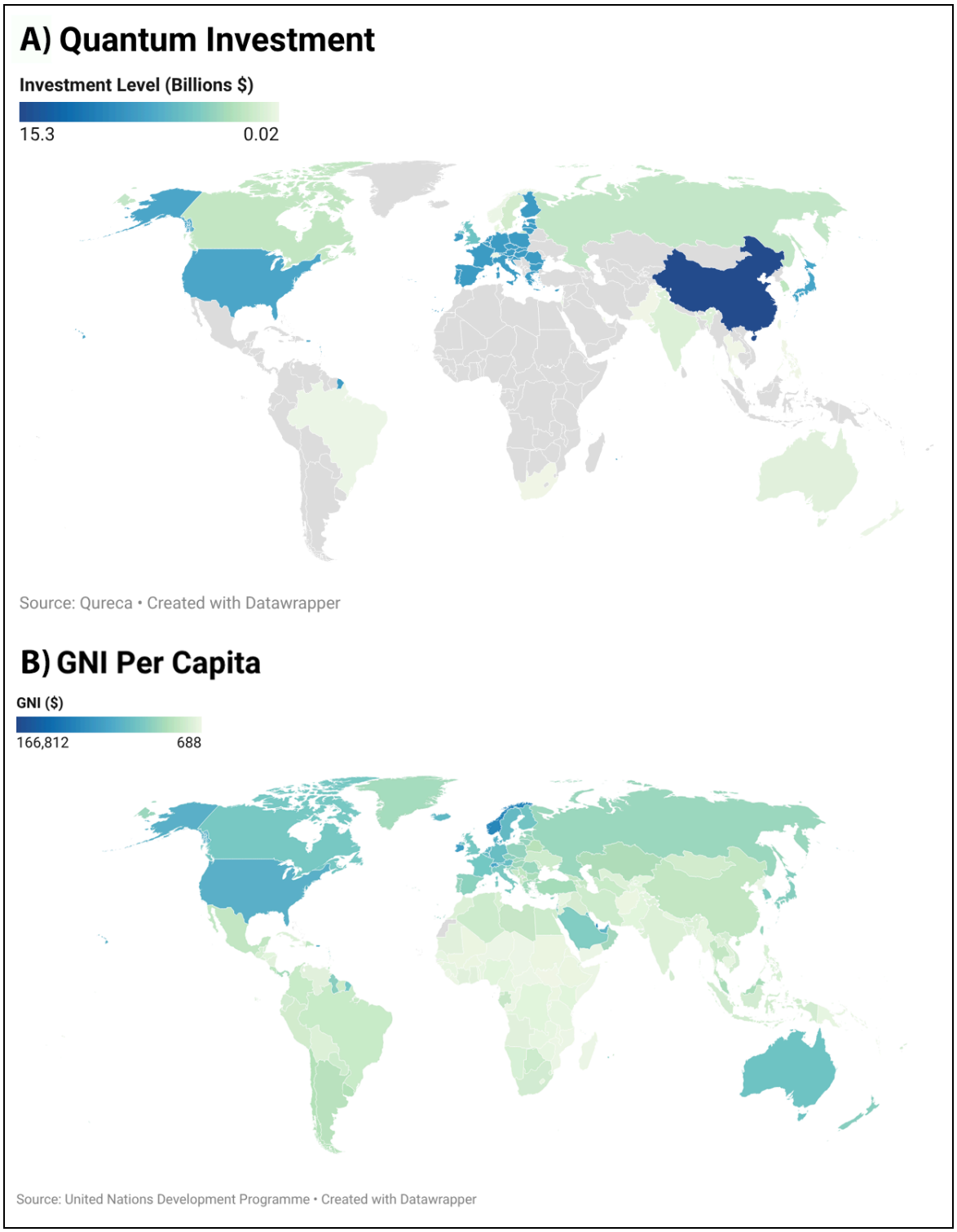

Figure 3. A) Global distribution of national investment in quantum technologies measured in billions of U.S. dollars. Higher investment levels are concentrated in technologically advanced economies such as the United States, China, and Western European countries. Data from [15]. B) Global distribution of

Gross National Income (GNI) per capita across countries, illustrating regional differences in economic capacity. Data from [16]. Gray shaded regions indicate areas for which no data was found.

A number of countries have taken early, proactive steps. For example, the European Union (EU) has embedded quantum security concerns into its financial regulatory agenda through the Digital Operational Resilience Act (DORA), which encourages early adoption of PQC standards and aims to protect critical financial infrastructure from cryptographic breaks [7]. Similarly, Singapore, Germany, France, Italy, Brazil, and Canada have begun pilot projects through their central banks, focusing on deploying quantum-safe communication channels and testing migration pathways for financial institutions [3]. These initiatives are often paired with government-backed investments in research and development, partnerships with private sector innovators, and participation in international standardization efforts such as those led by NIST.

In contrast, many countries lack comparable resources, regulatory clarity, or technical capacity. Financial systems in these regions often rely on outdated encryption infrastructure and lack formalized national strategies for quantum readiness. In some cases, governments have yet to issue guidance on PQC migration, leaving private institutions uncertain about when, or how, to act. Others may face economic and technical barriers that limit their ability to invest in large-scale cryptographic transitions, particularly those involving infrastructure-level upgrades [2, 3]. These implementation barriers are closely connected to broader economic capacity. Countries with higher GNI often have larger public research budgets, stronger university and industry research ecosystems, more developed cybersecurity markets, and more advanced digital infrastructure [16]. These conditions can make it easier to fund quantum-security research, participate in standards development, train specialized workers, and begin testing quantum-resistant systems. Lower-capacity countries, by contrast, may face competing budget priorities, shortages of trained cryptographers and quantum-security specialists, continued dependence on legacy systems, and limited regulatory guidance [2, 3]. Education systems can deepen these constraints, as a study in Ecuador found that cybersecurity education in the country remained mostly elementary and that universities faced structural barriers in developing the specialized training needed to support national cyber capacity [17]. As a result, the challenge is not simply awareness of quantum risk, but the institutional capacity to inventory cryptographic assets, coordinate vendors, and replace vulnerable public-key systems across financial networks.

This uneven pace of PQC adoption is closely tied to a nation's economic capacity, measured through gross national income (GNI) per capita (Figure 3B), and technological maturity. A comparison of national quantum investment patterns and income levels reveals a consistent geographic overlap (Figure 3A and B). Countries with the highest levels of quantum investment, including the United States, China, and several Western European states, also fall within the higher ranges of gross national income per capita, while regions with lower income levels show more limited investment activity (Figure 3A and B). This pattern matters because quantum cryptography readiness depends on adjacent forms of capacity, rather than direct quantum funding alone. For PQC migration, that capacity includes a cryptographic inventory, dependency maps showing where public-key algorithms are embedded in software, hardware, network

protocols, certificates, and third-party services, and testing environments to determine which systems should be replaced first without disrupting financial operations [18].

These resource differences make large-scale cryptographic transitions more feasible for wealthier countries because they can modernize infrastructure, integrate PQC standards into national strategies, and support private-sector adoption through subsidies, regulatory clarity, and public-private partnerships. Lower-income countries may face a slower transition when limited cybersecurity budgets, legacy systems, and workforce gaps delay implementation. This wealth-readiness correlation could deepen existing global inequities because nations with more resources may secure their financial systems sooner and strengthen their competitive positions, while lower-capacity countries could face prolonged vulnerability if quantum-vulnerable cryptography remains widely used [2, 3]. At the same time, lower income alone does not automatically make a country a major target. A lower-GNI country with limited integration into high-value digital financial networks may be less visible to quantum cryptographic threats, while a lower-readiness country with active cross-border payment, remittance, or correspondent-banking links could become more attractive because its systems connect to valuable financial flows. The income distribution illustrated in the data shows clear regional concentration. High per-capita income levels are clustered in North America, Western Europe, and parts of East Asia, while lower-income ranges are visible across much of Africa and South Asia (Figure 3B). Moreover, disparities in readiness could deepen geopolitical and economic divides. Countries able to secure their digital assets early may enjoy greater investor confidence, lower systemic risk, and more stable capital flows. Those lagging behind could face heightened exposure, regulatory pressure from international markets, and potential exclusion from secure financial networks. Over time, this could result in further fragmentation of the global financial system, where secure "quantum-ready" networks and vulnerable classical systems operate side by side: a scenario that could magnify the risks of coordinated attacks.

Addressing these gaps will require international coordination, standardized PQC frameworks, and capacity-building for less prepared countries. But technical standardization alone is not enough. Developing countries may need capacity-building initiatives, funding, and technical assistance to accelerate their adoption of PQC, similar to how cybersecurity frameworks were globally harmonized over the past decade. Without these efforts, the global financial system may enter the quantum era with uneven defenses, increasing exposure to asymmetric threats. Ultimately, the disparity in PQC readiness is technological, structural, and geopolitical. Ensuring that a wider range of countries can participate in secure quantum-era financial networks will be important for maintaining global trust, reducing sequential risk exposure, and preserving the integrity of international markets [2, 3, 7].

At the international level, early discussions on quantum coordination and cryptographic transition have begun within institutions such as the United Nations, particularly through bodies like the International Telecommunication Union and the UN Institute for Disarmament Research, which have highlighted the need for inclusive governance and capacity-building in emerging quantum technologies. However, these initiatives remain largely exploratory, with no fully comprehensive global framework established yet to

ensure that post-quantum cryptographic readiness advances equitably across countries at different levels of economic and technological development [19].

5.2. Effects of Global Standards on International Blocs

There is a growing international momentum to create global standards for quantum cybersecurity, particularly for PQC. NIST finalized three PQC standards: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), based on Kyber, Dilithium, and SPHINCS+ [20]. Many governments and technology vendors are aligning with these algorithms to maintain interoperability across borders [20]. This gives PQC an unusually strong push toward becoming a single global baseline, even if the pace of adoption differs by region.

The standardization landscape for QKD is less uniform. Organizations such as the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) are working on QKD protection profiles and network standards that aim to ensure compatibility across implementations [21, 22]. However, QKD is closely tied to physical infrastructure and supply chains, which means implementation choices often reflect geopolitical and industrial alignments, not just technical considerations. This geopolitical dimension is already emerging. The North Atlantic Treaty Organization's (NATO's) first quantum strategy emphasizes building a "quantum-ready alliance" through shared standards, coordinated industrial policy, and a unified security posture [23]. In practice, this means most G7 and NATO countries are likely to follow NIST PQC and ETSI/ITU QKD standards, ensuring tighter interoperability within the alliance. The distribution of quantum investment also shows distinct patterns across geopolitical groupings. Several NATO member states, including the United States, the United Kingdom, Germany, and France, appear among the higher investment levels, while within the BRICS grouping, investment activity is more uneven, with China showing particularly high funding compared to other member countries (Figures 3A and 3B).

By contrast, BRICS countries are pursuing a strategy that prioritizes technological sovereignty [24]. China, in particular, is developing large-scale quantum communication infrastructure, including satellite QKD links and experimental cross-border channels with Russia [25]. India, as another central BRICS member, is beginning to follow a complementary but distinct trajectory, according to recent government planning on post-quantum cryptography migration [26]. Rather than prioritizing large-scale QKD infrastructure deployment, India has emphasized strategic autonomy through domestic capability-building in quantum technologies, most notably via its National Quantum Mission. This initiative focuses on developing indigenous quantum communication systems, quantum-secure networks for government and defense use, and post-quantum ready cryptographic research, while maintaining interoperability with global software-based standards.

Taken together, these approaches suggest that BRICS quantum strategies are not monolithic but layered: China emphasizes infrastructure-led QKD sovereignty, while India prioritizes scalable, domestically governed quantum and post-quantum capabilities that can be selectively integrated into international systems [26]. If these trajectories continue, the risk is not necessarily a complete split in global

quantum-security standards. A more likely concern is partial fragmentation: broad convergence around PQC standards for software-based cryptography, alongside more region-specific QKD infrastructure shaped by national investment priorities, supply chains, and security partnerships. In this scenario, PQC could still provide a common baseline for cross-border financial interoperability, while QKD deployment may vary more sharply across geopolitical blocs because it depends on physical infrastructure and trusted network design. This fragmentation is already visible in the difference between U.S. guidance, which treats quantum-resistant cryptography as more cost-effective and maintainable than QKD, and QKD-oriented infrastructure efforts in Europe, China, and parts of Asia, where governments are deploying or planning quantum-secure communication networks under separate governance and certification models [27].

For the financial sector, this risk of partial fragmentation carries clear implications. A shared PQC baseline would still allow banks and clearing systems to maintain global interoperability in core cryptographic functions. But diverging QKD infrastructures could complicate cross-border financial messaging, authentication, and key exchange, especially where regulatory or trust frameworks are not aligned. Large multinational financial institutions may need to build crypto-agile gateways capable of operating across both alliance and BRICS-aligned networks, treating PQC as the common layer and QKD as a region-specific add-on.

6. FINANCIAL ORGANIZATION RESPONSES TO QUANTUM THREATS

After examining international standards and geopolitics, we now turn the analysis to organization-level responses in the financial sector.

6.1. Frameworks and Global Initiatives

A number of major regulatory bodies and financial governance organizations have already integrated quantum risk into their cybersecurity and operational resilience strategies. Regulatory frameworks like DORA and IMF guidance emphasize early PQC migration, cryptographic risk assessment, and coordinated international timelines [3, 7]. These policy-level initiatives represent a shift towards proactive governance, recognizing the long lead time required to implement cryptographic change at scale.

In addition to regulatory action, global initiatives are playing a central role in advancing quantum readiness. Central banks in France, Germany, Singapore, Italy, Brazil, and Canada have launched early quantum-safe communication pilots, often pairing PQC with QKD for secure interbank transactions. One example of this is Project Leap, a joint pilot led by the Bank of France with the Deutsche Bundesbank and the Bank for International Settlements Innovation Hub Eurosystem Centre, which focused on "quantum-proofing" central bank processes by testing post-quantum cryptographic protocols in payment-style use cases and creating a quantum-safe environment to protect data in transit, including trials of all NIST-selected algorithms plus FrodoKEM [7]. Another example is a cross-continental experiment between the same French central bank and the Monetary Authority of Singapore that trialled post-quantum cryptography for encrypting and digitally signing emails over conventional internet infrastructure, which is directly relevant to operational resilience because secure communications and

authentication underwrite payment operations, incident response coordination, and supervisory workflows. Moreover, Jančiūtė also points to related central bank efforts such as a feasibility study applying post-quantum methods to Brazil's instant payment system (Pix) and policy-oriented work on quantum-safe payments and post-quantum credentials from Italy and Canada, reinforcing the picture that adoption is currently dominated by scoped pilots and migration planning rather than full-scale deployment [7]. These coordinated pilots help identify interoperability challenges and shape shared international standards [3]. Platforms such as the Quantum Safe Financial Forum, Organization for Economic Co-operation and Development (OECD), IMF, and World Economic Forum (WEF) are further supporting alignment through collaborative information sharing, timeline coordination, and ethical standard-setting discussions [3, 6, 7]. These efforts reflect a growing understanding that quantum resilience must be treated as a global public good, not a purely national responsibility.

Alongside policy measures, technical standardization efforts are laying the foundation for a coordinated global transition to quantum-safe cryptography. The previously mentioned algorithms selected by NIST, Kyber (for encryption) and Dilithium (for digital signatures), and SLH-DSA, based on SPHINCS+, are first-generation PQC standards which provide the technical benchmarks around which both public and private institutions can build migration strategies. These standards give organizations clear implementation targets because they specify the standardized algorithm profiles and wire formats that implementations must follow, for example ML-KEM (standardized in Federal Information Processing Standards Publication 203, or FIPS 203, and derived from CRYSTALS-Kyber) with defined parameter sets, and ML-DSA (standardized in FIPS 204 and derived from CRYSTALS-Dilithium) for digital signatures. These standards also support interoperability with existing encryption systems because NIST's migration work explicitly centers on cross-vendor interoperability and protocol integration testing, and aligned national-security guidance, the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), similarly treats ML-KEM and ML-DSA as baseline migration targets, reinforcing that implementers should converge on the same standardized variants rather than bespoke ones. NIST's work has effectively become an easily accessible global reference point, enabling international interoperability and reducing fragmentation across financial networks. Furthermore, multinational research consortia funded by the EU, the U.S., and Singapore are accelerating PQC and QKD integration into existing financial systems, with a strong emphasis on interoperability, ethical deployment, and equitable access [2, 7]. These efforts align with central bank quantum-safe pilots and related coordination work conducted through international forums (e.g., the Quantum Safe Financial Forum), which have supported early experimentation and shared research on post-quantum transitions [3, 6, 7]. Together, these standardization efforts provide the technical backbone for organizational preparedness and reduce the risks of fragmented or incompatible cryptographic deployments.

While NIST's PQC standards provide the technical foundation for quantum-safe encryption, organization readiness requires a broader framework that addresses how institutions adopt and manage these technologies. The Responsible Quantum Readiness Levels (RQRL) framework proposed by Mehta and colleagues offers such a structure, adapting NASA's Technology Readiness Level model to the context of quantum finance. It outlines three maturity stages [6] (later exemplified in Table 2):

CONCEPTUAL, *"where companies navigate through the quantum realm, trying to decide sub-areas and related problems that could be solved by quantum methods… It involves time and investment spent on upskilling and delving into the fundamentals of the quantum domain along with straightforward experiments";*
ACTIONABLE, where *"the knowledge attainment and experimentation process reaches beyond testing general quantum concepts and algorithms… the feasibility and practicality of the chosen application is repeatedly examined using simulators, hybrid solvers, and quantum computing units";*
and **OPERATIONAL**, where *"Finally, as quantum technology matures … the organization works to productionize and scale up the selected use case… post-quantum cryptography (PQC) measures should be taken to safeguard the data and algorithms."*

These three stages guide firms from early exploration to secure deployment, emphasizing responsible planning. The framework helps financial institutions evaluate not only their technical capabilities but also their strategic, regulatory, and ethical preparedness for quantum integration. In practice, firms like Wells Fargo, Goldman Sachs, and Fidelity remain in the conceptual stages, using RQRL to coordinate pilot programs and academic partnerships while building the foundations for large-scale implementation [6]. By bridging technological readiness with governance and accountability, RQRL promotes a measured transition toward secure and sustainable quantum adoption across the financial sector.

Together, DORA, NIST's PQC standards, and RQRL help reduce uncertainty by giving institutions clearer regulatory expectations, technical targets, and readiness stages. A similar role can be seen outside quantum security in the Basel Core Principles for banking supervision, which give regulators a shared benchmark for evaluating supervisory systems across countries and are used in IMF–World Bank financial-sector assessments [28]. However, these frameworks do not remove the practical barriers that determine whether adoption can actually occur. Financial institutions still need funding for migration, staff with cryptographic and quantum-security expertise, testing environments for new algorithms, vendor coordination, and plans for replacing legacy systems that may be deeply embedded in existing payment, authentication, and data-storage infrastructure. As a result, standards can clarify the direction of quantum-safe finance, while implementation still depends on institutional capacity and sustained operational investment [3, 6, 7, 20].

These frameworks are not purely technical or regulatory; they also embed ethical considerations that shape how quantum security is approached. The Innsbruck Quantum Ethics Lab (IQEL) emphasizes that the rapid acceleration of quantum research demands an ethics of responsibility and reflection, ensuring technologies are developed in ways that respect human rights, social equity, and environmental sustainability [29]. Similarly, UNESCO's work on the ethics of quantum computing emphasizes that quantum technologies should be guided by responsible governance, equitable access, and transparency to prevent the concentration of benefits among a small group of technologically dominant actors [30]. Mauritz Kop's "Establishing a Legal and Ethical Framework for Quantum Technology" extends this argument, proposing a normative structure grounded in fairness and emphasizing the alignment with global human rights frameworks to maintain public trust and accountability [31]. The RQRL framework

extends these principles into practical implementation, embedding checkpoints for transparency, environmental responsibility, and fairness at each stage of readiness; ensuring that ethical oversight evolves alongside technical capability. Collectively, these ethical perspectives reinforce the importance of embedding normative governance directly into quantum cybersecurity frameworks. At the same time, transparency and ethical governance alone do not eliminate pre-existing economic disparities or unequal geopolitical power dynamics, which continue to shape how quantum technologies are accessed, prioritized, and implemented across countries. As financial institutions and governments adopt PQC and QKD systems, ethical foresight ensures that quantum resilience does not come at the cost of transparency or equity. By integrating ethics into both research and implementation, initiatives like IQEL and UNESCO's work on the ethics of quantum computing enhance regulatory efforts such as DORA and RQRL, working in tandem with technical standards such as NIST's PQC algorithms. Together, they provide a more holistic roadmap, one that balances innovation with moral responsibility, ensuring that quantum-secure finance evolves in a way that strengthens both digital and social resilience.

Taken together, these frameworks outline a staged timeline for organizational quantum readiness. In the near term (0-2 years), institutions are expected to conduct cryptographic asset inventories, integrate crypto-agility into their security architecture, and begin limited PQC pilot implementations. In the medium term (2-5 years), frameworks anticipate broader PQC production rollouts for asymmetric cryptographic use cases, alongside increased reliance on hybrid models that combine PQC with classical algorithms. In the long term (5+ years), organizations are expected to expand infrastructure-heavy measures such as quantum key distribution (QKD) or quantum random number generators (QRNG), particularly for high-value transactions and interbank communications [3, 6]. This timeline aligns closely with ongoing global initiatives and highlights that quantum cybersecurity is not a one-time upgrade but a sustained transformation: regulatory frameworks like DORA and RQRL, together with technical initiatives such as NIST's PQC standardization, provide structured near- and medium-term goals, while international coordination platforms and central bank pilots set the stage for longer-term infrastructure integration.

7. COMPANY-SPECIFIC QUANTUM CYBERSECURITY EFFORTS IN UNITED STATES AND UNITED KINGDOM

Consistent with its actionable readiness position in Table 2, JPMorgan Chase has taken some of the most visible steps toward preparing its infrastructure for quantum-era security. According to company announcements and industry reporting, in 2024 it announced the establishment of a quantum-secured, crypto-agile backbone between two of its data centers, using QKD over live optical fiber to support secure, high-speed communications [32, 33]. This network is designed to allow rapid migration to post-quantum algorithms as standards evolve, blending QKD and PQC to address both current and future threats. The bank has also invested in internal cryptography talent, hiring specialists to address "harvest now, decrypt later" risks before quantum computers become fully practical [32].

According to company announcements, HSBC also falls into the actionable category, reflecting its movement from experimentation toward applied quantum-secure financial use cases [34]. Moreover,

HSBC has also tested quantum computing applications in trading contexts, demonstrating how quantum-secure communications could be integrated into existing financial infrastructure [35]. Beyond network security, HSBC launched a pilot using PQC to safeguard tokenized assets, including physical gold, showing an interest in both protecting transactions and developing new products that are quantum-resilient from the start [34]. By experimenting simultaneously with defensive and operational use cases, HSBC has built a versatile early posture.

Names	RQRL Level (1-9)	Current Initiatives/Pilots in Accordance to RQRL	Primary Focus Area	Expected Adoption Timeline*
JPMorgan Chase	Actionable (RQRL 5-6)	Deployed QKD over live fiber and tested crypto-agile infrastructure for future PQC transition.	Network security, encryption migration	2024–2027 early deployment; full adoption by ~2030
HSBC	Actionable (RQRL 5-6)	Tested QKD in live FX trading; launched quantum-safe tokenized gold pilot secured with PQC.	Secure trading, digital assets	2024–2026 pilots; 2030 broader rollout
Goldman Sachs	Conceptual (RQRL 3-4)	Conducting internal simulations for derivatives pricing and risk modeling.	Quantum algorithms for finance	2026–2029 gradual adoption; post-2030 scaling
Fidelity	Conceptual (RQRL 3-4)	Through FCAT, exploring quantum methods relevant to financial modeling and investment research.	Risk modeling, crypto-agility	2026–2029 moving to early integration; 2030+ scaling
Barclays	Conceptual - Actionable (RQRL 4-5)	Explored quantum-computing applications with IBM in financial-market settlement and optimization-related use cases.	Settlement efficiency, financial optimization	2025–2028 prototypes; 2030 limited deployment
Wells Fargo	Conceptual - Actionable (RQRL 4-5)	Tested QKD-based symmetric key generation with Toshiba and Ciena in a lab proof-of-technology environment.	Quantum-secure key generation, encryption infrastructure	2026–2029 continued pilots; 2030+ broader adoption
KPMG	Actionable (RQRL 5-6)	Created Quantum Readiness Assessment Programs to	Advisory, risk audits	2024–2028 client migration phases;

		guide financial clients through PQC and QKD adoption.		continuous adoption

Table 2. Quantum cybersecurity readiness levels and projected adoption timelines for selected financial institutions based on the Responsible Quantum Readiness Levels (RQRL) framework. The table shows differences in organizational preparedness and implementation stages for post-quantum security technologies [6, 20, 32–41]. *Expected adoption timelines are author estimates based on the cited public initiatives and current readiness levels.

By contrast, the institutions listed as conceptual or early-actionable are focusing more on readiness and research than immediate deployment. Goldman Sachs has conducted internal quantum algorithm testing for pricing and risk calculations, while broader industry migration planning is being shaped by NIST's PQC standards [20, 39]. Fidelity, through its Fidelity Center for Applied Technology (FCAT), has taken a similar innovation-focused approach, exploring emerging technologies that may affect financial services and investment strategies [37]. While these early movers have the resources to fund pilot programs, many mid-sized institutions rely on advisory firms to guide their quantum transition. KPMG has developed quantum readiness programs that help firms identify their cryptographic dependencies, conduct security audits, and build migration plans aligned with PQC standards. This is often the first tangible step for firms without the scale to build QKD or PQC pilots on their own [38].

These case studies also provide evidence of a readiness gap within the financial sector. JPMorgan Chase and HSBC show what high-capacity institutions can do when they have the capital, technical staff, vendor relationships, and regulatory capacity to test quantum-secure infrastructure directly [32–35]. Smaller or less technically specialized institutions may move more slowly because they often depend on external guidance, advisory programs, vendor roadmaps, and clearer regulatory expectations before beginning large-scale migration [3, 6, 7, 20]. For this reason, company pilots should not be read as evidence of sector-wide readiness. They are better understood as early examples from institutions with unusually strong implementation capacity, while much of the broader financial sector may remain closer to assessment, planning, or staged software-based PQC migration.

The standards landscape is also shaping the pace and structure of adoption. NIST's formal standardization of ML-KEM, ML-DSA, and SLH-DSA gives institutions a clear technical target for interoperability and implementation. Larger firms like JPMorgan Chase are already testing and deploying quantum-secure networks and hybrid quantum security strategies that combine QKD with a crypto-agile architecture designed to accommodate emerging post-quantum cryptographic standards such as ML-KEM and ML-DSA, derived from CRYSTALS-Kyber and CRYSTALS-Dilithium [20, 32]. This emerging landscape reflects a practical divide. Large multinational banks are running live pilots on critical infrastructure, building the internal capacity to adapt early. Smaller institutions are preparing to follow once the standards stabilize, relying on external guidance rather than direct investment in experimental infrastructure. It is not just a matter of funding, but also operational capacity and regulatory readiness. As a result, early adopters like JPMorgan and HSBC are effectively setting the technical trajectory the rest of the sector could follow.

8. CONCLUSION

As quantum technologies move from theoretical exploration to real-world deployment, their influence on global finance is becoming increasingly clear. Quantum computing presents both unprecedented opportunities for innovation and profound risks to the digital infrastructure that underpins modern economies. Financial systems, dependent on the integrity of encryption, now face a transformation that extends beyond technology into policy, governance, and ethics.

Quantum cryptography, with its foundation in the physical laws of quantum mechanics, offers a means of achieving strong theoretical security for key distribution under ideal assumptions. Yet, as this paper has shown, its adoption raises complex challenges. Integrating quantum key distribution with classical encryption methods can strengthen resilience, but doing so requires extensive investment, international coordination, and careful regulation. Moreover, algorithms such as Shor's and Grover's continue to threaten current cryptographic systems, exposing the urgent need for PQC and hybrid defenses that bridge classical and quantum approaches.

At the same time, disparities in readiness across countries and institutions reveal that quantum resilience is not just a technical issue but a geopolitical and economic one. Wealthier nations are investing in PQC infrastructure and quantum-safe pilots, while less-developed economies risk being left behind, creating uneven defenses in a globally connected financial economy. The company case studies reinforce this broader pattern: institutions with greater capital, technical capacity, and vendor access are already piloting or planning quantum-safe pathways (often through staged, hybrid strategies), while others remain limited to risk assessment and longer-horizon transition planning. These asymmetries highlight that the overall strength of the system will be determined by the gaps in preparedness across the system, not by the innovation at the top.

Regulatory frameworks and global initiatives such as DORA, RQRL, and NIST's PQC standards demonstrate that a structured, phased approach to quantum adoption is both possible and necessary. They set near and mid-term goals for adoption, emphasize interoperability, and link regulatory oversight with technological deployment. Ethical oversight, addressed through initiatives like the Innsbruck Quantum Ethics Lab and UNESCO's work on the ethics of quantum computing, plays a supporting role, helping ensure that the pursuit of quantum advantage remains transparent.

Ultimately, the effects of quantum cryptography on financial infrastructure extend beyond computation; they redefine how innovation and security interact in a digital economy. Preparing for this shift requires not only advanced algorithms but also a unified strategy among governments, central banks, and private institutions. Although not discussed in this review, various other factors are important to consider when evaluating the long-term viability of quantum-secure finance. This includes workforce development; interdisciplinary training at the intersection of finance, cryptography, and quantum engineering; and institutional capacity to translate research advances into operational expertise. Uneven investment in these areas may further amplify existing disparities in quantum readiness across countries and financial

systems. Even after technical standards become available, unresolved challenges such as cost, interoperability, infrastructure dependence, legacy-system replacement, testing requirements, and workforce shortages may slow the transition to quantum-secure finance. The central contribution of this paper is therefore to show that quantum-secure finance will depend on implementation conditions as much as technical design: whether PQC, QKD, and hybrid approaches can be deployed affordably, interoperably, and evenly across institutions and countries. Those that adapt early will set the standards for quantum-era finance, and those that delay may face greater long-term exposure if vulnerable cryptographic systems remain widely used. The quantum transition, if managed responsibly, can strengthen both the technical and structural resilience of global financial systems for decades to come.

9. ACKNOWLEDGEMENTS

The making of this paper was partially supported by NSF award DMS-2231533. The author would like to thank Carl Miller for reviewing a draft and providing valuable feedback.

BIBLIOGRAPHY

[1] A. Naik, E. Yeniaras, G. Hellstern, G. Prasad, and S. Vishwakarma, “From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance,” Financial Innovation, vol. 11, 2025. doi: 10.1186/s40854-025-00751-6.

[2] C. Andriani, L. Bencivelli, A. Castellucci, M. De Santis, S. Marchetti, and G. Piantadina, “The Quantum Challenge: Implications and Strategies for a Secure Financial System,” Bank of Italy Occasional Paper, no. 877, 2024. doi: 10.2139/ssrn.5246652.

[3] M. Gorbanev, M. Malaika, and T. Saadi Sedik, “Quantum Computing and the Financial System: Spooky Action at a Distance?,” IMF Working Paper, 2021. doi: 10.5089/9781513572727.001.

[4] S. Dixit, “The Impact of Quantum Supremacy on Cryptography: Implications for Secure Financial Transactions,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2020. doi: 10.32628/CSEIT2064141.

[5] R. Orús, S. Mugel, and E. Lizaso, “Quantum computing for finance: Overview and prospects,” Reviews in Physics, vol. 4, 2019. doi: 10.1016/j.revip.2019.100028.

[6] B. Mehta, B. Tuscai, T. Wang, and K. Mahady, “Responsible Quantum Readiness: A Perspective from Financial Services Organization,” in Proceedings of the IEEE International Conference on Quantum Computing and Engineering, 2024. doi: 10.1109/QCE60285.2024.10255.

[7] L. Jančiūtė, "Cybersecurity in the financial sector and the quantum-safe cryptography transition: In search of a precautionary approach in the EU Digital Operational Resilience Act framework," International Cybersecurity Law Review, vol. 6, pp. 145–154, 2025. doi: 10.1365/s43439-025-00135-7.

[8] SWIFT, "Three years on from Bangladesh: Tackling the adversaries," SWIFT ISAC Report, 2019. Available: https://www.swift.com/swift-resource/210491/download?language=en.

[9] National Security Agency, "NSA 2024 Section 702 Certification D Amended Minimization Procedures," 2025. Available: https://www.intelligence.gov/assets/documents/702-documents/declassified/2025/NSA_MPs_Amended_2024_Cert_D_3-21-25_Redacted_8-19-25_final.pdf.

[10] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum cryptography," Applied Physics B, vol. 67, 1998. doi: 10.1007/s003400050574.

[11] U. Madje and M. Pande, "Use of Quantum Cryptography Environment for Authentication in Online Banking Transactions Security," in Proceedings of TEMSMET, pp. 1–8, 2021. doi: 10.1109/TEMSMET53515.2021.9768680.

[12] P. W. Shor, "A polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer," 1994. Available: https://arxiv.org/pdf/quant-ph/9508027.pdf.

[13] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996. Available: https://arxiv.org/pdf/quant-ph/9605043.pdf.

[14] S. Poledna, S. Martínez-Jaramillo, F. Caccioli, and S. Thurner, "Quantification of systemic risk from overlapping portfolios in the financial system," Journal of Financial Stability, vol. 52, 2021. doi: 10.1016/j.jfs.2020.100808.

[15] QURECA, "Quantum initiatives worldwide," 2025. Available: https://www.qureca.com/quantum-initiatives-worldwide.

[16] United Nations Development Programme, "Human Development Report data center: Documentation and downloads," 2024. Available: https://hdr.undp.org/data-center/documentation-and-downloads.

[17] F. E. Catota, M. G. Morgan, and D. M. Sicker, "Cybersecurity education in a developing nation: The Ecuadorian environment," Journal of Cybersecurity, vol. 5, no. 1, 2019. doi: 10.1093/cybsec/tyz001.

[18] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," arXiv, 2023. Available: https://arxiv.org/abs/2307.06520.

[19] D. Cho, "2024 Innovations Dialogue: Quantum Technologies and Their Implications for International Peace and Security," UNIDIR, 2024. Available: https://unidir.org/publication/2024-innovations-dialogue-quantum-technologies-and-their-implications-for-international-peace-and-security/.

[20] National Institute of Standards and Technology, "Post-quantum cryptography standards approved," 2024. Available: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved.

[21] European Telecommunications Standards Institute, "Quantum key distribution (QKD) technology overview," 2024. Available: https://www.etsi.org/technologies/quantum-key-distribution.

[22] International Telecommunication Union, "Quantum key distribution network security recommendations," 2023. Available: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13990.

[23] North Atlantic Treaty Organization, "NATO releases first quantum strategy," 2024. Available: https://www.nato.int/en/news-and-events/articles/news/2024/01/17/nato-releases-first-ever-quantum-strategy.

[24] BRICS, "Rio de Janeiro declaration: Strengthening global South cooperation for a more inclusive and sustainable governance," 2025. Available: https://brics.br/en/documents/presidency-documents/250705-brics-leaders-declaration-en.pdf.

[25] Mercator Institute for China Studies, "China Tech Observatory: Quantum Technology Report," 2024. Available: https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf.

[26] Telecommunication Engineering Centre, Government of India, "Migration to post-quantum cryptography: Technical report TEC 910018:2025," 2025. Available: https://www.tec.gov.in/pdf/TR/Final%20technical%20report%20on%20migration%20to%20PQC%2028-03-25.pdf.

[27] International Institute for Strategic Studies, "QKD governance gap: Certification, fragmentation and the cost of delay," IISS, 2026. Available: https://www.iiss.org/online-analysis/online-analysis/2026/04/qkd-governance-gap-certification-fragmentation-and-the-cost-of-delay/.

[28] F. Melo, K. Seal, and V. Salomao, "2024 Revised Basel Core Principles for Effective Banking Supervision," IMF Policy Paper, no. 2024/037, 2024. doi: 10.5089/9798400286636.007.

[29] University of Innsbruck, "Innsbruck Quantum Ethics Lab (IQEL)," 2022. Available: https://www.uibk.ac.at/projects/iqel/index.html.en.

[30] UNESCO World Commission on the Ethics of Scientific Knowledge and Technology, "The Ethics of Quantum Computing," UNESCO, 2025. Available: https://unesdoc.unesco.org/ark:/48223/pf0000398114.

[31] M. Kop, "Establishing a legal and ethical framework for quantum technology," Stanford Law School, 2021. Available: https://law.stanford.edu/wp-content/uploads/2021/04/Mauritz-Kop_Establishing-a-Legal-Ethical-Framework-for-Quantum-Technology_Yale-YJoLT.pdf.

[32] O. Alia, A. Huang, H. Luo, O. Amer, M. Pistoia, and C. Lim, "100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber," arXiv, 2024. Available: https://arxiv.org/abs/2405.04415.

[33] JPMorgan Chase, "JPMorgan Chase, Toshiba and Ciena build the first quantum key distribution network used to secure mission-critical blockchain application," 2022. Available: https://www.jpmorganchase.com/newsroom/press-releases/2022/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network.

[34] HSBC, "HSBC pilots quantum-safe technology for tokenised gold," 2024. Available: https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc-pilots-quantum-safe-technology-for-tokenised-gold.

[35] HSBC, "HSBC pioneers quantum protection for AI-powered FX trading," 2023. Available: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading.

[36] HSBC, "HSBC and quantum," n.d. Available: https://www.hsbc.com/who-we-are/hsbc-and-digital/hsbc-and-quantum.

[37] IonQ, "IonQ and Fidelity Center for Applied Technology announce development of scalable quantum state preparation for Monte Carlo algorithms," 2023. Available: https://www.ionq.com/news/ionq-and-fidelity-center-for-applied-technology-announce-development-of.

[38] KPMG, "Quantum and cybersecurity readiness for financial institutions," 2024. Available: https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html.

[39] Goldman Sachs, "Engineering Quantum Algorithms," 2021. Available: https://www.goldmansachs.com/careers/blog/possibilities-quantum-computing.

[40] T. Osborn, "Barclays, IBM test quantum computing for settlement," Risk.net, 2019. Available: https://www.risk.net/risk-management/7087566/barclays-ibm-test-quantum-computing-for-settlement.

[41] Toshiba Quantum Technology, "Wells Fargo technology case study: Quantum key distribution for symmetric key generation," 2024. Available: https://www.toshiba.eu/solutions/quantum/wp-content/uploads/resources/External-Case-Study-QKD-Symmetric-Key-Generation.pdf.