Implications of Quantum Computing on Financial Markets

FINAL REPORT

The Board of the
International Organization of Securities Commissions

FR/07/26 November 2026

Copies of publications are available from
The International Organization of Securities Commissions website

iosco.org

© International Organization of Securities Commissions 2026.
All rights reserved. Brief excerpts may be reproduced or translated
provided the source is stated.

Table of Contents

Table of Contents **iii**

1. Executive Summary **5**

2. Introduction **8**

A. Background 8

B. Purpose 9

C. Methodology 10

D. Structure 10

3. Applications of Quantum Computing in Financial Markets **12**

A. Key Concepts and Definitions 12

B. Potential Applications of Quantum Computing in Financial Markets 15

C. State of Development of Potential Quantum Computing Applications 21

4. Vulnerabilities in Firms' Cryptographic Systems and Blockchain Systems **27**

A. Key Concepts and Definitions 27

B. Vulnerabilities in Financial Institutions' Information and Communications Systems and Public Blockchains 35

5. Implications for Investor Protection, Market Integrity, and Financial Stability **42**

A. Overview 42

B. Investor Protection 43

C. Market Integrity 43

D. Financial Stability 45

6. Jurisdictional Quantum Preparedness and Migration Measures **46**

A. Overview 46

B. Common Elements of Quantum Preparedness Frameworks 47

C. Roadmaps and Migration Timelines 48

7. State of Quantum Preparedness 50

A. Overview 50

B. Governance and Organizational Structures 52

C. Technical Preparedness 54

D. Ecosystem Dependencies and Coordination 57

E. How Imminent and Serious is the Q-Day Threat? 60

F. Considerations for Further Engagement 60

8. Conclusion 62

1. Executive Summary

Quantum computing has the potential to affect financial markets through both new technological capabilities and emerging cybersecurity and operational risks. While practical quantum computers capable of delivering large-scale commercial advantages or compromising widely used cryptographic systems do not yet exist, continued advances in quantum technologies have increased attention on their potential implications for financial markets and market participants.

This Report examines four areas relevant to IOSCO's mandate: (i) potential applications of quantum computing in financial markets; (ii) vulnerabilities arising from quantum-related threats to cryptographic systems and blockchain networks; (iii) jurisdictional measures supporting quantum preparedness and the transition to post-quantum cryptography (PQC); and (iv) the current state of quantum preparedness among authorities and regulated firms. The analysis draws upon a survey of IOSCO members, stakeholder engagement with industry experts and market participants, and a review of relevant literature.

The Report finds that quantum computing applications in financial services are at an early stage of development. Potential use cases are concentrated in areas such as portfolio optimization, simulation and modelling, machine learning[1], derivatives pricing, risk management, fraud detection and market surveillance. Activity remains largely limited to theoretical research, proof-of-concept exercises and pilot testing. No surveyed jurisdiction reported operational deployment of quantum computing applications within regulated financial services at this stage. While quantum computing may eventually offer benefits for certain computationally intensive financial activities, significant technological and practical barriers remain before these applications can be deployed at scale. Given both the technical complexity and immaturity of the technology, there are potential risks of "quantum washing", where institutions may overstate the role, maturity, or performance of quantum computing use cases across products or services.

At the same time, quantum computing presents a significant medium to long-term cybersecurity challenge. A sufficiently capable quantum computer could undermine widely used public-key cryptographic algorithms that support secure communications, digital signatures, authentication mechanisms and other critical functions across financial markets. These risks extend across financial institutions, financial market infrastructures, and blockchain-based systems. Migration to post-quantum cryptography may be particularly challenging for blockchain systems because cryptography is embedded in their core architecture and implementation requires coordinated action across decentralized networks.

The possibility of "harvest now, decrypt later" attacks further highlights that some quantum-related risks may emerge (or even might be happening) before cryptographically relevant quantum computers become available. Advances in artificial intelligence may further compress the time available to detect, analyze, and respond to sophisticated attacks.

Importantly, the Report identifies migration to PQC and the development of "crypto-agility" capabilities to update cryptographic systems without significant redesign or operational disruption,

[1] Quantum Machine Learning (QML) explores quantum approaches to representing and processing data, with the aim of improving classical machine-learning models.

as crucial components of long-term preparedness against quantum risks. PQC and crypto-agility are the principal scalable measures for broad-based preparedness, while quantum key distribution may be suitable as a complementary solution for selected high-security communication channels.

IOSCO analysis also indicates that jurisdictions are increasingly developing measures to support quantum preparedness. While approaches differ, common elements include cryptographic discovery and inventorying, governance and transition planning, developing crypto-agility, testing and experimentation, and engagement with third-party providers and ecosystem participants. Many initiatives adopt risk-based and phased approaches to migration planning, reflecting the anticipated scale and complexity of transition efforts.

IOSCO members' survey responses and stakeholder engagement suggest that preparedness across the financial sector remains at an early stage. Most observed activities are concentrated on awareness-raising, governance development, training, identifying inventories of cryptographic assets at risk and preliminary migration planning. More advanced activities, including migration testing, validation and implementation, remain limited. Authorities and regulated firms identified several common challenges, including third-party dependencies, interoperability concerns, resource constraints, limited technical expertise and uncertainty regarding migration plans and timelines. Some described a tendency towards "quantum-procrastination", whereby organizations recognize the need to prepare but defer action in anticipation of clearer regulatory signals, greater technological maturity, or broader industry adoption.

A recurring theme throughout the Report is that quantum preparedness is not solely an individual organizational challenge but also a collective ecosystem challenge and change. It is not a one-time event and requires continuous action and effort from an operational resilience standpoint. Financial institutions, financial market infrastructures, technology providers, standard setting bodies, and regulators are interconnected through shared technologies, common standards, and operational dependencies. As a result, preparedness outcomes cannot solely depend on actions taken by individual organizations, but on coordination and collective action across sectors, stakeholders, and jurisdictions, including securities regulators and IOSCO. Uneven migration could leave residual vulnerabilities at points of interconnectedness, even where individual organizations have completed their own transition.

Overall, the findings suggest that financial market participants and authorities remain in the early stages of understanding and preparing for the implications of quantum computing. While uncertainty remains regarding the future development of quantum technologies, the scale and expected duration of transition efforts are driving increased attention on starting to prepare today. Accordingly, authorities and market participants should not wait for the emergence of cryptographically relevant quantum computers before beginning preparedness and migration planning.

As with previous emerging trends, such as AI or blockchain, there is a current investor protection risk that bad actors use the trend to mislead and take advantage of enthusiastic investors. It will remain critical for securities regulators to review disclosure to ensure it is not misleading and to take swift action against bad actors that appear to be "quantum washing."

Continued monitoring of technological developments, engagement with stakeholders, and the sharing of experiences and good practices may support more informed and consistent approaches to quantum preparedness across IOSCO's membership. The findings of this Report may also provide a basis for future IOSCO engagement on matters such as post-quantum readiness, capacity-

building, public-private dialogue, and international cooperation relating to quantum preparedness in financial markets.

2. Introduction

A. Background

Quantum computing uses the principles of quantum mechanics to perform computations.[2] While the concept of quantum computers (QCs) has been known since the 1980s and the first experimental small-scale QCs were built in the late 1990s, practical QC implementations are not yet available, and it remains uncertain when they will be. According to McKinsey's research, investment in quantum technology startups reached $12.6 billion in 2025 – more than six times the total recorded in 2024.[3]

QCs will not be faster versions of today's computers, and they will not be applicable to all tasks performed by classical computers today. Rather, quantum computing is suited to a specific, narrow set of computational tasks, typically involving complex calculations related to analysis, forecasting, and optimization. For these tasks, a QC could outperform classical supercomputers by several orders of magnitude, making it possible to solve computational problems that are practically unsolvable today.

At the same time, quantum computing poses a significant medium - to long-term cybersecurity risk, particularly for the financial sector, where digital trust depends fundamentally on strong cryptography. This risk is often described in terms of "Q-Day", the point at which a cryptographically relevant quantum computer becomes capable of compromising widely used public-key cryptographic systems. Cryptography underpins the confidentiality, integrity, and operational resilience of financial systems, making it essential that organizations prepare for the possibility that today's asymmetric cryptographic algorithms, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC),[4] could be broken by sufficiently powerful quantum computers. The global financial system – including in the areas of banking, payment services, securities markets, and asset management – relies extensively on RSA and ECC for core functions such as secure communications, digital signatures, transaction integrity, and confidentiality of records.

The migration to Post-Quantum Cryptography (PQC) is far more complex than simply replacing one encryption algorithm with another. The transition is expected to take many years and involves significant architectural, operational, and governance challenges. It requires a system-wide redesign of how cryptography is implemented, managed, and governed across multiple organizations, rather than a straightforward software update. Existing systems, applications, infrastructure, key management processes, and dependencies all need to be identified, assessed, and adapted to support quantum-resistant cryptography while continuing to protect sensitive financial information. In addition, sensitive data may face heightened retroactive risks once quantum attacks become

[2] To aid in reading this Report referencing various technical and complex words and concepts, see further United States NIST, *Glossary*.

[3] McKinsey, *Quantum Investment Surge*, 2026.

[4] RSA and ECC are the two most widely used forms of public-key cryptography. RSA relies on the difficulty of factoring large integers, whereas ECC relies on the difficulty of solving mathematical problems based on elliptic curves. RSA has been widely deployed for decades and remains common in existing systems, while ECC can provide comparable security using smaller cryptographic keys and is increasingly used in modern applications where computational efficiency is important.

feasible, as information harvested today may be decrypted in the future ("harvest now, decrypt later" or HNDL).

Considerable progress has already been made in developing quantum-safe standards, with the United States National Institute of Standards and Technology (NIST)[5] leading the standardization process, while other cryptographic approaches continue to be evaluated. As a result, the primary challenge is no longer the availability of suitable algorithms but the practical implementation of those standards at both organizational and ecosystem levels. Success depends on careful planning, governance, coordinated execution, and sustained investment over an extended period.

Although practical quantum computers capable of breaking today's encryption are not yet available, the threat is considered sufficiently significant that preparation is necessary. Despite this, many organizations continue to view the threat as distant and defer preparedness efforts, reflecting uneven awareness and a limited sense of urgency. This posture is also reinforced by a lack of resources and the existence of other competing priorities (e.g., frontier AI models relevant to cybersecurity risks). Given the scale and expected duration of the transition, many stakeholders emphasize the importance of beginning proactive preparations well before quantum computers become a practical threat.

Recognizing these developments and the evolving landscape, IOSCO's Board-level Fintech Task Force (FTF)[6] established the Quantum Computing Working Group (QWG) as a dedicated working group in 2026 to develop a shared understanding among IOSCO members on the implications of quantum computing in financial markets.

B. Purpose

This Report sets out the findings from IOSCO's analysis covering four key areas:

(a) **Applications of quantum computing in financial markets**: the state of development of quantum computing applications, their potential use cases in financial markets, and the implications for market integrity, investor protection, and financial stability;

(b) **Vulnerabilities in blockchain systems and firms' data systems**: the risks arising from the potential ability of quantum computing to undermine existing cryptographic standards, including vulnerabilities in blockchain-based systems and financial firms' data systems, as well as related risk transmission channels and mitigation approaches;

(c) **Capacity in quantum computing and quantum preparedness**: the current human, technological, and organizational capacity to develop, understand, and adopt quantum technologies, and to prepare for quantum-related risks across the financial sector;

[5] NIST – a US government agency within the U.S. Department of Commerce - has taken the lead in developing post-quantum cryptography, which aims to safeguard information from future quantum computers that could break codes widely used today to encrypt data. https://www.nist.gov/

[6] The FTF was established by the IOSCO Board to oversee IOSCO's policy agenda relating to Fintech developments. The FTF was chaired by Tuang Lee Lim from the Monetary Authority of Singapore (MAS) until April 2026 and is now chaired by Hanzo van Beusekom from the Dutch Authority for the Financial Markets (AFM).

(d) **Quantum preparedness measures**: a stocktake of measures and initiatives being undertaken across jurisdictions to advance quantum preparedness, including approaches to post-quantum cryptography migration and broader preparedness efforts.

This Report aims to analyze emerging risks from quantum computing and their impact on financial markets, to help IOSCO set a foundational base for future efforts to raise awareness and promote proactive cybersecurity preparedness. In addition to the data security risks arising from potential vulnerabilities in existing encryption systems, the Report addresses systemic risks that may threaten market stability and operational resilience.

C. Methodology

As part of its analysis, IOSCO gathered evidence through member surveys, stakeholder outreach, and literature review, as summarized below.

(a) **Survey of FTF members**: A survey of FTF members was conducted in March 2026 to understand members' perspectives on the potential applications and implications of quantum computing in financial markets, vulnerabilities arising from quantum-related risks, and quantum preparedness measures across jurisdictions.

(b) **External stakeholder engagement**: In 2025 and 2026, IOSCO hosted roundtables in Tokyo, New York, Zurich, and Mumbai gathering perspectives from experts representing different roles within the quantum computing ecosystem, including academia, technology providers, financial institutions, and professional services firms.

(c) **Literature review**: IOSCO reviewed publications from international organizations, standard-setting bodies, regulatory authorities, academia, industry associations, market participants, and other stakeholders on quantum computing and quantum preparedness. Relevant findings from the literature review have been incorporated throughout this Report.

D. Structure

This Report is structured as follows.

(a) **Chapter 3** examines the applications of quantum computing in financial markets. It discusses the current state of development of quantum computing, potential use cases in financial markets, and the implications for investor protection, market integrity, and financial stability.

(b) **Chapter 4** assesses vulnerabilities in blockchain systems and firms' data systems. It examines the risks arising from the potential ability of quantum computing to undermine existing cryptographic standards, including implications for blockchain systems, financial institutions, and critical financial infrastructure.

(c) **Chapter 5** provides a stocktake of quantum preparedness measures. It presents a factual and neutral overview of preparedness initiatives being undertaken across jurisdictions, together with thematic observations from IOSCO's outreach and survey work.

(d) **Chapter 6** examines capacity-building and readiness in quantum computing and quantum preparedness. It discusses current human, technological, and organizational capacity,

identifies capacity-building needs, and considers options to support preparedness across the financial sector.

(e) **Chapter 7** concludes the Report. It summarizes IOSCO's key observations and outlines potential considerations for regulatory authorities and future IOSCO engagement on quantum computing and quantum preparedness.

3. Applications of Quantum Computing in Financial Markets

A. Key Concepts and Definitions

A.1. What is Quantum Computing?

Quantum computing harnesses the principles of quantum mechanics to process information in a different way to classical computing. This enables quantum computers to solve certain types of problems more efficiently than today's classical computers. To do so, quantum computers use quantum bits, or *qubits*, which differ from classical bits due to three core quantum mechanical effects:

(a) **Interference:** Quantum computers produce probabilistic outcomes. Interference amplifies the probability of correct answers and suppresses incorrect ones, refining the output distribution toward useful solutions.

(b) **Superposition:** Unlike a classical bit, which can represent either one of two states (0 or 1), a qubit can exist in a probabilistic combination of multiple states ("**superposition**") until it is measured. When multiple qubits are combined, superposition gives rise to an exponentially larger computational space.

(c) **Entanglement:** Entanglement allows qubits to become interdependent, with the state of one instantaneously revealing full or partial information about the state of another regardless of the distance between them. Quantum computers exploit entanglement to generate complex correlations between qubits that have no classical equivalent. By using these correlations, quantum computers can represent and solve complex multi-dimensional problems with many variables and constraints more efficiently than classical computers.

Information in quantum computers (except for quantum annealers, discussed below) is manipulated through *quantum gates*, which operate on individual qubits or on sets of qubits to create and control quantum properties such as superposition and entanglement. A quantum computation typically involves three main steps: (i) encoding classical information into qubits; (ii) processing this information via sequences of quantum gates; and (iii) extracting classical information through measurement.

Quantum gates are the building blocks of quantum circuits, which are used to implement quantum algorithms. These algorithms are specifically designed to exploit quantum effects to perform certain computations more efficiently than classical algorithms – a phenomenon known as quantum speed-up. For certain computational problems, this quantum speed-up advantage becomes more significant at scale: these problems may become intractable for classical computers, and quantum computing could offer an alternative solution.

A related area of development is **quantum networking**, which aims to transmit quantum information between physically separated devices. Rather than processing qubits within a single quantum

computer, quantum networks seek to distribute qubits and quantum states across communication links while preserving quantum properties such as entanglement. Quantum networks could enable multiple quantum devices to operate together, support distributed quantum computing, and facilitate new forms of secure communication, including quantum key distribution.

A.2. General State of Development

Quantum Advantage and Relevance to Finance

The financial sector may be a particularly relevant and early beneficiary of quantum computing.[7] Financial institutions and financial market participants often deal with a range of computationally demanding problems for which a growing set of quantum algorithms has already been developed, especially those involving optimization, stochastic simulation, and some machine learning approaches. At the same time, quantum algorithms are typically tailored to address specific problems, which typically require complex calculations or multivariate computations, and must be executed on quantum hardware with sufficient capabilities to prevent practical overheads from offsetting theoretical performance gains. Despite notable progress in algorithm design, achieving *quantum advantage* – that is, a speed-up delivering tangible practical benefits – remains challenging for problems with commercially relevant specifications.[8]

State of Hardware

Current quantum computing capabilities remain insufficient to solve real-world, industry-scale financial problems more efficiently or more accurately than established classical approaches.[9] For this reason, the development of quantum computing within financial services remains limited to early test environments. Further advances are needed to reduce the resource requirements associated with tasks such as embedding classical data into quantum states, reading out quantum outputs, and performing classical pre- and post-processing. While it is still unknown whether quantum computing will ultimately deliver material advantages for financial applications, certain major financial institutions are already investing in quantum research and capability-building.[10]

At present, however, the technology remains in the so-called noisy intermediate-scale quantum (NISQ) phase of development.[11] This terminology reflects the fact that existing quantum devices are still limited in scale and are affected by multiple forms of noise, which restrict their reliability and practical scalability. Existing devices rely on fragile physical qubits that are extremely sensitive to environmental disturbance, including factors such as temperature, sound, and physical movement. These disturbances can lead to quantum decoherence, whereby qubits lose the quantum properties needed for computation, causing information to degrade and generating computational errors.

7 ESMA, *Quantum computing in financial markets: applications, investments and prospects*, 2026.

8 For an example of quantum advantage, see further below the description on Quantum Monte-Carlo Integration.

9 ESMA, *Quantum computing in financial markets*.

10 Examples include JPMorgan Chase, Goldman Sachs, BBVA and Banco Santander, which have publicly disclosed research programs, partnerships, proof-of-concept projects or broader investments relating to quantum computing and quantum-safe technologies.

11 Microsoft, *Microsoft achieves first milestone towards a quantum supercomputer*, 2023.

Error Correction and the Path to Fault-Tolerant Quantum Computing

Quantum error-correction techniques seek to address this challenge by encoding information across multiple physical qubits to form so-called *logical qubits.*[12,13] Progress towards more powerful quantum computers therefore depends on increasing the number of physical qubits, reducing their error rates, and improving error-correction methods so as to lower the physical qubit overhead needed to create a logical qubit.

A major objective of current research and industry development efforts is the achievement of *fault-tolerant* quantum computers, i.e., theorized large-scale systems capable of performing reliable quantum computations over extended periods without excessive degradation from noise and decoherence. [14]

Quantum computing has developed along two main technological approaches: gate-based quantum computing and quantum annealing.

(a) **Gate-based quantum computers**, also known as universal quantum computers, perform calculations using quantum gates that manipulate qubits. They can execute any quantum algorithm but are highly susceptible to external noise and lack error tolerance. Several competing hardware platforms exist for universal quantum computation, including superconducting circuits, photonic systems, neutral atoms, and trapped-ion technologies. [15]

(b) **Quantum annealers** represent an alternative approach: they rely on physical interactions between qubits embedded in specific materials. While they can be scaled more readily, they are primarily suited to a narrow class of optimization problems.[16]

Industry Adoptions and Hybrid Workflows

Despite the early stage of the technology, several firms – including major technology companies such as IBM, Microsoft and Amazon, as well as specialized start-ups – already provide access to quantum computing hardware and software platforms. This growing access facilitates experimentation and the development of potential applications, including those relevant to financial services. However, access to quantum computing resources remains comparatively costly, and the uncertain commercial benefits of current-generation systems may limit incentives for broader adoption beyond research, experimentation, and capability-building activities.

Currently, most approaches rely on hybrid computing models, in which specific parts of a workflow are run on a quantum computer while the rest are processed using classical systems. This reflects the fact that data preparation, orchestration, error correction, and post-processing generally remain more efficient on classical computers, while quantum processors are typically used only for narrowly defined computational tasks. As a result, hybrid approaches are likely to remain the dominant model

12 Microsoft, *Introduction to quantum error correction*, 2024.

13 Microsoft, *Microsoft and Quantinuum create 12 logical qubits and demonstrate a hybrid, end-to-end chemistry simulation*, 2024.

14 IBM, *What is fault-tolerant quantum computing?* 2025.

15 ESMA, *Quantum computing in financial markets: applications, investments and prospects*.

16 ESMA, *Quantum computing in financial markets: applications, investments and prospects*.

in the near term, as realizing the potential for quantum advantage will require close integration across an increasingly heterogeneous computing infrastructure.

B. Potential Applications of Quantum Computing in Financial Markets

B.1. Overview

Drawing on an extensive literature review, this section identifies and examines the most prominent application areas through which quantum computing could affect financial markets. It focuses on optimization, simulation and modelling, and machine learning, and considers where quantum advantage may emerge within each of these areas. In particular, quantum approaches are expected to be most relevant for problems involving complex, high-dimensional calculations, large numbers of variables, or computationally intensive simulations, where classical methods can become resource-intensive or impractical. The section considers where quantum advantage may emerge within each of these areas. It also examines these applications at the more granular level of financial market lifecycle activities, drawing on real-world examples to illustrate how the theoretical capabilities discussed throughout the section are beginning to be explored and tested in financial market contexts.

B.2. Optimization

Optimization problems commonly require finding an optimum – i.e., a number that minimizes or maximizes the objective function, under a set of given constraints. In the context of financial use cases, the solution could be the optimal allocation of assets that maximizes expected return for a given level of risk, known as portfolio optimization, or assessing the adequate levels of liquidity across a financial network (liquidity management).

In these types of optimization problems, the limiting factor for classical approaches tends to be "scale". Put simply, as the number of variables increases, the number of possible solutions grows rapidly, often exponentially. In financial services, optimization problems may need to account for a significant number of variables, correlations, constraints, market behavior, and time factors.[17] This can make the exhaustive exploration of the resulting search space infeasible for classical approaches and often leads to approximate solutions rather than truly optimal ones.

These characteristics mean that optimization problems are often perceived as potential candidates for quantum advantage. This is primarily due to how quantum computers reapproach these types of problems leveraging two key features:

(a) Quantum computers utilize **superposition** to express more than one solution configuration. This enables quantum approaches to encode a larger search space of possible solutions. While this increases the size of the search space, **interference** diminishes the probability of invalid outcomes and amplifies the probability of finding the optimal solution. The combination of these quantum capabilities enables the quantum computer to navigate an enlarged search space and directs calculations towards more optimal answers.

(b) Additionally, relationships between variables, such as correlations and constraints, can be encoded within the quantum state through **entanglement.** As a result, real-world

[17] C. Markham and R. Grassie, *Quantum computing applications in financial services*, Financial Conduct Authority, 2025.

complexity between variables could be more efficiently translated as correlations between bits at a hardware level.[18]

Portfolio Management and Investment Optimization

Portfolio management is one of the most widely cited financial use cases in which quantum advantage may emerge. This is largely due to the combinatorial optimization problem at its core, which involves identifying the most suitable combination of assets from a large investment universe while accounting for multiple constraints.[19]

At an application level, quantum approaches could support asset selection and portfolio construction by identifying improved combinations of investments across a large number of possible allocations.[20] These approaches could also be used to balance competing considerations such as expected return, risk, and diversification.[21]

Financial institutions are already testing these approaches against practical portfolio construction problems. For example, in proof of concept, BBVA and Multiverse Computing used real market data to compare quantum and quantum-inspired methods for dynamic portfolio optimization.[22] This project examined the ability of these approaches to construct portfolios that balanced risk and return while accounting for transaction costs and other constraints.

A related application is "index tracking", where an investment manager seeks to replicate the performance of a broader market index using a smaller selection of assets. Constraints on the number and combination of assets that can be included form a complex optimization problem. As such, quantum approaches are being explored as a method of identifying portfolios that closely replicate benchmark indices, while reducing the number of assets required.[23]

Quantum approaches are also being explored for index portfolio construction. For example, Vanguard and IBM have explored a hybrid quantum-classical approach to the construction of an exchange-traded fund portfolio under real-world constraints.[24] While this work did not provide a quantum advantage, it demonstrates how quantum optimization techniques are beginning to be applied to more specific portfolio construction problems.

Trade Execution, Clearing, Settlement and Liquidity Optimization

Beyond portfolio management and investment, quantum optimization approaches could also impact the execution and post-trade stages of market activity. Across these activities, firms and market infrastructures must determine how trades, assets, and liquidity should be routed, sequenced, and allocated under multiple constraints. While the specific problems differ, they share forms of combinatorial complexity that can grow rapidly as the number of trades, counterparties, and venues

18 Markham and Grassie, *Quantum computing applications in financial services*.

19 A. S. Naik et al., *From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance*, *Financial Innovation* 11 (2025): 88.

20 Markham and Grassie, *Quantum computing applications in financial services*.

21 Markham and Grassie, *Quantum computing applications in financial services*.

22 S. Mugel et al., *Dynamic portfolio optimization with real datasets using quantum processors and quantum-inspired tensor networks*, Physical Review Research, 2022.

23 ESMA, *Quantum computing in financial markets*.

24 G. Agliardi, G. et al., *Portfolio construction using a sampling-based variational quantum scheme*, 2025.

increase. These characteristics make them potential candidates for quantum optimization techniques, which are designed to address large and complex optimization problems that can become increasingly difficult and resource-intensive for classical computing systems. This potential may become more relevant as financial markets continue to process larger volumes of transactions and operate under increasingly compressed operational timelines.

In the case of trade execution, quantum approaches could support firms determining how best to route, sequence, group, and time trades. Execution decisions require firms to account for order size, venue selection, liquidity, price impact, timing, trading costs, and market conditions. As with portfolio optimization, the number of possible execution strategies can grow rapidly as more trades and constraints are introduced.

Similarly, quantum computing could affect post-trade market infrastructure by improving clearing, settlement routing, settlement matching, liquidity optimization and multi-party netting. These processes involve large volumes of trades, counterparties, settlement instructions, timing constraints, and operational rules. The operational challenge may become more pronounced as markets transition towards shorter settlement cycles, such as the recent move from T+2 to T+1 in some jurisdictions, and as discussions continue regarding same-day or even faster settlement models. Shorter settlement windows reduce the time available for trade processing, funding, collateral mobilization, and exception management, increasing the computational demands associated with optimizing settlement and liquidity flows.

Specific use cases could include optimizing the order in which trades settle when securities or cash are scarce, selecting collateral to meet margin requirements at the lowest opportunity cost, or improving netting arrangements across multiple counterparties. These applications are currently less supported by real-world evidence and public pilots compared to portfolio optimization, but they are closely aligned with the types of combinatorial optimization well suited for potential quantum advantage, namely large-scale optimization problems with numerous interacting constraints and possible solution paths.

B.3. Modelling and Simulation

Many computational problems across financial services involve understanding how complex systems evolve under uncertainty. For example, how asset value, portfolios, or risk may evolve over time and under changing market conditions. The solution to these problems is not deterministic, but instead, is a probabilistic outcome. Modelling and simulation techniques provide solutions by evaluating many possible future scenarios to estimate the likelihood of different outcomes.

Monte-Carlo simulations are a typical example where random samples of variables are taken to simulate probable outcomes. For instance, identifying potential future financial losses based on the Value at Risk (VaR) calculations.[25] Monte Carlo simulations are based on the law of large numbers, and, as such, typically require running a significant number of randomized trials, which can be computationally demanding.

Quantum approaches to Monte Carlo simulation are referred to as Quantum Monte-Carlo Integration (QMCI). These methods seek to accelerate the rate at which Monte Carlo estimates converge, reducing the number of samples required to achieve a given level of accuracy. This improvement arises from how qubits store and process information. In the context of QMCI,

[25] Markham and Grassie, *Quantum computing applications in financial services*.

superposition enables a quantum computer to explore outcomes in parallel, rather than simulating them one-by-one. [26]

QMCI can theoretically achieve a quadratic speedup. This means that if a classical approach requires *N* simulations to achieve a given level of accuracy, a quantum approach would theoretically require only the square root of *N* simulations. For example, one million classical simulations could be reduced to approximately one thousand quantum-enabled simulations.[27]

Product Pricing and Derivatives Valuation

Quantum computing could affect product pricing by enhancing the simulation and valuation of derivatives (e.g., options and swaps), structured products, fixed-income instruments, and path-dependent products. Pricing these instruments often requires large-scale Monte Carlo simulation, stochastic modelling or scenario analysis (see above), especially where payoffs depend on multiple risk factors over time.[28]

One of the most widely discussed use cases is derivatives pricing based on Monte Carlo simulation. A specific example is the work conducted by researchers from JPMorgan Chase, IBM Research, and ETH Zurich on option pricing using gate-based quantum computers.[29] This research publication presents a method for pricing vanilla options, multi-asset options, and path-dependent options such as barrier options using quantum amplitude estimation, which provides a theoretical quadratic speed-up compared with classical Monte Carlo.

In financial-market terms, quantum approaches such as the example above affect front-office and risk-control functions. Faster valuation could help firms reprice complex products more frequently, analyze sensitivities more efficiently, and support intraday risk monitoring. However, at this stage, this use case is still primarily a research and proof-of-concept area rather than a mature production capability.

Risk Management, VaR and Stress Testing

Quantum computing could support risk management by improving risk simulations, stress testing, VaR, Conditional VaR (CVaR), counterparty exposure modelling, and macro-financial scenario analysis.

From an application perspective, quantum-enabled VaR could enable faster or richer risk simulations across portfolios. In turn, these simulations could improve intraday risk monitoring, particularly during periods of market volatility when risk positions must be updated rapidly.[30]

Quantum approaches to CVaR could support improved tail-risk modelling and loss estimation by improving the efficiency of simulations.[31] Additionally, quantum approaches for stress testing could

[26] Markham and Grassie, *Quantum computing applications in financial services*.

[27] N. Stamatopoulos, et. al., *Option Pricing Using Quantum Computers*, *Quantum* 4 (2020): 291.

[28] Markham and Grassie, *Quantum computing applications in financial services*.

[29] N. Stamatopoulos, et. al., *Option Pricing Using Quantum Computers*, *Quantum* 4 (2020): 291.

[30] Markham and Grassie, *Quantum computing applications in financial services*.

[31] Markham and Grassie, *Quantum computing applications in financial services*.

allow for more complex macroeconomic and market stress scenarios.[32] While such potential applications appear across the literature, to date, there are few public examples of real-world experiments to prove the viability of these theoretical approaches.

B.4. Machine Learning

Machine learning is another area in which quantum computing is being actively explored. Many machine-learning techniques involve identifying patterns within large, high-dimensional datasets and learning relationships between variables. Quantum Machine Learning (**QML**) explores quantum approaches to representing and processing data, with the aim of improving classical machine-learning models, and over the longer term, enabling some inference to be performed by quantum hardware.[33] Areas of exploration include:

(a) **Quantum Feature Engineering**, i.e., the process of creating, transforming, or selecting improved features to input into a classical model (e.g., making data patterns easier to detect);

(b) **Quantum Support Vector Machines (QSVMs) and Quantum Neural Networks (QNNs)** which embed complexity into quantum states to potentially produce models that are more compact, scalable, and better at generalization. These approaches are being actively explored to understand the extent to which they can improve or streamline model training, testing and evaluation, including for tasks such as forecasting, classification, and pattern recognition where stronger predictive performance may be achievable under certain conditions.

(c) Finally, **Quantum-Based Natural Language Processing (QNLP)** could enhance textual analysis and classification, potentially leading to more efficient processes and more accurate outputs.[34]

Trade Execution

QML approaches could also affect the development of trading strategies by improving how firms analyze market data, identify patterns, and generate predictive signals. Financial markets produce large volumes of complex and rapidly changing data, which firms use to forecast price movements, assess trading opportunities, and determine when to enter or exit positions. QML methods are being explored to assess whether quantum-enhanced models could identify relationships within this data that are difficult for classical models to capture.

One practical example is the use of QML to predict the probability that a trade will be completed at a given price. In September 2025, HSBC and IBM published the results of a collaborative project exploring the use of quantum and classical computing resources in algorithmic bond trading. The specific use case focused on predicting the probability that a request-for-quote trade would be filled at a given price.[35] Using real production-scale data from the European corporate bond market,

[32] R. Auer et al., *Quantum computing and the financial system: Opportunities and risks*, Bank for International Settlements, 2024.

[33] FINRA Office of Financial Innovation, *Quantum computing and the implications for the securities industry*, Financial Industry Regulatory Authority, 2023.

[34] Markham and Grassie, *Quantum computing applications in financial services*.

[35] HSBC, *HSBC demonstrates world's first-known quantum-enabled algorithmic trading with IBM*, 2025.

the project tested whether quantum-generated data transformations could improve the performance of classical predictive models. According to HSBC, the approach delivered up to a 34% improvement in predicting the likelihood that a trade would be filled at a quoted price compared with common classical techniques used in the industry. This result illustrates how quantum methods could potentially enhance predictive analytics in specific financial-market applications, although further validation and assessment of quantum advantage and scalability would be required.

Credit Scoring and Credit-Risk Assessment

Credit scoring often involves selecting and weighting many borrower characteristics, transaction variables, and macroeconomic indicators. Credit scoring already relies on classical machine learning to classify borrowers, estimate default probability, and support lending decisions.

As such, QML approaches could affect the way lenders assess creditworthiness. The literature suggests that quantum-enabled approaches could support faster model training and improve the identification of complex patterns in borrower data, including those associated with higher credit risk.[36] These improvements could strengthen borrower classification, default prediction, and the assessment of lending risk.[37] The downstream benefits could include faster onboarding, more efficient credit assessments, improved model validation and, potentially, lower losses arising from borrower default.[38,39]

One illustrative example is the collaboration between Crédit Agricole and Quandela, which explored the use of a hybrid quantum-classical approach to improve credit-risk prediction.[40] The project applied quantum techniques within a broader machine-learning workflow designed to predict borrower default risk and reported improvements in predictive performance relative to certain classical benchmark approaches. While still experimental, the project demonstrates how quantum methods are being investigated as a complement to, rather than a replacement for, existing machine-learning techniques used in credit-risk assessment.

It must be noted, however, that QML approaches to credit scoring remain experimental. Their integration into live credit decision-making systems would require significant technological advancement alongside rigorous assessment before they could be feasibly integrated into live credit-decision systems.

Fraud Detection, AML and Market Surveillance

Quantum machine learning could affect fraud detection, anti-money-laundering monitoring, and market surveillance by improving classification, anomaly detection, and pattern recognition across large datasets.[41]

[36] Association of German Banks, *Quantum computing in the financial sector: Revolutionary approaches and future perspectives under the EU Quantum Act*, 2026.

[37] E. Yndurain, S. Woerner, and D. J. Egger, *Exploring quantum computing use cases for financial services*. IBM Corporation, 2019.

[38] Naik et al., *From portfolio optimization to quantum blockchain*.

[39] O. Zapata, *Quantum computing for finance*, CFA Institute Research Foundation, 2025.

[40] Quandela, *Quantum innovation for finance: Crédit Agricole CIB and Quandela optimise default risk prediction models*.

[41] Naik et al., *From portfolio optimization to quantum blockchain*.

Specific use cases could include detecting money mule networks or suspicious transaction patterns by analyzing relationships among accounts, payment flows, locations, counterparties, and behavioral signals and market abuse surveillance, where firms and trading venues look for unusual order patterns, spoofing, layering, or collusive behavior. While these are plausible applications, the public evidence base is less mature than for areas such as portfolio optimization or option pricing research.

C. State of Development of Potential Quantum Computing Applications

C.1. Overview

Building on the previous section, which introduced the application areas through which quantum computing could affect financial markets, this section examines their current state of development. It draws on survey responses from IOSCO jurisdictions to provide greater insight into how quantum approaches are being explored and developed across different application areas and types of financial institutions. The section concludes by considering the emerging areas of opportunity, alongside the key barriers and challenges identified by survey respondents.

C.2. Observation of Quantum Use Cases Across Jurisdictions

Survey responses suggest that quantum computing applications in financial services remain at an early stage overall, with no observed operational deployment. No IOSCO member jurisdiction reported observing the operational deployment of a quantum application currently. Activity is instead concentrated in theoretical research and, to a lesser extent, proof-of-concept and pilot testing.

In line with the limited capabilities and availability of current quantum hardware, the responses suggest that firms are still in the experimentation and monitoring phase rather than one approaching operational adoption. In practice, activity is uneven across use cases and jurisdictions, with a significant number of respondents reporting no observed activity.

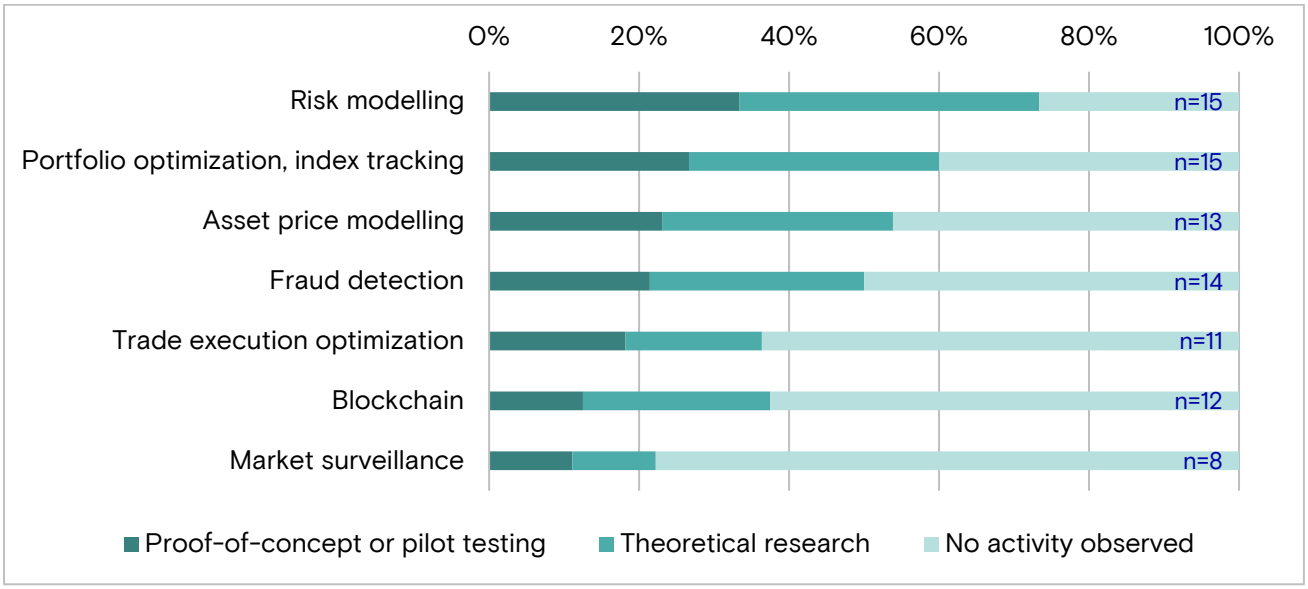

FIGURE 1. *Quantum use cases across jurisdictions.*

Survey responses indicate that activity is uneven across quantum computing use cases and remains concentrated in theoretical research and early experimentation. Risk modelling recorded the highest level of observed activity among the specified use cases. Respondents highlighted both research as well as proofs-of-concept being undertaken by major financial institutions, including credit rating agencies and large banks, as well as observations on potential application of quantum approaches to risk modelling and derivatives pricing.

Portfolio optimization and index tracking also recorded comparatively high levels of activity. Survey submissions point to several signs of growing activity around this use case, including proofs-of-concept conducted by large banks and research partnerships between quantum technology providers and financial institutions. Respondents also describe broader industry interest, reflected in informal and exploratory discussions with firms in their jurisdictions, suggesting that the use case is viewed as an area of both current experimentation and future focus. This may suggest that, where firms have identified a sufficiently clear use case, some are already starting to test how quantum approaches could be applied in practice.

Taken together, the survey responses suggest that **early activity is concentrating around use cases that are already computationally intensive, have a direct bearing on financial institutions' commercial and risk outcomes, and align closely with the optimization and simulation capabilities associated with quantum computing.**

Fraud detection and asset price modelling also showed evidence of development, although activity remains weighted towards research. Among the proofs-of-concept identified by respondents, activity appears to be concentrated among large banks.

Lower levels of activity were reported for trade execution optimization, blockchain, and market surveillance. Overall, the survey indicates selective research and experimentation across a limited number of use cases, but no observed operational deployment.

C.3. Observation of Quantum Use Cases Across Financial Service Types

The analysis by financial service type reinforces the finding that members have observed limited activity relating to quantum computing applications. No respondent reported observing operational deployment among the financial service types covered by the survey. Instead, reported activity was concentrated in theoretical research and, less frequently, proof-of-concept or pilot testing.

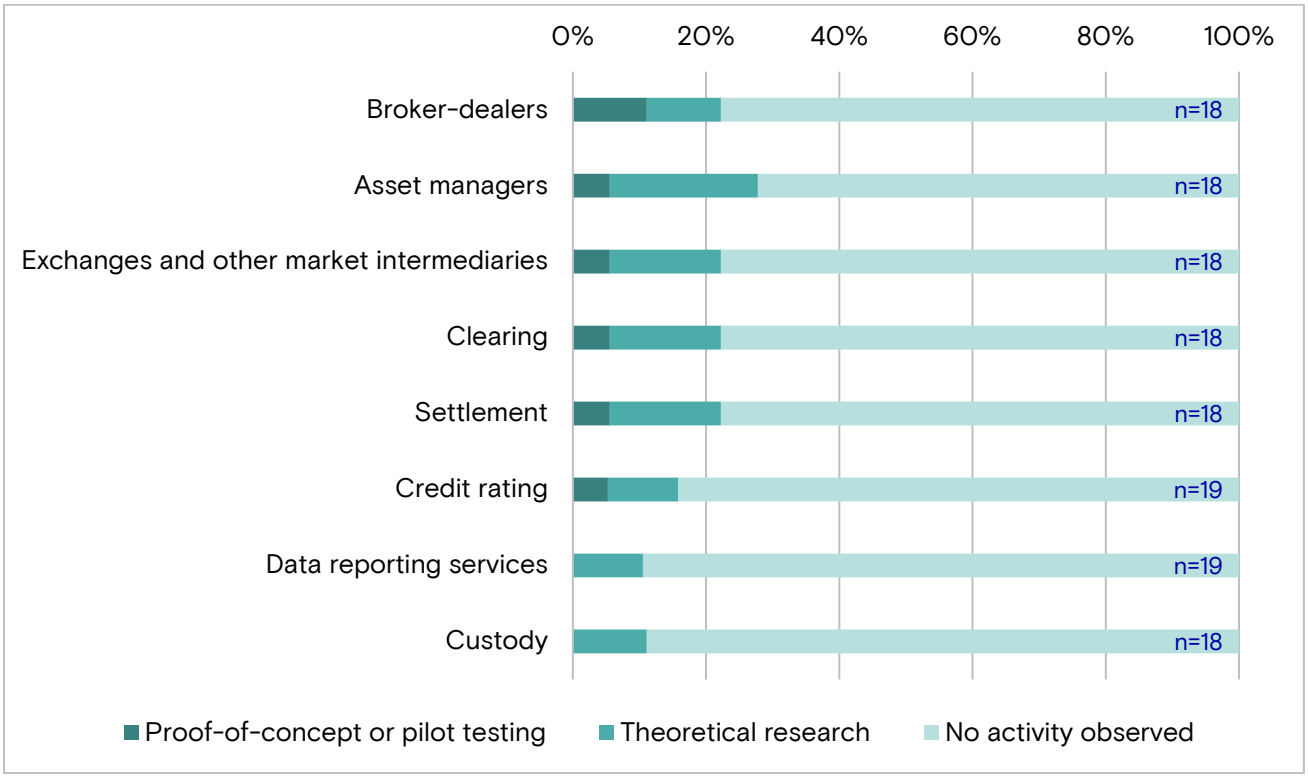

FIGURE 2. *Level of activity observed across financial service types.*

Differences across financial service types were relatively limited. Broker-dealers recorded the highest level of observed activity, while asset managers recorded a slightly greater overall level of activity, driven primarily by theoretical research. Exchanges and other market intermediaries, clearing, and settlement services showed broadly similar, research-led levels of activity. By contrast, credit rating agencies, custody services, and data-reporting services recorded the lowest levels of observed activity.

Qualitative responses indicated that activity was concentrated among large financial institutions, rather than being broadly distributed across regulated financial services providers. The greater extent of experimentation among larger institutions may indicate an emerging capability gap across financial services.

Box 1. Developments in Use Cases Identified by IOSCO FTF Members

Several jurisdictions indicated that the majority of activities identified in relation to quantum computing are found in the banking sector. Some sizeable banking institutions have indeed begun more actively exploring opportunities in quantum computing, assigning resources to investigate business use cases such as product pricing, portfolio optimization, and risk analysis.

One Italian bank identified several quantum computing use cases, including portfolio optimization, credit risk analysis, derivatives pricing, transaction settlement optimization, and post-quantum cybersecurity, which are currently being developed and tested internally.

Currently, these use cases are at research, proof-of-concept, and advanced experimentation stages, with no production level deployment at present.

In Singapore, common use cases that global and local financial institutions are exploring include portfolio optimization and risk simulation, such as Quantum Approximate Optimization Algorithm (QAQO), which iteratively applies different types of operations to a quantum state, allowing for the simultaneous evaluation of multiple portfolio configurations, potentially offering theoretical quadratic speedup over classical methods. Beyond such use cases, institutions are also assessing the predictive capabilities of hybrid quantum machine learning models for forecasting tasks. For example, these models can leverage customer behavioral data to anticipate changes in service usage patterns, enabling early detection of potential discontinuations.

In the United Kingdom, several banks have developed proof-of-concept use cases whereby quantum computing could be used in areas such as optimizing trades in corporate bond markets, AML and fraud detection, and portfolio optimization or trade settlement.

C.4. Opportunities and Challenges of Quantum Computing Applications in Financial Services

The survey responses indicate early signals of a sector where quantum computing opportunities are recognized and actively explored, forging a pathway for adoption and proven value. They also demonstrate that the most credible opportunities for quantum computing use cases are concentrated in a small number of areas where some research or pilot activity is already visible.

However, opportunities remain largely prospective and the barriers to further advancement remain substantial: uncertainty regarding quantum advantage, immature hardware and software, limited firm capability, a shortage of expertise, and incomplete supervisory visibility of this emerging trend. Several respondents indicated that supervisory visibility remains limited because quantum experimentation is concentrated among a relatively small number of firms, often relies on third-party technology providers, and remains at an early stage of development.

This subsection considers these opportunities, barriers, and challenges in greater detail, to provide a holistic view of the state of development of quantum computing use cases.

Optimization, Simulation, and Machine Learning

As demonstrated throughout both the literature review and survey responses, the industry focus is on three computationally intensive financial problems: optimization, simulation and modelling, and machine learning. In the survey responses, portfolio optimization appears repeatedly as an observed use case across jurisdictions, with responses illustrating both a more detailed knowledge of the use case and greater levels of institutional activity. These two factors could indicate a slightly higher level of development given the levels of familiarity across both supervisors and financial institutions.

Modelling and simulation also appear frequently throughout the survey responses. However, a wider degree of use cases, such as derivative pricing and credit risk analysis, are mentioned in relation to this broader category. This suggests that modelling and simulation is a developing area of interest and that the identification and testing of specific use cases may be at an earlier stage.

Survey responses also refer to quantum or hybrid quantum-classical approaches to machine learning to eventually support predictive analysis. While responses refer to ongoing experimentation, the general sentiment points towards quantum machine learning as a longer-term opportunity.

Quantum-Safe Communications and Post-Quantum Resilience as an Opportunity

Although many respondents frame the cybersecurity implications of quantum around risk mitigation, several responses imply an opportunity to strengthen the resilience through PQC, and Quantum Key Distribution[42] (QKD) specifically. Across the survey responses IOSCO members highlight the early research and development of quantum random number generation for improving classical cryptographic encryption as well as QKD for critical, sensitive communications within banks and the potential security benefits for critical communication channels.

Additionally, a recurring theme is the focus on preparing for the migration to post-quantum cryptography across the global financial system. In contrast to the other revenue-generating activities discussed throughout the survey, these responses imply that the emerging risk also provides a welcomed opportunity to future-proof cyber resilience across the sector.

Low Visibility and Lack of Data

One of the most prominent challenges of quantum computing applications in financial services may not relate to the development of use cases but rather that many authorities do not yet have direct evidence from regulated institutions. Survey responses highlight an absence of supervisory engagements to either raise awareness on use cases or to better understand activities. As a result, much of the current evidence base is a mixture of public announcements, informal conversation, academic research, vendor activity, and limited surveys. The visibility gap may be particularly pronounced in jurisdictions where quantum computing activity remains at an early stage, as well as among smaller market participants that may have fewer resources to dedicate to exploratory research and experimentation. Conversely, available information is often concentrated among a relatively small number of large financial institutions, technology providers, and specialised research collaborations that actively publicise quantum-related initiatives. Given the early and experimental nature in developing quantum use cases, this lack of direct engagement means that regulatory authorities cannot confidently assess development trends, risk exposure, or adoption readiness. This in turn limits the readiness of regulators to either facilitate safe and responsible innovation or prepare the sector to manage the emerging and associated risk.

Technological Maturity, Lack of Clear Business Cases, and Ecosystem Readiness

Several responses emphasize that quantum technology is immature or lacking an established business case. The qualitative responses underline that no production-ready deployment is present across observed activity on use cases, and that most activity amounts to publicly available research sources and experimentation partnerships. The survey responses point to several significant technical challenges that are limiting the further development of use cases, including high qubit error rates, which can introduce computational inaccuracies and limit the reliability of results;

[42] The most well-known application of quantum cryptography is quantum key distribution (QKD), which is in development mode. QKD is a pivotal element of quantum cryptography and is based on quantum properties of particles, typically photons. This enables the parties of a communication channel to obtain a shared secret key with the assurance that any interception attempts will be detected. BIS Papers No 149 Quantum computing and the financial system: opportunities and risks.

scalability challenges, as current systems provide only a limited number of logical qubits relative to the much larger numbers expected to be required for commercially relevant applications; programmability limitations arising from the relative immaturity of quantum software development tools and the lack of standardization across hardware platforms; as well as the development of quantum algorithms and software, and integration challenges for enterprise-ready systems.

These responses indicate a more practical barrier for financial institutions. Given the current state of development, it may be difficult to justify the levels of investment required to develop use cases towards business-ready deployment, even where there are signals or potential quantum advantage. This challenge may be compounded by the fact that quantum hardware is still developing, and classical alternatives present relatively much cheaper, reliable, and iterative alternatives.

4. Vulnerabilities in Firms' Cryptographic Systems and Blockchain Systems

A. Key Concepts and Definitions

A.1. Overview

Cryptography is a foundational element underpinning the security and trustworthiness of modern financial systems. It safeguards the confidentiality and integrity of data and transactions and supports authentication mechanisms that enable secure communications, protecting sensitive information and supporting the reliable operation of payment systems, trading platforms, and distributed ledger technologies such as blockchains. The widespread adoption of digital financial services and the increasing reliance on interconnected infrastructures have made robust cryptographic mechanisms essential for maintaining public confidence and ensuring the resilience of the global financial sector.

The emergence of quantum computing presents a significant challenge to the robustness of current cryptographic standards. While classical cryptographic algorithms, particularly those based on public key infrastructure, have long provided effective protection against conventional computational threats, the emergence of a CRQC could undermine the mathematical assumptions on which these algorithms depend. Quantum algorithms, such as Shor's algorithm,[43] have the potential to compromise widely used encryption and digital signature schemes and thereby causing a severe degradation in the security of financial systems, data, and communications, exposing financial systems to new and unprecedented risks.

Given the critical role of cryptography in securing financial data and operations, it is essential to assess the sector's vulnerability to quantum threats. A comprehensive vulnerability assessment enables financial institutions, market infrastructures, and regulatory authorities to understand the scope and scale of potential exposures, prioritize mitigation efforts, and coordinate the transition to quantum-resistant solutions. Proactive evaluation and preparedness are necessary to ensure the continued security, stability, and trust in financial markets as the quantum era approaches.

[43] Shor's algorithm is a quantum algorithm that can efficiently solve certain mathematical problems, including integer factorization and discrete logarithms, on which widely used public-key cryptographic systems such as RSA and ECC rely. A sufficiently powerful CRQC capable of running Shor's algorithm could therefore compromise these cryptographic systems.

A.2. Cryptography Systems

Definition and Role of Cryptography

Cryptography can be defined as an overarching field that includes a body of mechanisms or methods that allow for the transformation of data in order to:

(a) Hide their information content;

(b) Establish their authenticity;

(c) Prevent their modification;

(d) Prevent their repudiation;

(e) Prevent their unauthorized use.[44]

Cryptography is widely used throughout the financial sector because it is essential for securing communications and information systems, protecting sensitive and personal information, maintaining trust in financial networks, and supporting electronic commerce. Financial institutions rely on cryptographic methods to prevent unauthorized access to, modification of, or misuse of data, thereby helping to protect financial information and payment transactions and underpinning public trust in the financial system.

Cryptography is used to encrypt confidential data so that only authorized parties can view them and ensures data integrity by allowing detection of unauthorized alteration. Authentication verifies the identity of users, processes or devices, while digital signatures ensure non-repudiation by binding a signatory's identity to a document.[45]

In more practical terms, cryptography relies on encryption algorithms, hashing, creation of key pairs, and coding. These mathematical processes allow the generation of cryptographic keys, encryption of data, and creation of digital signatures. Used with an algorithm and sensitive data, a cryptographic key will generate the outcome of an encryption or signing algorithm. Cryptographic security relies

[44] OECD, *Recommendation of the Council concerning Guidelines for Cryptography Policy*, 1997:

"Cryptography is a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use. It is one of the technological means to provide security for data on information and communications systems as well as trust in economic and social activities that rely on such data.

"Cryptography can be used to protect the confidentiality of data, such as financial or personal data, whether that data is in storage or in transit. Cryptography can also be used to verify the integrity of data by revealing whether data has been altered and identifying the person or device that sent it. These techniques are critical to the development and use of digital technologies for economic and social purposes."

[45] R. Auer et al., *Quantum-readiness for the financial system: a roadmap*, Bank for International Settlements, 2025: *"Cryptography is used extensively across the financial system to provide assurances including confidentiality, integrity, authentication, access control and nonrepudiation. Confidentiality means that messages or data are transformed into an unreadable encrypted format so that unauthorized parties are unable to view them. Data integrity ensures that data cannot be modified or altered without detection. Cryptographic authentication serves to verify the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system. Digital signatures, used for authenticating the identity of the signatory, can demonstrate to a third party that a signature was generated by the claimed signatory, thereby providing non-repudiation for electronic documents and contracts."*

on the difficulty for a malicious actor to solve the key, i.e. without the exact key, it is nearly impossible to decrypt data or to forge a digital signature.

Symmetric and Asymmetric Cryptography in the Financial Sector

The security of the financial system relies on both symmetric and asymmetric cryptography, supported by public key infrastructure (PKI). Symmetric encryption uses a unique key shared between the sender and the receiver for both encryption and decryption, making it efficient for protecting large volumes of data, such as those stored in databases. However, the main challenge lies in key management: if the shared key is exposed, all protected data is compromised. Symmetric algorithms also provide limited assurance of data, as either party can encrypt or decrypt. The Advanced Encryption Standard (AES) is the most widely used symmetric algorithm worldwide, handling the lion's share of both transport encryption and encrypted data storage, and forms part of the most commonly used transport protocol, Transport Layer Security (TLS). While symmetric methods ensure data integrity, their main weakness is the need for secure key distribution and limited third-party verification of authenticity.

Asymmetric encryption**,** or public key cryptography, uses a pair of mathematically related keys: a public key for encryption, and a private key for decryption. This structure enhances security, as the private key is never shared. Asymmetric algorithms, such as RSA and ECC, are effective for establishing secure communication channels and verifying digital signatures, but are more computationally intensive than symmetric methods, so they are only used for small amounts of data, such as those involved in authenticity verification. They are also frequently combined with symmetric methods; for example, the asymmetric method may be used solely to transmit a session key for a symmetric method, as is the case with the widely used Pretty Good Privacy (PGP) email encryption. Furthermore, in signature schemes, a checksum is usually calculated first using a symmetric method; subsequently, only this value is signed using the signature key of the asymmetric method.

Keys in these systems are usually valid for several months to a year before they are replaced, and compromise of the private key can expose previously encrypted data and allow impersonation until the key's expiry date. By contrast, public blockchains generally do not rely on a centralized certificate authority, but use protocol-level cryptographic and consensus mechanisms to validate transactions across a distributed network.

Asymmetric methods also include key exchange or protocols such as Diffie–Hellman key exchange, which is used in the TLS transport protocol. Key exchange algorithms have the property that all key material is generated only immediately before use and can be destroyed after a single use. An attacker must therefore break each intercepted transmission individually, which is why this is also referred to as perfect forward secrecy.

Symmetric and asymmetric key encryptions serve different purposes and are used together to secure digital interactions.

The efficiency of cryptographic algorithms depends on the following essential elements:

(a) **Key management** which are processes that allow the generation, distribution, use, storage, renewal, and destruction of cryptographic keys. The most prevalent approach to key management is PKI.

(b) **Implementation practices** represent the rigorous fashion in which algorithms are integrated into systems to prevent failures.

(c) **Security protocols** are rules and standards that organize the secure interactions between systems.

Public Key Infrastructure

PKI is a trust framework for managing public keys and digital certificates, which are essential for secure communications in financial systems. It illustrates how key management and identity authentication establish public trust in cryptography, which is fundamental for the stability and the credibility of the financial system. In asymmetric cryptography, each party has a pair of keys, a public one and a private one. PKI addresses the challenges of verifying that a public key belongs to an entity and solves this by using digital certificates, which are electronic documents issued by a trusted third party called a certificate authority[46] (CA). The CA verifies the identity of the party holding the public key and issues a digital certificate linking the identity of that party to a given public key. This process is used, for example, in HTTPS connections for secure online banking.

In today's financial systems, security relies on a combination of symmetric key cryptography (for efficient data encryption), asymmetric key cryptography (for secure key exchange), and PKI (for verifying public keys and establishing trust).

Cryptographic Security and Vulnerabilities

A key element of all common encryption methods consists of so-called one-way functions. These are functions that are easy to compute in one direction, but whose inversion is computationally intensive. For example, the widely used RSA algorithm exploits the fact that prime factorization is extremely difficult to achieve, even with the best-known approaches. The computational effort required for all common methods is so high that an attacker would need thousands of years – or even longer – even if they had access to all the computing power available on Earth.

An important consideration for the security of an encryption scheme is the mathematical relationship between the key length and the effort required to break it, whereby the most efficient known algorithm is always taken into account. Should an attacker possess sufficient computing power to compromise such a scheme, the previous level of protection can be restored by a manageable key extension, with comparatively little additional effort required for encryption and decryption.

In contrast, methods in which there is merely a linear relationship (or a polynomial relationship with a low exponent) between key length and attack complexity are vulnerable. Once an attacker has sufficient capacity to carry out a successful attack, the additional computational effort required for a key extension is well within their capabilities. Such encryption schemes can therefore only be regarded as non-critical as long as the computational effort required far exceeds the attacker's technical capabilities.

Cryptographic schemes can also be broken using so-called "side-channel attacks". In such attacks, the attacker attempts to exploit implementation weaknesses to obtain additional information that makes it much easier to solve the underlying problem. A typical technique, which is particularly favored in asymmetric methods, involves, for example, using the implementation of the encryption method to encrypt known messages consisting usually of just a few bits (e.g. a single character) in order to draw conclusions about the key from the result ("known-plaintext attack"). Side-channel

[46] The authentication of the identity of parties involved in a financial transaction is achieved when a trusted certification authority issues a digital certificate linking the identity of a party to a given public key. Certification authorities are third-party organizations playing an essential role in PKI, by issuing, managing, and revoking digital certificates.

attacks are known to affect all common algorithms and must be mitigated by the developer. In extreme cases, a multitude of possible side-channel attack vectors can render an algorithm that is mathematically sound completely unusable in practice.

All common encryption algorithms can only encrypt or decrypt data blocks of a fixed size, for example, 128 bits in the case of AES-128. Larger amounts of data are therefore divided into blocks, which are processed one after the other. In doing so, two aspects must be defined in the form of the operating mode: the cryptographic chaining of the individual data blocks[47] and the padding of incomplete data blocks to the specified block size ("padding method"). For both of these, current standards recommend several alternatives that offer attackers only a limited attack surface.

To better compare the security of different algorithms (including quantum-secure algorithms) and their associated parameters, such as key lengths, the German Federal Office for Information Security (German BSI) and other security authorities have defined a quantitative measure of the computational effort required to attack them. The reference value used is the computational effort required to encrypt or decrypt a single block using an efficient symmetric algorithm such as AES. As of July 2026, the German BSI's technical guideline lists only those algorithms and their associated parameters that offer a minimum security of 120 bits.

Cryptographically Relevant Quantum Computer

A cryptographically relevant quantum computer (CRQC) is a quantum computer powerful enough to break widely used cryptographic systems within practical timeframes.[48] Despite the severe limitations of current quantum computers, ongoing improvements may eventually enable the development of CRQCs. Such a breakthrough would threaten the security of today's widely used public-key cryptographic algorithms, such as RSA and ECC, which underpin digital security in the financial sector.

Modern cryptography currently relies on mathematical problems that are extremely difficult for classical computers to solve. As mentioned previously, the two main categories are symmetric cryptography and asymmetric cryptography. While quantum computers can solve the symmetric key algorithms using Grover's algorithm, the quantum attack risk can be mitigated by increasing key sizes, for example, by using the AES-256 algorithm instead of the AES-128 one.

As for asymmetric cryptography, a CRQC can efficiently run Shor's algorithm to allow an attacker to break the RSA or ECC algorithms within a practical amount of time (whereas these are computationally infeasible for classical computers). Consequently, digital systems using existing standards for public key cryptography will become vulnerable to the quantum threat of a CRQC.

"Harvest Now, Decrypt Later" (HNDL) Risk for Long-Lived Data

While a CRQC may not be deployed for several years, quantum computing still poses a threat to the financial sector today. The most important and immediate threat to confidentiality is HNDL. Malicious actors may already be storing encrypted data traffic with the intention of decrypting it in the future using a CRQC. This risk particularly affects data with extremely long retention periods and statutory retention requirements.

47 Not to be confused with the principle of the blockchain.

48 M. Mosca and M. Piani, *Quantum Threat Timeline Report 2025*, Global Risk Institute, 2026.

IOSCO discussions with the industry representatives confirmed the belief that once CRQCs become available, attackers could decrypt previously collected data, disrupt systems through fraudulent authentication, and manipulate digital records and contracts by forging digital signatures. The expected timeline for such capabilities remains uncertain, but conservative estimates assume that relevant quantum computers could emerge in the 2030–2035 timeframe. This creates a near-term urgency for PQC migration, given the lead time required to transition systems and the long-term sensitivity of data.

In the banking sector, for example, this affects the lending stage of the value chain – such as construction financing or syndicated loans with terms spanning several decades – where sensitive customer and corporate data is exchanged. Similarly, virtual data rooms in the mergers and acquisitions sector contain highly sensitive acquisition plans and patents. Decrypting this data retroactively in ten years' time could still cause significant economic damage. In the insurance industry – particularly in underwriting and portfolio management at life insurers and private health insurers – highly sensitive health data are processed. The confidentiality of this data must be maintained for decades, in some cases even beyond the insured individuals' lifetimes. The HNDL scenario poses an existential risk to reputation and data protection in this context. During recent IOSCO roundtables, some quantum experts highlighted that HNDL risk may be overstated, and trusted connections underpinning business operations and ecosystems present a more systemic concern. Thus, HNDL might be more relevant to cases where sensitive information that must remain confidential over an extended period is at stake.

A.3. Post-Quantum Cryptography, Crypto Agility, Quantum Key Distribution

Post-Quantum Cryptography

PQC can be defined as new cryptography methods and standards that have been developed to provide a secure and resistant environment against CRQC capabilities. As mentioned in the previous sections, the current cryptography standards used by market participants in capital markets will be vulnerable to a CRQC since this new computer will have the ability to solve complex mathematical problems and consequently break current cryptography algorithms. The goal of PQC is to develop cryptographic systems to be used in our global communication digital infrastructure, and that are secure against both CRQCs and classical computers.[49]

PQC would rely on algorithms and mathematical problems that would be nearly impossible, or extremely difficult for CRQCs to solve, as well as classical computers. Otherwise, in the absence of post-quantum cryptography, CRQCs would have the ability to break the protection currently provided by cryptography systems in our communications and many other applications that rely on cryptography. In other words, all secret symmetric keys and private asymmetric keys that are now protected using current public-key algorithms, as well as the information protected under those keys, will be subject to decrypted. This includes all recorded communications and other stored information protected by those public-key algorithms. Any information still considered to be private or otherwise sensitive will be vulnerable to decryption and modification.[50]

[49] L. Chen et al., *Report on Post-Quantum Cryptography*, United States NIST, 2016.

[50] W. Barker et al., *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, United States NIST, 2021.

PQC is intended to support a broad range of cryptographic functions across existing digital systems, whereas QKD, discussed below, has a narrower role focused on the secure distribution of cryptographic keys.

The NIST framework

The United States National Institute of Standards and Technology (NIST) has been developing and promoting standards for PQC. In 2016, NIST officially launched the PQC Standardization process with a Call for Proposals.[51] This initiative was designed to solicit, evaluate, and standardize cryptographic algorithms resistant to both CRQCs and classic computers, and to replace existing standards (like RSA and ECC) that will be vulnerable to attacks from CRQCs.

To date, NIST has released three principal PQC standards:[52]

(a) FIPS203: the Module-Lattice-Based Key-Encapsulation Mechanism,

(b) FIPS204: the Module-Lattice-Based Digital Signature Algorithm, and

(c) FIPS205: the Stateless Hash-Based Signature Algorithm.

No cryptography scheme can be proven to be permanently unbreakable and NIST continues to develop additional PQC standards and alternative algorithms.

Crypto Agility

Crypto agility is defined as *"[t]he capabilities needed to replace and adapt cryptographic algorithms in protocols, applications, software, hardware, firmware, and infrastructures while preserving security and ongoing operations"*.[53] In other words, crypto agility refers to the ability to rapidly update and adapt cryptography systems without business disruption. In public blockchains, achieving crypto agility may require coordinated changes to protocol rules and adoption across decentralized participants, making cryptographic transitions more complex.

Cryptographic algorithms are widely used throughout organizations and are often implemented differently across applications, systems, and technologies. As highlighted in the above definition, cryptography is embedded in communication protocols, software applications, hardware devices, firmware, and infrastructures. Consequently, implementing crypto agility is not a single technical exercise but a broad enterprise effort that aims to address all cryptographic systems. This enterprise effort requires a comprehensive inventory of cryptographic use, a coordinated governance effort, and the involvement of multiple stakeholders including IT and cybersecurity architects, software and standards developers, hardware designers, and management.[54] Achieving crypto agility therefore demands both a holistic view of cryptography across the organization and a consistent approach to managing cryptographic transitions over time. From a defense-in-depth perspective, crypto agility helps ensure that the compromise or obsolescence of a particular cryptographic algorithm does not leave systems dependent on a single security mechanism, thus facilitating the timely deployment of replacement or complementary cryptographic controls.

[51] United States NIST, *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*, 2017.

[52] United States NIST, *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, 2024.

[53] United States NIST, *Glossary*.

[54] E. Barker et al., *Considerations for Achieving Crypto Agility*, United States NIST, 2025.

Achieving crypto agility would also demand coordination with third-party providers since transitions to PQC require interoperability across software, hardware, services, and communication protocols supplied by multiple vendors. This may require institutions to engage proactively with suppliers, including reviewing contractual arrangements and service expectations to ensure that vendors can support PQC migration and related cryptographic updates. A resilient technology supply chain is essential for crypto agility, as it allows organizations to update or replace cryptographic components without overhauling entire systems. Conversely, delays or inconsistencies in vendor readiness could complicate migration efforts and potentially create operational and business continuity challenges where critical systems depend on third-party products or services.

Market participants should understand that migration to new quantum-resistant cryptography standards is not a one-time event. Those standards will keep evolving and cryptography systems need to be designed to accommodate and implement future changes quickly and at low cost. NIST has developed a maturity model to help organizations assess and improve their level of crypto agility.[55]

To summarize, efficient crypto agility implementation would initially require organizations to maintain comprehensive cryptographic inventories to understand where cryptography is used across their systems, applications, and infrastructures. Systems would need to be designed with the expectation that cryptographic standards and algorithms will evolve over time, allowing cryptographic components to be replaced or adapted without operational disruption. Finally, organizations need to rely on strong governance, policies, and risk management processes that support consistent and coordinated cryptographic transitions across the organization.

PQC migration is not simply a technological upgrade but an enterprise-wide transformation requiring complete visibility over cryptographic use and close coordination across systems, applications, and third parties. The migration involves updating a wide variety of systems and technologies, each with unique needs and constraints, making the process highly complex. This extends beyond technology vendors and includes third parties that operate, host, or process systems and data on behalf of an organization, such as providers of software-, platform- and infrastructure-as-a-service offerings. The preparedness of these third parties for PQC migration may be as important as that of the institution itself, particularly where critical operations or sensitive data depend on externally managed services. As a result, PQC migration may require enhanced third-party risk-management activities, including due diligence, ongoing engagement, assessment of migration readiness, and monitoring of dependencies across critical service providers. The migration involves updating a wide variety of systems and technologies, each with unique needs and constraints, making the process highly complex.

To support PQC, every layer of the technology architecture must be adapted or upgraded. This highlights the importance of crypto agility to achieve this transition. Moreover, ensuring interoperability between old and new cryptographic methods, especially when using hybrid approaches, increases technical complexity and can introduce additional technical, operational, and security challenges.

Quantum Key Distribution

Quantum cryptography (not to be confused with *post*-quantum cryptography) uses principles of quantum mechanics (like superposition and entanglement) to secure data. Quantum cryptography employs quantum devices, such as sensors capable of recording individual particles of light

[55] Barker et al., *Considerations for Achieving Crypto Agility*, section 6.5.

(photons), to protect data from an adversarial attack.[56] It is considered resistant to quantum computing attacks.[57]

QKD is the advanced application of quantum cryptography. More specifically, it can be defined as: *"a technology, based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. Sending randomly encoded information on single photons produces a shared secret that is a random string and the probabilistic nature of measuring the photon state provides the basis of its security."* [58]

QKD aims to securely exchange encryption keys and can detect attempts to intercept communications by leveraging the principles of quantum physics. In contrast, classical cryptography and PQC rely on the difficulty of solving complex mathematical problems, with PQC specifically designed to remain secure against attacks from quantum computers.

While quantum cryptography technologies such as QKD offer promising capabilities, their implementation remains limited due to infrastructure and operational challenges. The main issue is that imperfections in how quantum states are prepared, transmitted, and measured make it hard to tell if errors are caused by normal system flaws or by eavesdropping. Because of this, QKD systems require extremely high performance to ensure security. These technical challenges affect the speed, distance, cost, and overall security of QKD.

Due to these unresolved issues, PQC is generally considered a more cost-effective and practical response to quantum cryptographic risks.[59] PQC migration is consistently presented as preferable to quantum cryptography technologies for most use cases, given its broader applicability and compatibility with existing digital systems. By contrast, QKD is designed specifically for the secure distribution of cryptographic keys and requires specialised infrastructure. It may therefore complement PQC for selected high-security communication channels, but is not a substitute for broader PQC migration. NIST has already released PQC standards that can be adopted.[60]

B. Vulnerabilities in Financial Institutions' Information and Communications Systems and Public Blockchains

B.1. Financial Institutions' Information and Communications Systems

The operational resilience of financial institutions (**FIs**) and financial market infrastructures (**FMIs**) depends in part on the integrity of cryptographic controls embedded across their systems, networks, and operational processes. Cryptography should therefore be understood not simply as a collection of individual algorithms, but as a system-wide dependency supporting critical financial

56 United States NIST, *What is Quantum Cryptography?* 2025.

57 FS-ISAC, *Building Cryptographic Agility in the Financial Sector*, 2024.

58 United States NIST, *Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration*, 2009.

59 United States National Security Agency, *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*.

60 United States NIST, *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, 2024.

services, including payment processing, securities clearing and settlement, collateral management, and supervisory reporting. It provides assurances relating to the confidentiality and integrity of data, the authentication of users, devices and transactions, access control, and non-repudiation.[61]

These assurances generally rely on a combination of symmetric and asymmetric cryptography. Symmetric algorithms are commonly used to encrypt large volumes of data, while public-key algorithms such as RSA and ECC support digital signatures, authentication, and the establishment of shared keys for secure communications. A CRQC could compromise the mathematical assumptions underpinning RSA and ECC, potentially allowing an attacker to derive private keys, re-create digital signatures or compromise the exchange of symmetric keys used to secure financial data and communications.[62]

The resulting exposure is not confined to particular algorithms or individual applications. Cryptographic dependencies extend across the technology stack, including the hardware, firmware, operating systems, applications, networks, and security processes supporting FIs and FMIs. They encompass secure communications and system access; identity and access management; the signing, authorization and secure exchange of transactions and information; and the protection of cryptographic keys, software, databases, backups and system logs.[63] Many of these dependencies are deeply embedded in legacy systems and operational processes and may require separate adaptations during migration.

PKI, including digital certificates and certificate authorities, forms a foundation for authentication across financial markets. Certificates are used to control access to trading venues, payment and settlement systems, financial messaging networks, regulatory reporting portals, cloud services, and internal enterprise environments. Hardware security modules (HSMs) and cloud-based key-management services are also used to generate, store, and manage the cryptographic keys on which these functions depend.[64]

The risk therefore extends beyond the compromise of individual certificates or cryptographic keys. Authentication and key-management ecosystems are highly interconnected, and the same certificate hierarchy, identity provider, cryptographic library, HSM environment, cloud key vault or vendor product may support multiple business services. This creates common points of dependency: weaknesses or disruption affecting a shared cryptographic component could impair otherwise separate systems or processes. The compromise of digital-signature mechanisms could also permit unauthorized system access or allow malicious software or system updates to appear authentic, creating vulnerabilities in operational resilience as well as information security.[65]

At the level of financial operations, weakened cryptographic assurance could affect confidence in the authenticity and integrity of payment instructions, settlement messages, collateral movements,

61 Auer et al., *Quantum-readiness for the financial system*.

62 Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*.

63 Auer et al., *Quantum-readiness for the financial system*. Examples include TLS, virtual private networks (VPNs), Secure Shell (SSH), application programming interface (API) security, secure file-transfer protocols, and message and machine-to-machine authentication; privileged access management, federated identity, device credentials and service accounts; digital signatures, transaction authorization, regulatory submissions and secure messaging; and database and backup encryption, firmware, code and container signing, log-integrity controls and secure software-update mechanisms.

64 Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*.

65 Auer et al., *Quantum-readiness for the financial system*.

reconciliations, and regulatory submissions. The wider consequences would depend on the affected systems, the duration and extent of the disruption, and the availability of operational alternatives. For FMIs in particular, uncertainty over the authenticity of transactions or settlement instructions could impair the reliable processing of financial activity and, in more severe circumstances, affect liquidity and market functioning.[66]

These interdependencies also complicate migration. Changes to cryptographic algorithms may require corresponding updates to protocols, certificates, software libraries, authentication systems, hardware and operational processes. Coordination may be required among certificate issuers, financial institutions, FMIs, network and technology providers, and other stakeholders. Differences in system architecture, continued reliance on legacy technologies, and the availability of vendor upgrades may therefore affect the sequencing and duration of migration.[67] Uneven migration could also leave vulnerabilities at points of interconnectedness, even where some market participants have completed their own transition.

Payment and settlement systems illustrate the breadth of these dependencies. Cryptographic controls are applied at multiple stages of transaction processing to authenticate participants, verify the origin and integrity of payment messages, protect information in transit, and support non-repudiation. Public-key algorithms are commonly used for participant authentication, initial key exchange, and digital signatures, while symmetric algorithms support the encryption of high-volume messages. A compromise of the public-key components could consequently undermine trust in payment instructions and financial communications even where the underlying transaction data are encrypted using symmetric cryptography.[68] In practice, the security of the overall system depends on both components: the compromise of public-key mechanisms used for authentication, key exchange, or digital signatures may enable impersonation, message forgery or other attacks, despite the continued strength of the symmetric encryption protecting the transaction content.

BIS Project Leap, an experiment conducted by the BIS Innovation Hub to assess the feasibility of implementing post-quantum cryptography in cross-border payment systems, demonstrated that post-quantum signatures could be implemented and validated within a payment-system test environment. It also showed that migration affects multiple interacting components operated by central banks, network service providers, and technology vendors. The experiment required software reconfiguration, updated cryptographic libraries and connectors, and new signature-verification components. Existing configurations did not support all intended hybrid arrangements without further development, while certificate-based validation and HSM integration remained areas for additional testing.[69]

Digital signatures are also used more broadly to authenticate electronic transactions, regulatory submissions, contractual records, and settlement instructions and to support non-repudiation. The associated risk differs from HNDL attacks against encrypted data. HNDL concerns information intercepted before a cryptographically relevant quantum computer becomes available and decrypted subsequently, whereas signature forgery generally requires access to such a computer

66 BIS Innovation Hub, *Project Leap: Quantum-proofing payment systems*, 2025.

67 Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*; BIS Innovation Hub, *Project Leap*.

68 BIS Innovation Hub, *Project Leap*.

69 BIS Innovation Hub, *Project Leap*.

when the forgery is performed. Nevertheless, earlier migration may be relevant where digital signatures, authenticated records or devices must remain valid over extended periods.[70]

The transition to PQC itself may introduce operational challenges. Post-quantum algorithms can require larger keys and signatures, greater processing and memory capacity, and adaptations to protocols and key-encoding formats. Project Leap demonstrated the feasibility of processing payment messages using post-quantum signatures, but also identified differences in verification performance and the need for further testing across hardware, certificates, and other system components. These considerations are particularly relevant to high-volume or latency-sensitive FMIs and will affect the selection, testing, and sequencing of migration approaches.[71]

B.2. Blockchains

The exposure of public blockchain systems to quantum-related cryptographic risks, and the challenges associated with PQC migration, can be considered across different architectural layers. At the base layer, cryptographic mechanisms support transaction authorization, identity, consensus, and settlement. Applications and scaling arrangements may introduce further dependencies through smart contracts, bridges, wallets, and transaction-processing mechanisms. Although the distinction between Layer 1 and Layer 2 does not apply uniformly across all blockchain architectures, it provides a useful framework for considering where cryptographic vulnerabilities arise and how migration requirements may differ.

While this section focuses on public blockchains, many of the underlying cryptographic risks are also relevant to permissioned and private distributed ledger systems. The primary difference is not the nature of the cryptographic vulnerability itself, but the governance, migration, and operational arrangements available to participants.

Layer 1

Layer 1 (L1) blockchain systems face particular migration challenges because cryptographic primitives are embedded in transaction formats, account structures, consensus processes, and validation rules. Current public L1 systems (such as Ethereum, Solana, and Tron) rely heavily on ECC for identity verification and transaction validation. ECC provides efficient, compact signature footprints, typically 64 bytes per signature, whereas NIST-standardized post-quantum signature schemes require substantially larger keys and signatures and greater computational resources.[72] For example, signatures produced using ML-DSA-44 (FIPS 204) are approximately 2,420 bytes, representing an increase of roughly 35 to 40 times compared to commonly used ECC signature schemes. As a result, migrating to post-quantum signature schemes could affect throughput, bandwidth, storage, block propagation, and other aspects of protocol operation.

This increased data load materially impacts the *core state transition capacity* of an L1 system, which is the maximum rate at which a blockchain can process, validate, and transmit incoming data. This

[70] Auer et al., *Quantum-readiness for the financial system*

[71] Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*; BIS Innovation Hub, *Project Leap*.

[72] T. Mallick et al., *Quantum disruption: An SOK of how post-quantum attackers reshape blockchain security and performance*, 2025.

capacity is strictly constrained by node bandwidth and block size limits, so expanding signature data directly degrades network throughput, and consequently network performance.

Integrating PQC primitives directly into an L1 system creates a substantial trade-off; while enhancing cryptographic resilience, it creates significant on-chain network congestion, increases node storage requirements, and spikes transaction fees. For example, evidence from Solana's quantum-resistant testnet demonstrated throughput degradation of approximately 90% when substituting ECC with post-quantum signatures.[73]

Further, L1 systems face critical operational vulnerabilities during a PQC migration due to their decentralized network and governance architectures that create challenges for uniform collective action. Unlike traditional, centrally managed financial software that can deploy security patches uniformly overnight, L1 systems depend on the independent, voluntary coordination of thousands of geographically dispersed validators and node operators to migrate at the same time. Given that cryptographic primitives are embedded in the foundational transaction structures and consensus rules of L1 systems, replacing such cryptographic primitives requires hard forks of L1 systems.

Decentralized networks also lack an enforcement mechanism to mandate fast software adoption, making any post-quantum migration slow and fragmented. Uneven migration could leave residual exposures after a network introduces quantum-resistant functionality. Accounts, smart contracts, and other arrangements controlled through quantum-vulnerable keys could remain exposed until the relevant assets and control mechanisms are migrated. A sufficiently capable attacker could derive private keys from exposed public keys and use them to impersonate withdrawal, transaction, or governance signatures, even after other parts of the network have adopted PQC. As a result, the security of the network may continue to be constrained by the least-migrated components until migration reaches a sufficiently broad level across users, assets, and applications.

The degree of exposure also depends on the transaction and address model used by each network. In some systems, a public key is concealed until an address is used. Once a transaction is broadcast and the public key becomes visible, a sufficiently capable quantum attacker could attempt to derive the corresponding private key and issue a conflicting transaction before the original transaction is confirmed. This is sometimes described as an “on-spend” attack because the attacker must act within the transaction-confirmation window. By contrast, an “at-rest” attack may target assets associated with public keys that remain exposed for longer periods. The feasibility of such an attack depends on several factors, including the capabilities of the attacker, the time required to derive the key, and the time available before transaction confirmation or finality. Account-based systems in which public keys are more readily recoverable may present a broader population of exposed accounts. Assessments of quantum vulnerability should therefore consider not only the signature scheme, but also whether and when public keys are exposed, whether addresses are reused, and the time available before transaction finality.[74] Dormant or abandoned assets associated with exposed public keys may present particular migration challenges where the relevant holders cannot be identified or are unable to transfer the assets to quantum-resistant addresses.

[73] M. Nijkerk, *Solana's quantum-threat readiness reveals harsh tradeoff: security vs speed*, CoinDesk, 2026.

[74] A. Mutha and J. Sandu, *Literature review of the effect of quantum computing on cryptocurrencies using blockchain technology*, 2025.

Layer 2

Layer 2 (L2) scaling solutions process or aggregate transactions outside their host L1 networks to achieve high throughput but remain cryptographically tethered to their host L1 networks. By design, L2 systems may use cryptographic mechanisms that differ from those of the host network, but their end-to-end security can still depend on L1 settlement contracts, bridge mechanisms, proof-verification components, data-availability arrangements, and governance or upgrade keys. A quantum vulnerability affecting one of these dependencies could therefore undermine relevant aspects of the L2 system, even where other L2 components use quantum-resistant cryptography.[75]

The nature of this exposure varies across L2 architectures. For rollups, two broad models are particularly relevant: optimistic rollups, which allow proposed state transitions to be challenged through fraud proofs, and zero knowledge rollups, which submit validity proofs that state transitions have been executed correctly.

(a) **Fraud Proofs**: Optimistic rollups generally treat proposed state transitions as valid unless they are successfully challenged within a defined period (typically seven days for Ethereum-based systems). Their security therefore depends on the ability of an honest validator to detect an invalid transition and submit a fraud proof before that period expires. Quantum computers can forge digital signatures, enabling attackers to submit fraudulent transaction sequences or maliciously censor honest validators during these critical multi-day dispute windows.

(b) **Validity Proofs**: Zero knowledge rollups (such as zkSync and StarkNet) rely on cryptographic proofs to demonstrate the correctness of off-chain state transitions before settlement on L1. The quantum exposure of the proof mechanism depends on its construction. Many currently used Succinct Non-Interactive Arguments of Knowledge (SNARK) systems rely on ECC and could therefore require modification or replacement in a post-quantum environment. Scalable Transparent Arguments of Knowledge (STARK) systems rely primarily on hash-based constructions that are resistant to quantum attacks. However, their security still depends on the quantum-adjusted strength of the underlying hash functions and on appropriate parameters.[76]

The resilience of either type of rollup also depends on components beyond the proof mechanism itself. A quantum-resistant proof system would not provide end-to-end protection if the L1 verifier contract, settlement bridge, asset-control mechanism, or governance keys remained dependent on quantum-vulnerable cryptography. The potential consequences would depend on the affected component and could include interference with settlement, withdrawals, proof verification, or protocol upgrades.

PQC migration will therefore require coordination between L1 and L2 ecosystems. L2 operators can strengthen their own proof systems, transaction-signature mechanisms, and governance arrangements, but cannot independently ensure end-to-end resilience while relying on vulnerable L1 components. Migration planning must account for dependencies among L1 protocol developers,

[75] H. Khodaiemehr, K. Bagheri, and C. Feng, *Navigating the quantum computing threat landscape for blockchains: A comprehensive survey*, *Computer Science Review*, Vol. 59 (2025), 100846.

[76] R. Babbush et al., *Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations*, 2026.

L2 operators, bridge providers, sequencers, validators, application developers, and users, as well as the sequencing of upgrades across these components.

Historical Data and Privacy Risks

Distributed ledger systems may also present distinct HNDL risks because ledger data are replicated across network participants and may remain permanently available. An adversary could retain a copy of information protected using quantum-vulnerable cryptography and attempt to access the underlying data once CRQCs become available. Even where a network subsequently migrates to PQC, that migration cannot remove copies already held by third parties or retrospectively protect information that was previously collected.[77]

This risk is distinct from the potential compromise of transaction signatures or future transaction validation. HNDL does not itself affect ownership or the validity of transactions already recorded on the ledger, but may affect encrypted information used or stored by blockchains or associated applications. Migration to quantum-resistant signatures can protect the authenticity and integrity of future activity, whereas HNDL concerns the continuing confidentiality of historical data. Its significance will depend on whether the ledger contains encrypted or otherwise cryptographically protected information that must remain confidential over an extended period. The persistence and replication of ledger data may make such exposure particularly difficult to remediate once the information has been collected.

[77] J. Mascelli and M. Rodden, *"Harvest now, decrypt later": Examining post-quantum cryptography and the data privacy risks for distributed ledger networks*, Board of Governors of the Federal Reserve System, 2025.

5. Implications for Investor Protection, Market Integrity, and Financial Stability

A. Overview

Development and adoption of quantum computing use cases in financial services could have implications for investor protection, market integrity, and financial stability. The implications arising from these use cases remain prospective, given that the applications considered in this section are largely at the research or experimental stage. Their nature and significance will depend on how quantum approaches are incorporated into financial products, services, and decision-making processes; the extent to which institutions rely on specialized providers; and whether existing governance, validation, and regulatory frameworks remain appropriate as the technology develops.

Separately, the development of quantum computing could create significant cybersecurity risks, given their potential to undermine the cryptographic protections embedded across digital financial services and the wider digital economy. The financial sector relies extensively on cryptography to protect the confidentiality and integrity of data, authenticate users, institutions, and transactions, control access to systems, and support non-repudiation. A CRQC would compromise widely used forms of public-key cryptography, potentially allowing encrypted information to be accessed, private keys to be derived, and digital signatures or certificates to be forged.[78] The consequences would depend on the affected cryptographic functions and systems but could extend across investor data, communications, authentication mechanisms, transaction processing, and market infrastructure.

Three principal forms of exposure arise. First, sensitive information encrypted using quantum-vulnerable public-key algorithms could be accessed by an adversary with a CRQC. This includes information collected before such capabilities become available through HNDL attacks.[79] Second, the compromise of digital signatures and certificates could permit unauthorized transactions, impersonation, or access to systems and undermine confidence in the authenticity and integrity of financial activity.[80] Third, where affected cryptographic mechanisms support critical institutions, shared infrastructure, or interconnected market processes, the resulting operational disruption could have wider implications for market integrity and financial stability.[81]

78 Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*.

79 G7 Cyber Expert Group, *Statement on Planning for the Opportunities and Risks of Quantum Computing*, 2024; Auer et al., *Quantum-readiness for the financial system*.

80 Auer et al., *Quantum computing and the financial system*; Auer et al., *Quantum-readiness for the financial system*.

81 Auer et al., *Quantum-readiness for the financial system*; G7 Central Bank Quantum Technologies Working Group, *Preparing for Quantum Technologies*.

B. Investor Protection

Risks to investor protection may emerge from the deployment of quantum computing use cases. As explored earlier in this section, quantum approaches to machine learning could eventually be incorporated into investor or consumer-facing products and services, including robo-advisory tools, credit-scoring models, fraud-detection systems, algorithmic trading strategies, investment recommendation engines, and other automated decision-making systems. It is still unclear the extent to which the integration of quantum approaches into these use cases will affect outputs and how institutions might explain outcomes to consumers. In this sense, quantum computing use cases may increase complexity, reduce transparency, and prove difficult to validate, resulting in investors being less informed or capable of challenging decisions that impact them. To mitigate these risks before they materialize, supervisors and regulatory entities may need to build technical expertise and revisit model risk frameworks to account for the opacity and hardware-dependency of quantum models.

Additionally, as quantum computing use cases mature from theoretical research and experimentation, authorities may also need to monitor how firms describe their capabilities to investors, clients, and the market. Given both the technical complexity and immaturity of the technology there are potential risks of "quantum washing", where institutions may overstate the role, maturity, or performance of quantum computing use cases across products or services. Investors may face challenges in distinguishing between use cases that demonstrate robust evidence of quantum advantage and use cases that utilize quantum terminology for marketing purposes. As the technology matures, further consideration may be needed regarding how existing disclosure and conduct frameworks apply to claims relating to quantum computing capabilities and performance.

For investors, a quantum-enabled compromise of cryptographically-secured information could result in the disclosure of personal and financial information, the compromise of communications or authentication credentials, and increased exposure to fraud and unauthorized transactions.[82] HNDL creates a distinct long-term confidentiality risk because information intercepted today could be accessed later if it remains sensitive when CRQCs become available.[83]

Investor exposure could also arise during migration. Financial institutions will need to identify vulnerable cryptographic dependencies, coordinate upgrades with technology and service providers, and implement changes across interconnected systems while maintaining operational continuity.[84] Delayed, incomplete, or poorly coordinated migration could leave gaps in protection or create disruption as institutions operate with a combination of legacy and post-quantum systems.

C. Market Integrity

The uneven adoption of quantum use cases could also create asymmetries among market participants. Survey responses already indicate that the early experimentation on quantum

82 G7 Cyber Expert Group, *Statement on Planning for the Opportunities and Risks of Quantum Computing*.

83 Auer et al., *Quantum-readiness for the financial system*.

84 Auer et al., *Quantum-readiness for the financial system*; Cross Market Operational Resilience Group, *Guidance for Post-Quantum Cryptography*, 2025; G7 Cyber Expert Group, *Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector*, 2026.

computing use cases predominantly occurs in larger institutions. As the technology matures, these institutions may be better positioned to adopt and benefit from quantum use cases compared to others with resource constraints who may face competitive disadvantages from barriers to entry and delayed adoption.

Such competitive asymmetries do not amount to market integrity considerations in and of themselves. Competitive advantages are a feature of markets and may even prove transient as access to quantum use cases broadens. However, consideration should be given to whether the scale or concentration of capabilities affects the ability of market participants to meaningfully compete. More broadly, uneven adoption of quantum-resistant technologies could create negative externalities for slower adopters, particularly if attackers concentrate on participants that continue to rely on quantum-vulnerable systems or cryptography.

Equally, if quantum use cases do mature towards market deployment, it may become more difficult to understand how outputs have been produced and whether use cases act as intended. This could be further complicated by the variety of quantum computing hardware platforms and the extent to which current validation methodologies remain adequate. In the near term, classical approaches may provide a suitable benchmark. However, if quantum computing applications are deployed precisely because they produce materially different outputs, classical benchmarks may not constitute a meaningful standard.

These challenges extend towards market integrity considerations where poorly understood outputs expand beyond individual applications to impacting market activity. It is therefore important that governance arrangements co-evolve with quantum computing use cases as they mature from experimentation, proof-of-concept activities, and pilot deployments towards market deployment. In this process firms will need to establish clear accountability and validation mechanisms, while regulatory authorities will need to attain sufficient technical capabilities to assess use cases, understand their limitations, and monitor their impact on market activity.

Financial markets rely on cryptography to authenticate participants and instructions, protect communications and transactions, and preserve the integrity of trading, clearing, and settlement processes.[85] If the authenticity of transactions, instructions, or system credentials could no longer be reliably established, market activity could become disputed and confidence in the operation of market functions could weaken.

The interconnected nature of financial markets amplifies these dependencies. Trading, clearing, and settlement processes involve financial institutions, FMIs, technology providers, and other third parties. The security of shared market functions therefore depends not only on the preparedness of individual institutions, but also on the readiness of the wider ecosystem.[86] Uneven migration could leave vulnerabilities at points of interconnectedness even where some market participants have completed their own transition.

Loss of cryptographic assurance would not necessarily reverse transactions that have already achieved finality. However, compromise of relevant private keys, certificates, or control mechanisms could enable forged transactions or instructions, unauthorized transfers, manipulation of

[85] BIS Innovation Hub, *A Strategic Framework for Quantum-Cryptography in FuSSE*, 2024; Auer et al., *Quantum computing and the financial system*.

[86] Auer et al., *Quantum-readiness for the financial system*; G7 Cyber Expert Group, *Statement on Advancing a Coordinated Roadmap*.

subsequent activity, or disputes over whether activity was validly authorized.[87] In blockchain-based systems, alteration of historical ledger records would additionally require the attacker to overcome the relevant consensus and finality arrangements.

D. Financial Stability

Financial stability considerations may arise mainly from the concentration of quantum capabilities among a small number of third-party providers. Where multiple institutions rely on the same providers, operational failures or service disruptions could create common points of dependency, and in turn, increase the potential for disruption to affect a number of institutions. While this echoes existing considerations around concentration in critical third parties, the risks could be amplified by the replaceability of highly specialized quantum capabilities, and the difficulties institutions may face in transitions between different hardware modalities.[88] Financial stability considerations may also arise where uneven migration leaves vulnerabilities at points of interconnectedness, even where some market participants have completed their own transition.

Financial stability implications could also arise where quantum-enabled cryptographic compromise affects critical institutions, shared infrastructure, or services on which multiple participants depend. A compromise affecting common communications, payment, clearing, or settlement systems could create simultaneous disruptions across interconnected institutions. Shared certificate hierarchies, key-management services, software libraries, and technology providers could also create common points of dependency.[89]

Recovery could be particularly complex if institutions become unable to establish which credentials, instructions, or transactions remain trustworthy. Restoring operations may require not only replacing compromised keys and algorithms but also validating previously processed activity, re-establishing trusted identities, and determining when affected systems can safely reconnect to counterparties and shared infrastructure. Where critical market functions are involved, uncertainty over the authenticity of activity or the integrity of restored systems could prolong disruption and increase its wider effects.[90]

87 Auer et al., *Quantum computing and the financial system*; Babbush et al., *Securing elliptic curve cryptocurrencies*.

88 G7 Central Bank Quantum Technologies Working Group, *Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants*, 2026.

89 Auer et al., *Quantum-readiness for the financial system*; G7 Central Bank Quantum Technologies Working Group, *Preparing for Quantum Technologies*.

90 Auer et al., *Quantum-readiness for the financial system*.

6. Jurisdictional Quantum Preparedness and Migration Measures

A. Overview

Jurisdictions have begun adopting measures that establish expectations or requirements for financial institutions to prepare for the cybersecurity implications of quantum computing, particularly PQC migration. These measures appear in sectoral initiatives, cybersecurity frameworks, critical infrastructure guidance, and broader national quantum transition programs.

Some initiatives apply specifically to financial institutions or financial market participants. Examples include the Monetary Authority of Singapore's advisory to financial institutions,[91] the Bank of Israel's letter to banking corporations and payment service providers,[92] and the G7 Cyber Expert Group's roadmap for the financial sector.[93]

Other initiatives apply more broadly to private-sector organizations and critical infrastructure operators. Examples include Australia's guidance on planning for post-quantum cryptography, the European Union's coordinated roadmap for the transition to PQC,[94] India's Quantum Safe Ecosystem program,[95] and the United Kingdom's PQC migration timelines.[96]

A further category of initiatives applies primarily to government departments, public-sector entities, and regulatory authorities. Examples include the United States' federal PQC migration requirements[97] and the Government of Canada's roadmap for migrating non-classified IT systems to PQC.[98]

91 Monetary Authority of Singapore, *Advisory on Addressing the Cybersecurity Risks Associated with Quantum*, 2024.

92 Bank of Israel, *Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities*, 2025.

93 G7 Cyber Expert Group, *Statement on Advancing a Coordinated Roadmap*.

94 EU's NIS Cooperation Group – PQC Workstream, *A coordinated implementation roadmap for the transition to post-quantum cryptography*, European Commission, 2025

95 India Department of Science & Technology, *Implementation of Quantum Safe Ecosystem in India*, 2026.

96 United Kingdom National Cyber Security Centre, *Timelines for Migration to Post-Quantum Cryptography*, 2025.

97 United States Executive Office of the President, *Securing the Nation Against Advanced Cryptographic Attacks*, 2026.

98 Canadian Center for Cyber Security, *Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada*, 2025.

B. Common Elements of Quantum Preparedness Frameworks

B.1. Cryptographic Discovery and Risk Assessment

Across the initiatives, measures relating to cryptographic discovery and risk assessment typically involve identifying where cryptography is used, maintaining inventories of cryptographic assets, assessing quantum-related exposures, and classifying systems according to risk and criticality. The common objective is to establish visibility over cryptographic dependencies and provide a basis for future risk management and migration planning. These measures often extend beyond applications and communications systems to encompass infrastructure, business processes, products, data assets, and third-party services that depend on cryptographic technologies.

B.2. Governance and Transition Planning

Across the initiatives, measures relating to governance and transition planning typically involve establishing governance arrangements, assigning responsibilities, developing transition plans, identifying migration priorities, and implementing structured planning processes. Many initiatives adopt a phased approach linking discovery, prioritization, planning, implementation, and migration. This reflects the expectation that PQC migration will require coordination across technology, cybersecurity, risk, legal, procurement, operational resilience, and business functions. The literature similarly describes quantum preparedness as an enterprise-wide governance and operational resilience issue rather than a narrow technical exercise.

Several initiatives recommend a risk-based approach to prioritization that considers factors such as the criticality of systems and business functions, the sensitivity and longevity of data, and the complexity of migration activities. Initiatives emphasize the need to identify and prioritize systems supporting critical market functions, such as payment infrastructures, clearing and settlement platforms, and core trading systems, where a compromise of cryptographic security could have significant implications for financial stability and market confidence. Initiatives also highlight the importance of protecting highly sensitive and long-lived data, including regulatory records, contractual agreements, settlement instructions, and identity credentials, due to the risks associated with HNDL attacks.

Institutional size and operational capacity are important considerations in migration planning. Larger organizations often have the resources and regulatory obligations to launch comprehensive PQC migration programs, while smaller firms or certain market infrastructures may face unique challenges, including limited technical expertise, resource constraints, and reliance on third-party vendors.

Some jurisdictions have established more specific governance requirements or recommendations. For example, Israel requires banking corporations and licensed payment service providers, through a supervisory letter, to prepare formal preparedness plans that are reviewed by boards of directors and senior management before submission to the supervisor. India's Quantum Safe Ecosystem Task Force report similarly recommends leadership structures, governance arrangements, and cross-functional quantum risk management processes as part of broader transition planning.

B.3. Crypto Agility

Several initiatives include measures relating to crypto agility. These measures generally encourage organizations to assess whether existing systems and architectures can support future

cryptographic upgrades, identify barriers to migration, and incorporate flexibility for future cryptographic change into technology and operational planning.

The objective is to enable future replacement or upgrading of cryptographic algorithms, certificates, protocols, and related technologies without extensive redesign or disruption. Several initiatives identify crypto agility as an important capability supporting both the transition to PQC and future cryptographic modernization efforts.

B.4. Testing and Early Migration Activities

Several initiatives include measures relating to testing, experimentation, and early implementation. These measures include proof-of-concept exercises, validation of quantum-resistant technologies, pilot deployments, and limited implementation in selected environments before broader migration. The objective is to identify operational, interoperability, performance, and implementation issues before migration occurs at scale.

B.5. Third-Party Providers and Ecosystem Coordination

Critically, several initiatives include measures relating to third-party providers and ecosystem coordination. These measures recognize that preparedness depends not only on individual organizations but also on technology suppliers, cloud providers, operating system developers, software vendors, managed service providers, and shared infrastructures. Common measures include engagement with technology suppliers, assessment of supply chain dependencies, incorporation of PQC readiness into procurement and planning processes, and coordination across interconnected systems and infrastructures.

The G7 Cyber Expert Group places particular emphasis on coordination across financial institutions, financial market infrastructures, authorities, service providers, technology vendors, and standards bodies. This reflects the interconnected nature of financial systems and the dependence of migration efforts on common standards, vendor readiness, and coordinated implementation.

This emphasis is also consistent with the literature, which identifies third-party and vendor dependencies as a significant transition challenge because many cryptographic functions are embedded within externally supplied products and services.

C. Roadmaps and Migration Timelines

Several initiatives include structured roadmaps or indicative migration timelines. These generally follow a similar sequence of activities, beginning with cryptographic discovery and risk assessment, followed by planning and prioritization, implementation and migration of higher-priority systems, and broader migration activities.

The timelines differ in scope and level of prescriptiveness. Some initiatives establish milestones for discovery, planning, implementation, and migration, while others focus primarily on preparedness activities without specifying end-state migration objectives. Figure 3 summarizes selected supranational and national migration timelines identified in publicly available initiatives. The initiatives summarised in Figure 3 do not specifically address migration timelines for public blockchain systems; the distinct migration challenges presented by such systems are discussed separately in the Blockchains section.

Supranational	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
G7 Cyber Expert Group	🛡	🗋	○			◐					●
BIS Roadmap	🗋										
EU / NIS Cooperation Group		🛡🗋				◐					●
Selected national	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**	**2033**	**2034**	**2035**
Israel		🛡🗋									
Australia			🗋		○		●				
India					🛡🗋○		◐			●	
UK					🛡🗋○			◐			●

🛡 Discovery & Prioritization 🗋 Migration Planning ○ Commence Migration ◐ Migrate High-Priority Systems ● Migrate All Systems

FIGURE 3. Illustration of supranational and national post-quantum migration timelines applicable to financial institutions, across jurisdictions. The initiatives shown include both financial sector-specific measures and broader cybersecurity or critical infrastructure measures that may apply to private-sector firms, including financial institutions.

7. State of Quantum Preparedness

A. Overview

Quantum preparedness remains at an early and evolving stage across most jurisdictions, with member authorities and regulated firms generally at the awareness and planning phases of preparedness rather than implementation. Current efforts are primarily focused on understanding potential quantum-related risks, increasing organizational awareness, conducting preliminary assessments, and monitoring developments in PQC. More advanced activities, such as large-scale migration planning, migration testing, and deployment of quantum-resistant technologies, remain limited.

Quantum preparedness is increasingly understood as a complex organizational transition rather than a simple technical deployment. External stakeholders emphasized that quantum risk affects a wide range of functions, including technology, cybersecurity, operational resilience, procurement, legal, and risk management. Cryptographic asset inventories and migration roadmaps represent only part of the broader preparedness challenge, which also includes governance, prioritization, and long-term change management. Quantum preparedness depends not only on actions taken by individual firms, but also on the readiness and coordination of the wider ecosystem, including financial market infrastructures, technology providers, cloud service providers, and other market participants.

Survey responses similarly indicate that preparedness is shaped by a range of organizational, technical, and ecosystem-wide challenges. Among regulated firms, the most frequently identified challenges include dependence on third-party service providers, uncertainty regarding migration timelines, cost and resource constraints, and interoperability challenges (see Figure 4). Member authorities reported broadly similar concerns, although uncertainty regarding migration timelines appeared to be a less prominent challenge among authorities than among regulated firms (see Figure 5).

While awareness of quantum-related cybersecurity risks continues to increase and foundational preparedness activities are beginning to emerge, migration planning, technical implementation, and ecosystem coordination remain comparatively less developed. The following sections examine these themes through the various aspects of governance and organizational structures, technical preparedness, and ecosystem dependencies and coordination.

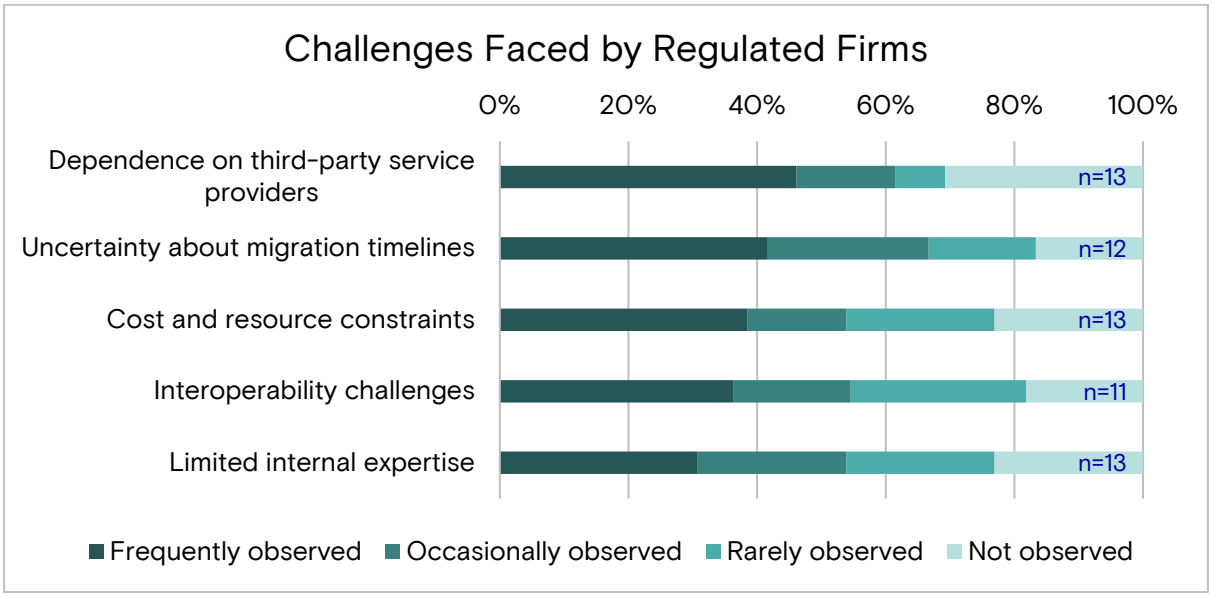

FIGURE 4. *Members' observations of challenges faced by regulated firms in supporting quantum preparedness.*

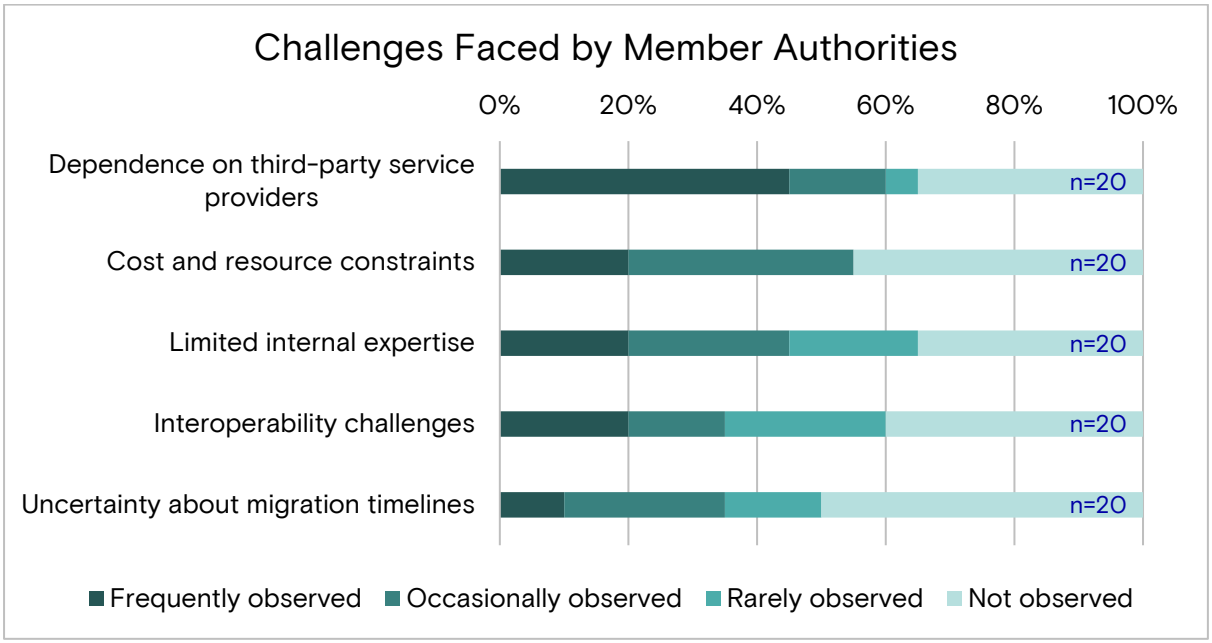

FIGURE 5. *Challenges faced by member authorities in supporting quantum preparedness.*

As per the feedback IOSCO gathered from quantum experts via industry outreach, migration should be understood as occurring in three phases: addressing cryptographic foundations, deploying post-quantum cryptography in priority use cases, and a clean-up phase where dependencies on vulnerable cryptography are eliminated. The clean-up phase is often overlooked, but is essential. It involves identifying and removing remaining uses of vulnerable cryptographic algorithms, retiring legacy systems and certificates, validating that PQC solutions have been consistently deployed across interconnected systems, and addressing residual cryptographic dependencies that may persist after initial migration efforts. Depending on the use case, organizations may also need to consider the treatment of

historical data, archives, backups, and long-retention records that remain protected by vulnerable cryptographic mechanisms, particularly where information is expected to remain confidential or accessible over extended periods.

B. Governance and Organizational Structures

Quantum preparedness is increasingly recognized as requiring governance and organizational structures that extend beyond traditional cybersecurity functions. Effective preparedness begins with establishing a clear understanding of quantum-related risks and building organizational consensus around the need for long-term cryptographic transition. Governance arrangements are viewed as a foundational element of preparedness, supported by clear ownership of migration activities, executive sponsorship, and coordination across technology, cybersecurity, operational resilience, legal, procurement, compliance, risk management, and other business functions. Organizations are also encouraged to establish cross-functional teams to oversee preparedness activities, identify priorities, and coordinate migration planning across the institution.[99]

Dedicated resources are needed to support transition efforts and build organizational capability. Training and upskilling programs help strengthen understanding of cryptography and emerging quantum-related challenges across relevant functions. Senior management support, organizational accountability, and sustained coordination across functions are important enablers of long-term preparedness and effective execution of what is expected to be a multi-year transition process.[100]

Uncertainty regarding the timing of cryptographically relevant quantum computers can further complicate preparedness efforts, requiring organizations to make planning and investment decisions despite uncertainty regarding future technological developments. At the same time, preparedness decisions are influenced not only by estimates of future quantum capabilities, but also by the time required to complete inventories, planning, testing, vendor engagement, and migration activities. For organizations with long-lived systems, sensitive data, or extensive technology estates, migration programs may require many years to complete, increasing the importance of early planning and sustained organizational commitment.

Reflecting similar themes, participants in the QWG's stakeholder engagement sessions emphasized that PQC migration should be viewed as a long-term organizational transformation program rather than a technology replacement exercise. Preparedness was described as involving governance, prioritization, coordination, and change management across multiple functions and over extended time horizons. Several participants observed that the central challenge is not simply predicting when cryptographically relevant quantum computers may emerge but ensuring that organizations can complete the transition within the available timeframe. Participants also noted that uncertainty regarding future developments, combined with competing cybersecurity, technology, and operational priorities, can make it difficult to sustain management attention and justify significant investments in preparedness activities. Some described a tendency towards "quantum-

99 Auer et al., *Quantum-readiness for the financial system*.

100 Auer et al., *Quantum-readiness for the financial system*; Europol, *Quantum Safe Financial Forum*, 2025.

procrastination", whereby organizations recognize the need to prepare but defer action in anticipation of clearer regulatory signals, greater technological maturity, or broader industry adoption. Participants further emphasized that responsibility for preparedness cannot rest solely with Chief Information Security Officers (CISOs) or technology functions, given the implications for procurement decisions, third-party relationships, operational resilience, business continuity, legal arrangements, and strategic planning. Effective preparedness therefore requires sustained senior management engagement and coordination across functions throughout the transition process.

Consistent with these observations, regulated firms are beginning to establish cross-functional structures to support preparedness activities, including working groups, task forces, dedicated teams, and management-level committees. However, these structures remain at an early stage of development and are unevenly observed across jurisdictions and organizations (see Figure 6).

Member authorities are also establishing governance structures to support quantum preparedness. Cross-functional working groups and task forces are the most frequently established arrangements, reported by approximately 55% of members. Dedicated teams are less common, with approximately 25% of members reporting that such structures have been established. Overall, many authorities continue to rely on existing organizational arrangements and resources to monitor developments and assess the implications for their regulatory and supervisory responsibilities (see Figure 7).

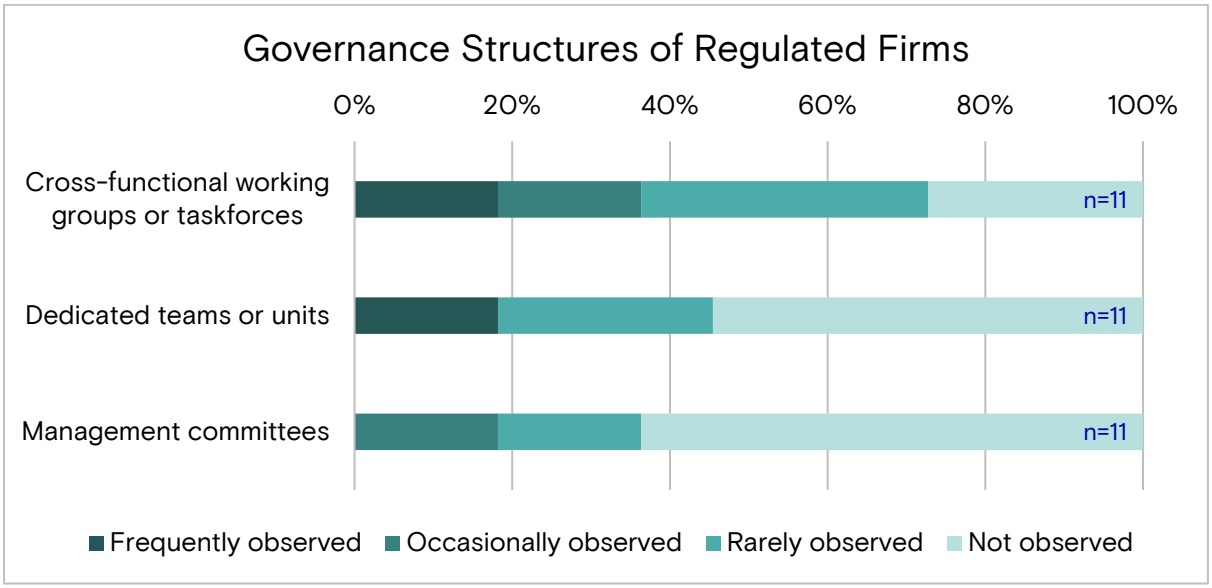

FIGURE 6. *Percentage of member authorities indicating the extent to which regulated firms have established various governance structures supporting quantum preparedness.*

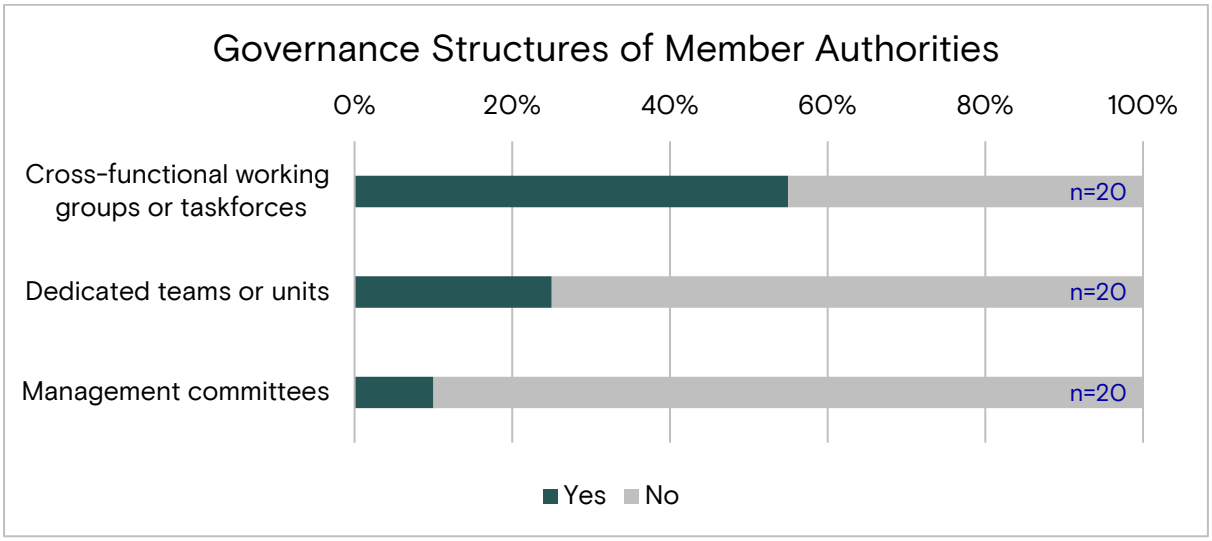

FIGURE 7. *Percentage of member authorities indicating the extent to which they have established various governance structures supporting quantum preparedness.*

C. Technical Preparedness

Effective migration depends on the development of several foundational technical capabilities. Cryptographic discovery, inventorying, and asset prioritization are widely recognized as essential prerequisites for quantum preparedness. A key early step is identifying where cryptography is deployed across the technology environment. This requires not only identifying cryptographic algorithms and implementations, but also understanding how they support business processes, interact with other systems, and depend on external providers. Comprehensive inventories and dependency mapping therefore provide the foundation for assessing exposure, identifying critical assets and systems, sequencing remediation activities, and developing migration plans.[101]

Crypto agility is similarly identified as a core preparedness objective, reflecting the ability to update cryptographic systems without significant redesign or operational disruption. Preparedness depends not only on the adoption of quantum-resistant cryptography, but also on the ability to implement future cryptographic changes efficiently and at scale. Organizations with strong crypto-agility capabilities are better positioned to replace vulnerable algorithms, respond to emerging threats, adopt new standards, and maintain security without extensive system redevelopment.

Conversely, systems in which cryptographic functions are tightly embedded within applications, protocols, or infrastructure may face greater cost, complexity, and operational risk during migration. Achieving crypto agility requires systems to be designed with modular cryptographic components, visibility over cryptographic dependencies, and governance

[101] W. Newhouse et al., *Migration to post-quantum cryptography: Preparation for considering the implementation and adoption of quantum-safe cryptography*, United States NIST, 2023; W. Newhouse et al., *Migration to post-quantum cryptography: Quantum readiness—Cryptographic discovery*, United States NIST, 2023; FS-ISAC Post-Quantum Cryptography (PQC) Working Group, *Infrastructure inventory technical paper*, FS-ISAC, 2023; Dutch General Intelligence and Security Service (AIVD), Centrum Wiskunde & Informatica, & Netherlands Organisation for Applied Scientific Research, *The PQC Migration Handbook*, 2024.

processes that enable cryptographic updates to be implemented efficiently across the technology environment.[102]

Technical preparedness also requires organizations to understand and manage the significant challenges associated with PQC migration. Unlike many technology upgrades, the transition is not viewed as a simple, one-time replacement of existing cryptographic algorithms. Cryptography is deeply embedded across applications, infrastructure, communications protocols, software libraries, hardware devices, and third-party services, meaning that migration may require broader and ongoing changes to system architectures, authentication mechanisms, certificate management arrangements, and operational processes. While post-quantum cryptographic algorithms are intended to provide equivalent security functions, they often introduce different implementation requirements and operational characteristics, including larger keys and signatures, higher computational demands, different communication patterns, and additional requirements for secure implementation. Depending on the algorithm and use case, organizations may need to address issues such as public-key validation, key management, protocol redesign, certificate handling, and the selection of supporting cryptographic functions. These differences can have implications for system performance, interoperability, latency, scalability, and operational resilience, potentially requiring significant modifications to systems and infrastructures. The challenges may be particularly acute in legacy environments where cryptographic functionality is embedded in hardware, firmware, or specialized systems that cannot readily accommodate new algorithms.[103]

Reflecting similar themes, participants in the QWG's stakeholder engagement sessions emphasized that PQC migration should not be viewed as a "drop-in replacement" exercise, but rather as a phased process involving discovery, initial and ongoing risk assessment, prioritization, planning, testing, implementation, and eventual retirement of vulnerable cryptographic solutions. Several participants highlighted the importance of understanding cryptographic dependencies, identifying critical assets, maintaining inventories, and embedding quantum readiness into existing technology lifecycle processes. They also noted that risk assessments may need to be periodically revisited as migration progresses, given the evolving understanding of quantum threats, cryptographic dependencies, technology roadmaps and implementation priorities.

Participants further emphasized that inventories should not be viewed as one-off exercises. As technologies, standards, and system architectures continue to evolve, maintaining visibility over cryptographic dependencies increasingly requires dynamic and continuously updated capabilities rather than static assessments. Emerging approaches such as cryptographic bills of materials (CBOMs), software bills of materials (SBOMs), and automated monitoring tools were identified as potential mechanisms for improving visibility and supporting ongoing risk assessment.

[102] E. Barker et al., *Considerations for Achieving Crypto Agility*, United States NIST, 2025; FS-ISAC PQC Working Group, *Current State (Crypto Agility) Technical Paper*, FS-ISAC, 2023.

[103] Newhouse, et al., *Quantum readiness—Cryptographic discovery*. United States NIST. For example, the United States government estimated that its migration of prioritized information systems to PQC between 2025 and 2035 could cost approximately US$7.1 billion. A significant portion of the overall estimate was due to the cost of replacing systems whose cryptographic algorithms were hardwired into the hardware or firmware and systems that lack the capacity to accept replacement cryptographic algorithms. United States Office of Management and Budget, *Report on Post-Quantum Cryptography*, 2024.

Survey responses indicate that most regulated firms remain in the early stages of technical preparedness for post-quantum cryptography (PQC) migration. Preparatory activities are concentrated in a relatively small number of areas, particularly cryptographic inventorying, awareness and training initiatives, identification and prioritization of assets for migration, and assessments of crypto agility capabilities. More advanced activities, such as migration testing, validation, implementation, and deployment of quantum-resistant technologies, are less commonly observed.

The survey results also indicate a clear progression in readiness activities. Measures relating to awareness, inventories, prioritization, and crypto agility are generally more advanced than implementation activities (see Figure 8). The descriptive responses similarly suggest that larger or more systemically important firms have begun their PQC migration journeys, although most remain at an early stage and continue to focus on planning, assessment, and preparedness rather than deployment.

Similar patterns can be observed among member authorities. Current activities are focused primarily on awareness-building, engagement with external stakeholders, assessments of crypto agility, inventorying exercises, and identification of assets requiring future migration. Practical migration activities, testing programs, and implementation exercises remain comparatively limited. These findings suggest that member authorities, like regulated firms, are currently concentrated on building preparedness and understanding exposures rather than undertaking large-scale migration activities (see Figure 9).

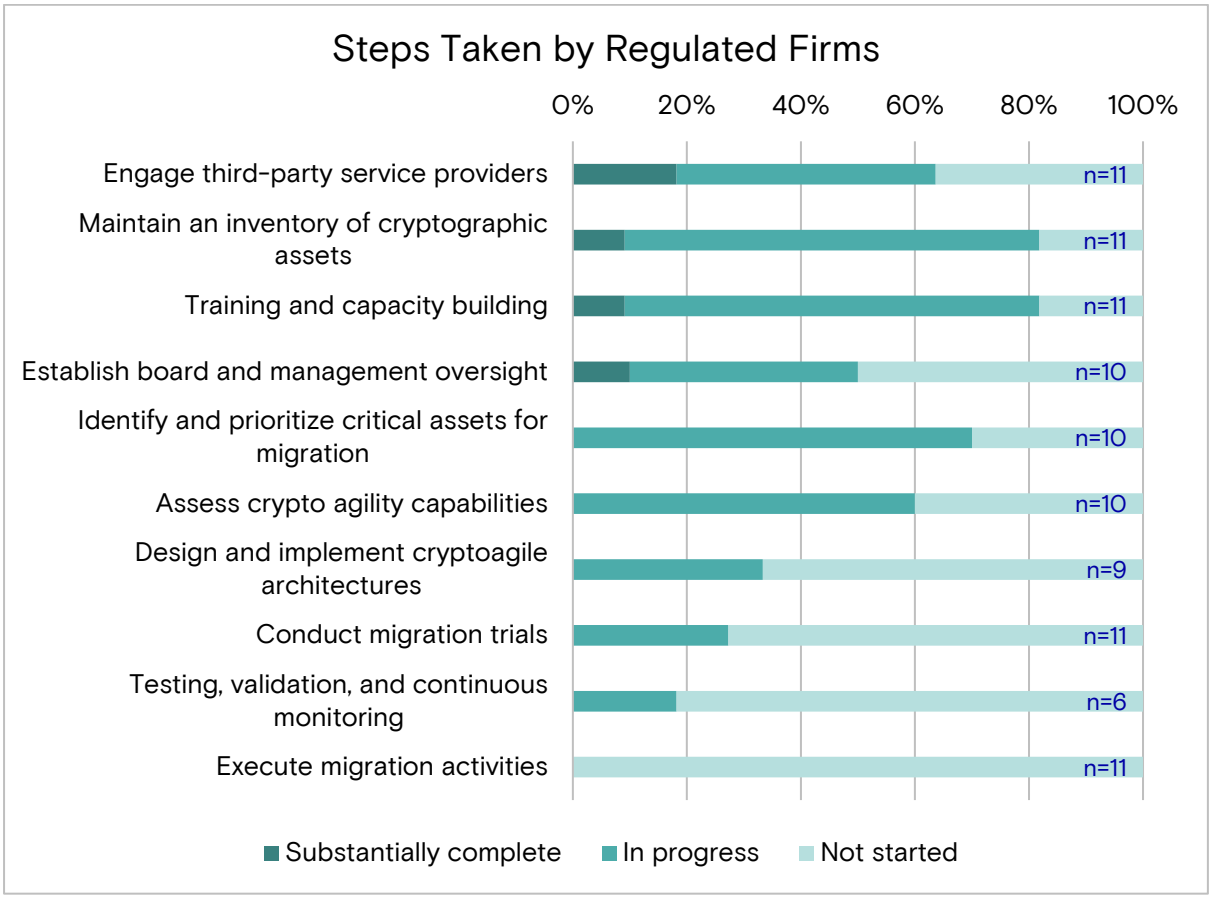

FIGURE 8. *Percentage of member authorities indicating the extent to which regulated firms have taken various steps in supporting quantum preparedness.*

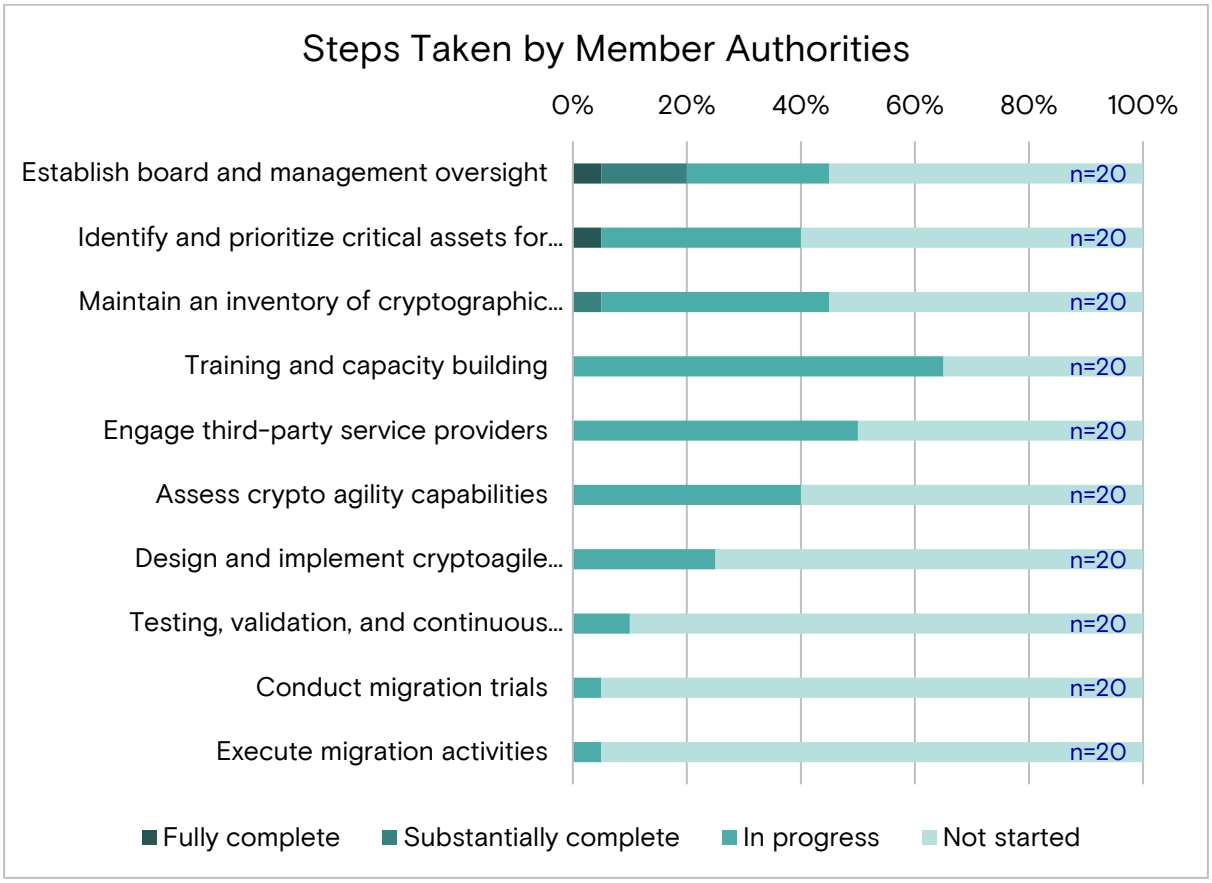

FIGURE 9. *Percentage of member authorities indicating the extent to which they have taken various steps in supporting quantum preparedness.*

D. Ecosystem Dependencies and Coordination

Quantum preparedness is increasingly recognized as extending beyond individual organizations and requiring coordination across broader financial and technology ecosystems. Financial institutions operate within interconnected environments comprising financial market infrastructures, cloud service providers, technology vendors, software providers, telecommunications networks, and other third parties. As a result, migration planning must consider not only internal systems and capabilities, but also external dependencies and the readiness of counterparties, suppliers, and service providers. Shared infrastructures, common technology platforms, cross-border operations, and interoperability requirements mean that participants are likely to transition at different speeds and operate in mixed environments where quantum-vulnerable and quantum-resistant cryptographic solutions coexist for extended periods. Consequently, fragmented or uncoordinated migration approaches may increase operational complexity, create interoperability challenges, and introduce new vulnerabilities during the transition process.[104]

[104] Dutch AIVD, *The PQC Migration Handbook*; Auer et al., *Quantum-readiness for the financial system*; Europol, *Quantum Safe Financial Forum*; G7 Cyber Expert Group, *Statement on Advancing a Coordinated Roadmap*.

Third-party dependencies are also identified as a significant practical constraint on preparedness efforts. Many cryptographic functions reside within externally supplied software, hardware, cloud services, communications infrastructure, and managed services, limiting the ability of individual organizations to assess or remediate vulnerabilities independently. Vendor readiness, product availability, technology refresh cycles, and support for emerging standards may therefore influence migration outcomes as much as the preparedness of individual institutions. Reliance on a relatively small number of major technology providers may further create concentration risks, with delays or implementation challenges potentially affecting multiple institutions simultaneously. Engagement with technology providers, procurement processes, supplier relationships, and vendor risk management arrangements is therefore viewed as an important component of transition planning.[105]

Similar themes emerged from the QWG's stakeholder engagement sessions. Participants repeatedly emphasized that quantum preparedness cannot be addressed solely through firm-level action and described coordination across financial institutions, financial market infrastructures, technology providers, counterparties, and authorities as a central challenge. Migration was frequently characterized as a collective-action problem requiring consistent sequencing, shared expectations, ongoing information-sharing, and coordination across interconnected stakeholders. Participants also highlighted concerns regarding uneven adoption across the ecosystem, noting that early adopters may need to maintain compatibility with organizations that have not yet migrated, while delays by critical service providers could create bottlenecks affecting broader transition efforts. As a result, stakeholders emphasized the importance of interoperability planning, supplier engagement, and collaboration across institutions, sectors, and jurisdictions throughout the transition process.

Survey responses suggest that ecosystem coordination activities are developing across a number of jurisdictions, although progress remains uneven. Industry outreach and awareness-building activities are the most commonly observed forms of engagement, with many authorities reporting briefings, workshops, consultations, or participation in working groups and task forces. Information-sharing and stakeholder engagement activities also appear more developed than more operational forms of coordination (see Figure 10).

The findings indicate that coordination capacity is generally stronger at the strategic and awareness levels than at the operational level. While many authorities reported engagement with industry participants and other stakeholders, fewer reported coordinated assessments, joint implementation initiatives, structured migration planning arrangements, or joint exercises spanning multiple institutions. This suggests that ecosystem coordination efforts remain focused primarily on awareness, information-sharing, and preparedness planning.

Similar patterns can be observed in relation to inter-agency cooperation. Information-sharing arrangements, participation in formal inter-agency structures, and working groups are more commonly observed than joint assessments, coordinated reviews, or joint communications. These findings suggest that inter-agency cooperation is developing,

[105] Dutch AIVD, *The PQC Migration Handbook*; Auer et al., *Quantum-readiness for the financial system*; Europol, *Quantum Safe Financial Forum*https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf.

although operational coordination mechanisms remain comparatively less mature (see Figure 11).

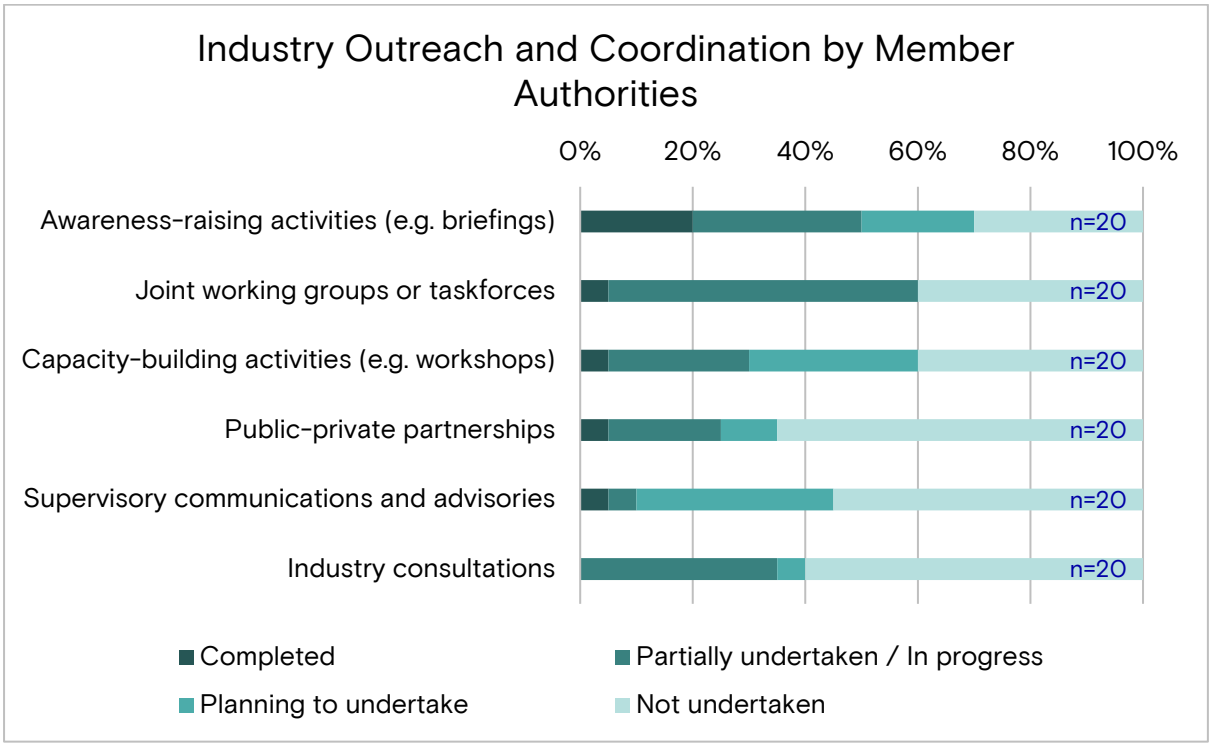

FIGURE 10. *Percentage of member authorities indicating the extent to which they have conducted various industry outreach and coordination activities.*

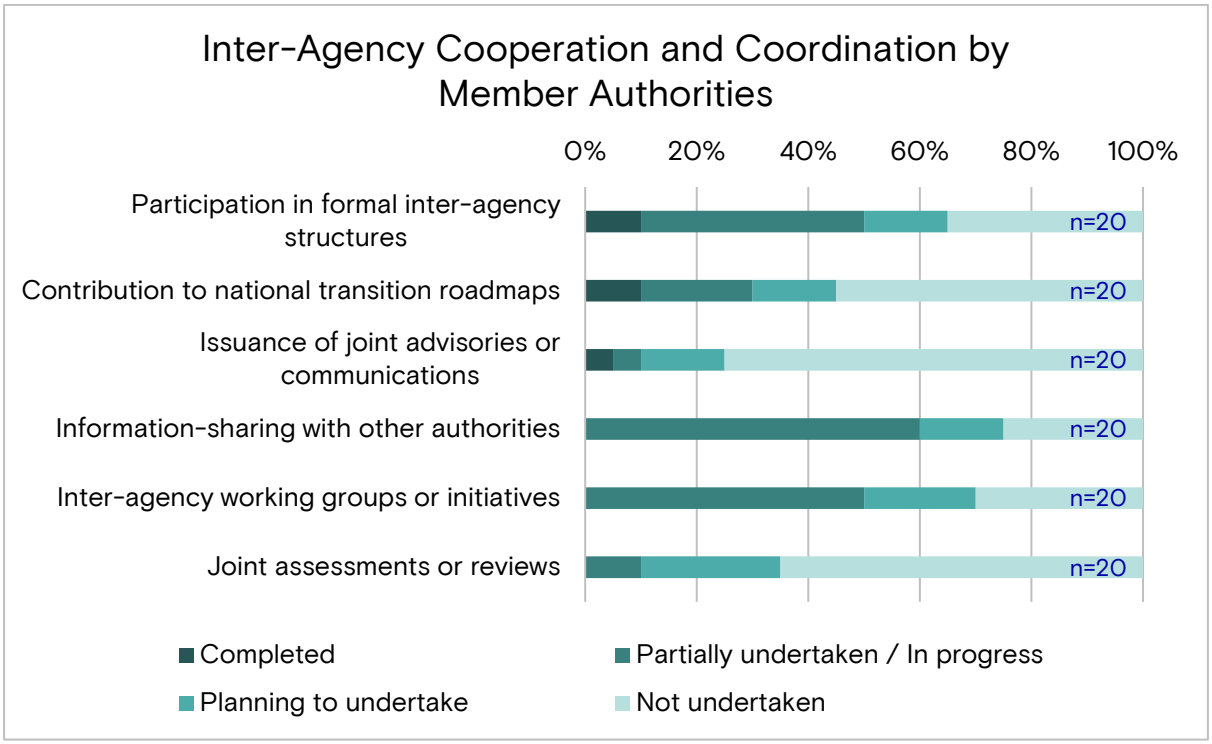

FIGURE 11. *Percentage of member authorities indicating the extent to which they have participated in various inter-agency cooperation and coordination activities.*

E. How Imminent and Serious is the Q-Day Threat?

IOSCO's stakeholder engagement indicates that a cryptographically relevant quantum computer would undermine the foundations of digital trust, posing one of the most significant long-term threats to the sound functioning of global financial markets. Experts consistently stressed that the principal risk is systemic rather than institution-specific. The most plausible scenario may not be a series of isolated cyber incidents, but a coordinated, large-scale attack capable of disrupting critical financial infrastructure and entire economies.

Accordingly, the global priority must shift from incremental preparation to achieving genuine cryptographic resilience through enterprise-wide cryptographic risk management — a discipline that has, to date, received insufficient strategic attention. The timeline for quantum attacks has compressed materially. Quantum technologies have moved beyond experimentation and into a scaling phase, with several platforms already highly advanced and others expected to mature rapidly. As these technologies scale, the timeline to cryptographically relevant capability will become shorter, more predictable, and less uncertain. While the exact timing of cryptographically relevant quantum computers remains uncertain, several industry participants argued that organizations should prepare for the possibility that relevant capabilities emerge within the next five years, potentially accelerated by the use of AI systems.

The debate is therefore no longer about *whether* or even *when* quantum computing will become a threat. The more pressing question is how far behind the financial system already is in preparing for it. Immediate action is required. As one industry expert observed, framing the challenge in terms of the number of board meetings or quarters remaining, rather than a distant "Q-Day", is far more effective in conveying its urgency. Transitioning to quantum-safe cryptography is a multi-year transformation that cannot be accelerated at the last minute. Delayed action materially increases the risk to operational continuity, supply-chain integrity, and the long-term confidentiality of sensitive information, while creating a real possibility that critical systems will not be migrated before quantum attacks become viable.

The ultimate objective therefore is effective cryptographic risk management. While robust cryptographic standards remain essential, managing cryptographic risk requires a broader enterprise risk management approach. A particular concern is hyper-concentration risk: the financial system's widespread dependence on a narrow set of cryptographic assumptions creates common points of failure, making vulnerabilities both systemic and difficult to detect, contain, or remediate.

Importantly, attackers will not need to own a quantum computer — they will only need access to one. At the same time, advances in artificial intelligence are expected to further compress the time available to detect, analyze, and respond to sophisticated attacks. Financial institutions should therefore plan for the possibility of a genuine cryptographic zero-day event, with little or no advance warning.

F. Considerations for Further Engagement

The findings suggest that quantum preparedness across the financial sector remains at an early-to-mid stage of maturity. While awareness of quantum-related cybersecurity risks is increasing and governance discussions are becoming more widespread, technical

implementation and migration capabilities remain comparatively less developed. Across both member authorities and regulated firms, capacity-building efforts are primarily focused on awareness-raising, governance development, workforce training, preliminary risk assessments, and early-stage migration planning. More advanced capabilities, including migration testing, operational deployment, and ecosystem-wide coordination, remain less mature.

The findings also highlight the importance of continued investment in technical expertise, workforce development, and organizational capabilities. Preparedness requires not only awareness of quantum-related risks, but also the ability to understand cryptographic dependencies, evaluate migration options, manage implementation risks, and oversee long-term transition programs. As migration planning progresses, strengthening knowledge-sharing, training, and practical implementation capabilities will become increasingly important for both regulated firms and supervisory authorities.

The findings further suggest a potential role for international coordination and capacity-building initiatives in supporting more consistent preparedness approaches across jurisdictions. Awareness sessions, thematic discussion forums, information-sharing initiatives, coordinated official communications from regulatory authorities, practical guidance on PQC migration and crypto agility, and the exchange of supervisory and industry experiences may help support preparedness efforts and reduce implementation fragmentation. Such coordination may be particularly important given the interconnected nature of the financial system, where uneven adoption of quantum-resistant technologies could create negative externalities. For example, institutions or infrastructures that lag in their transition may continue to expose counterparties, service providers and interconnected systems to residual vulnerabilities, even where other participants have made substantial progress. Engagement with FMIs, technology providers, standard setting bodies (SSBs), and other stakeholders could also help strengthen ecosystem-wide readiness and support more coordinated transition planning.

Ultimately, capacity-building is likely to be a key determinant of long-term quantum preparedness across the securities sector. While awareness, governance arrangements, and foundational preparedness activities are beginning to emerge, continued investment in technical expertise, implementation capabilities, coordination mechanisms, and practical guidance will be important to support an effective transition to post-quantum cryptography.

8. Conclusion

Quantum computing presents both risks and opportunities to financial markets and their participants. On the opportunity side, quantum approaches are being explored across a range of computationally intensive financial activities, including optimization, simulation and modelling, and machine learning. Despite all its benefits, the cyber readiness challenge quantum computing brings is immediate and requires action.

The evidence gathered by IOSCO suggests that quantum applications remain at an early stage of development. Activity is currently concentrated in research, proof-of-concept exercises and pilot testing, with no surveyed jurisdiction reporting operational deployment of quantum computing applications within regulated financial services.

The cybersecurity implications of quantum computing are a significant medium - to long-term risk and challenge for financial markets. The widespread reliance of financial institutions and market infrastructures on cryptographic systems creates potential vulnerabilities when CRQCs become available. These risks extend beyond individual institutions and may affect communications, authentication mechanisms, transaction processing, operational resilience and interconnected financial infrastructures. The possibility of HNDL attacks further highlights that some quantum-related risks require action well before cryptographically relevant quantum computers emerge.

This Report highlights that preparedness efforts are beginning to emerge across jurisdictions. Common themes include cryptographic discovery and inventorying, governance and transition planning, crypto agility, testing and experimentation, and engagement with third-party providers and interconnected stakeholders. While approaches differ across jurisdictions, there is growing recognition that quantum preparedness is not solely a cybersecurity issue but an enterprise-wide operational resilience challenge requiring sustained planning and coordination.

While commercial quantum computing applications remain largely experimental, the cybersecurity preparedness challenge is already relevant. Migration to post-quantum cryptography is expected to require sustained, multi-year effort across systems, applications, infrastructure and third-party dependencies. Despite increasing attention to these issues, preparedness across the financial sector remains at an early stage. IOSCO findings indicate that both authorities and regulated firms are primarily focused on awareness-building, organizational preparedness, inventorying exercises and preliminary planning. More advanced activities, including migration testing, implementation and ecosystem-wide transition arrangements, remain comparatively limited. The findings of this report also point to ongoing challenges relating to third-party dependencies, interoperability, resource constraints, technical expertise and uncertainty regarding migration timelines.

A recurring observation throughout the Report is that quantum preparedness represents a collective challenge. Financial institutions, financial market infrastructures, technology providers and authorities all depend on shared technologies, common standards, and interconnected operational environments. As a result, preparedness and migration outcomes will depend not only on actions taken by individual organizations but also on coordination across ecosystems and jurisdictions, and on a global scale.

Taken together, IOSCO findings suggest that financial markets remain in the early stages of understanding and preparing for both the opportunities and risks associated with quantum computing. While the timeframe for the emergence of cryptographically relevant quantum computers remains uncertain, the scale and complexity of potential transition efforts are already driving increased attention to preparedness across jurisdictions.

Given the magnitude and persistence of the quantum threat, the financial sector has an opportunity and responsibility to lead in proactively addressing these risks. Rather than waiting for the arrival of CRQC, institutions should already be advancing preparedness and planning for the transition towards quantum-resistant technologies. Timely adoption of quantum-resistant technologies will support long-term confidentiality, regulatory compliance, and the trust of clients and stakeholders. By taking forward-looking steps today, the financial sector can strengthen its resilience and demonstrate its commitment to securing information in an evolving technological landscape.

As authorities and market participants progress from planning to migration awareness-raising, capacity-building, practical implementation guidance and international coordination are likely to become increasingly important. Continued monitoring of technological developments, engagement with stakeholders, and the sharing of experiences and good practices may support more informed and consistent approaches to quantum preparedness across IOSCO's membership.

This Report provides a basis for future IOSCO engagement on issues such as PQC readiness, capacity-building initiatives, public-private sector dialogue and international cooperation, to promote more consistent preparedness approaches and reduce the risk of fragmented implementation across interconnected global financial markets.