Entangled Markets: Preparing Exchanges for the Quantum Era

Adrián Febrián[1]
AI Model Validation & Emerging Tech
Nasdaq

Rahelah Syed[2]
North American Markets & Transformation Risk
Nasdaq

Abstract

While quantum computing remains in its infancy, with proven applications largely limited to scientific modeling in research environments, its rapid development indicates that the technology will inevitably permeate broader industries in the coming years, particularly financial exchanges. This paper provides an overview of the essential principles of quantum technology and examines its significant implications for the exchange sector, including the possible disruption of contemporary cryptographic systems. It further delineates the necessity for exchanges to enhance their risk management frameworks to ensure effective adaptation to emerging technological challenges. Additionally, the paper investigates the potential applications and impacts of quantum technology on both exchange operations and product offerings.

Keywords: Quantum computing, Cryptography, Financial infrastructure, Cybersecurity, Risk management

Introduction

Quantum computing represents a paradigm shift in computational capabilities, leveraging the principles of superposition and entanglement to tackle problems beyond the reach of classical systems. While its applications remain largely theoretical—constrained by current hardware limitations and the immaturity of quantum algorithms—the potential for adoption across industries, including financial exchanges, is undeniable.

However, alongside this promise comes significant risk, most urgently in the realm of cybersecurity. The ability of quantum computers to break widely used encryption protocols could have profound implications for data integrity and operational resilience across global market infrastructures. Safeguarding exchanges against these threats is essential to maintaining trust and stability in the financial ecosystem.

This paper examines both the opportunities and risks associated with quantum computing, offering a forward-looking perspective on its potential impact on exchange operations and strategic planning. First, we explore the scientific and technological fundamentals of quantum computing. Second, we highlight cybersecurity as the most pressing implication. Third, we analyze the risks and challenges specific to financial exchanges. Finally, we discuss theorized opportunities within the industry.

SECTION I

SCIENTIFIC AND TECHNICAL BACKGROUND OF QUANTUM COMPUTING TECHNOLOGY

In this section, we will review the scientific and technical concepts that enable quantum computing. The main challenge of the technology is its very **high understanding barrier**. To fully comprehend both the capabilities and limitations of quantum computing, one must first grasp the counterintuitive principles of quantum mechanics which defy classical logic and stretch the boundaries of human intuition. These phenomena form the foundation of quantum information theory and are essential to understanding how quantum computers operate.

Beyond the physics, quantum computing introduces a new paradigm in hardware and software design. *Qubits*, the basic units of quantum information, are fragile and susceptible to environmental noise, requiring extreme conditions and sophisticated error correction techniques to function reliably.

As we explore these concepts, we will use pedagogical examples to highlight the key points that a non-technical reader should realise. These examples will serve as robust anchoring points for the exploration of the opportunities and risks of the technology in a financial exchange's setting, helping bridge the gap between theoretical and technical foundations and future practical implications.

I.1. Physical Foundations

> I, at any rate, am convinced that [God] does not throw dice.
> — Albert Einstein (1926)

The quantum mechanical nature of the universe is both fascinating to study and deeply frustrating to grasp. Our brains evolved over millions of years to distinguish prey from predators, to shoot arrows at animals following parabolic trajectories, and to navigate complex social environments. They were never naturally equipped to unravel the secrets of atoms.

For these reasons—and to better engage the reader's attention—this section will briefly explore two highly complex topics in fundamental physics, adopting a heuristic approach to convey

[1]Email: adrian.febrian@nasdaq.com
[2]Email: rahela.syed@nasdaq.com

the basic principles underlying quantum computers, even if the explanations remain necessarily incomplete.

First, a bit of history. During the last couple of decades of the 19th century, physics was thought to be a "done business". Only a few details remained to be ironed out before achieving a relatively complete and fundamental understanding of the world. One such detail was the mystery of how electromagnetic waves could seemingly propagate through the vacuum of space. The quintessential ether hypothesis, once proposed as an explanation, was famously disproved by the Michelson–Morley experiment of 1887. The ultimate conclusion? The speed of light appeared to be a constant and universal speed limit. That was puzzling. In practice, this means that information can be transmitted at most at the **speed of light**—never faster.

A second unresolved issue was the so-called **ultraviolet catastrophe**. Physics at the time incorrectly predicted that an ideal *black body* (an object that perfectly absorbs all incident radiation and emits energy solely based on its temperature) would emit an infinite amount of energy at short wavelengths (such as ultraviolet light) as it was heated.

The solution to the first problem—why the laws of physics seemed inconsistent for objects moving at high speeds—was provided by Albert Einstein, who introduced his theory of special relativity in one of his four papers during the *annus mirabilis* of 1905. The solution to the second problem—why classical physics failed to explain how atoms emit and absorb energy—came from Max Planck in the year 1900. Planck proposed that at atomic scales, energy is emitted and absorbed in small, discrete ***quantum***[3] packages, rather than being continuous. Later, physicists discovered that quantum theory paints a radically different picture of reality: at the smallest scales, certainty disappears—events unfold in a world governed by **probability**.

Those two "minor" details became the seeds of a revolution that transformed our understanding of the universe. In Einstein's hands, God appeared as a precise cosmic geometer; in the quantum realm, an improbable gambler.

With the previous historical context in mind, we will first define the two core physical principles underlying quantum computers: **superposition** and **entanglement**. Later, we will explore what a quantum computer is and what problem it aims to solve.

> Einstein, stop telling God what to do.
> — Niels Bohr (1927)

I.1.1. Quantum Superposition

According to the principles of quantum mechanics (Hidary, 2021), systems assume a definite state only once they are measured. That is, before measurement, a system exists in an **indeterminate state**; after measurement, it collapses into a definite state.

Let us imagine a system that can occupy one of two discrete states, which we can represent using a convenient mathematical notation called **Dirac (braket) notation**: $|0\rangle$ and $|1\rangle$.

A superposition of states, denoted as $|\psi\rangle$, can then be expressed as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha,\beta \in \mathbb{C} \tag{1}$$

The coefficients α and β are constrained by the **Born rule**, which states that the modulus squared of each number represents the **probability** of observing that state upon measurement:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

For example, if both states are equally likely, then $|\alpha|^2 = |\beta|^2 = \frac{1}{2}$, so $\alpha = \beta = \frac{1}{\sqrt{2}}$. Therefore, the system's state can then be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|1\rangle + \frac{1}{\sqrt{2}}\,|0\rangle \tag{3}$$

Upon measurement, there is a 50% chance of finding the system in $|1\rangle$ and 50% in $|0\rangle$. In short, **superposition** refers to indeterminate state of quantum objects before measurement. Is the system in the $|1\rangle$ or $|0\rangle$ state before we measure it? The answer is, in a sense, **both**.

Importantly, in quantum computing, these two-state systems are abstracted as *qubits*, the fundamental units of quantum information.

I.1.2. Entanglement

Quantum superposition feels like something out of *Alice in Wonderland*—a world where quantum objects can exist in different states at once. Yet reality becomes even stranger as we step *Through the Looking Glass*. Entanglement pushes this peculiarity further, linking two or more quantum objects so that their states are inseparably connected, defying classical intuition.

A classic example illustrates this phenomenon: imagine we create two entangled quantum balls and place each inside a separate box. One box is given to Alice, the other to Bob. Each quantum ball exists in a superposition of being red or blue. In a classical system, opening one box shouldn't affect the other. However, in the quantum world, if Alice opens her box and observes a red ball, this **immediately determines** that Bob will also observe a red ball—even though his ball was previously in a superposition of red and blue states. In simple terms, entangled particles share a connection that defies classical explanation: it's not just pre-arranged matching, but a fundamentally quantum link.

The act of measurement on one side instantaneously collapses the state of the other, regardless of spatial separation. Note, however, that this phenomenon does not violate Einstein's special relativity. Although the collapse appears instantaneous, no usable information is transmitted **faster than light**. The effects of entanglement can only be verified after the fact, when Alice and Bob compare their results. This preserves **causality** (the principle that causes precede effects) and complies with relativistic constraints, as we discussed earlier when we noted that information cannot travel faster than light I.1.

This "spooky action at a distance" seems at odds with our intuition and with classical physics. Indeed, while we can describe quantum entanglement mathematically, why nature behaves this way at the smallest scales remains one of the deepest mysteries in fundamental physics.

[3] From the Latin word *quantus*, meaning "how much".

Entanglement, in a nutshell, offers a different way of **encoding information**. When two particles are entangled, the information about their states is not stored locally in each particle, but rather in the correlation between them. Science often proves stranger than fiction—even the fantastical worlds imagined by Lewis Carroll.

I.2. What Is a Quantum Computer?

> Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.
> — Richard Feynman (1981)

The principles of superposition and entanglement form the foundation of a radically powerful model of computation. Yet bridging the gap between elegant theory and practical implementation is a *quantum leap* in its own right.

Classical computers use bits (0 for closed circuitry and 1 for open) to encode and process information. Similarly, a **qubit**, or *quantum bit*, is the fundamental unit of quantum information. Like a classical bit, it can represent the states 0 or 1, but unlike a classical bit, it can also exist in a superposition of both states, taking on a continuous range of values between them.

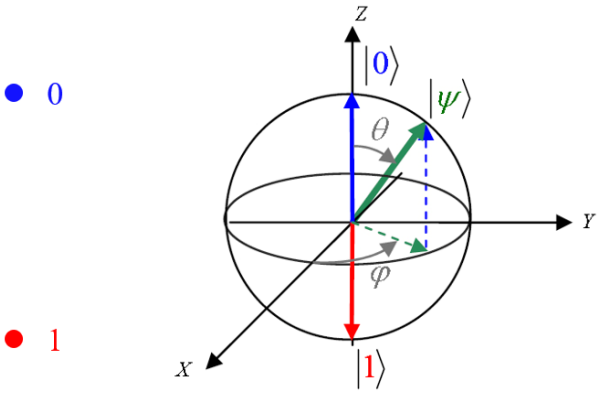

Figure 1: Classical (left) vs. quantum (right) bits. A classical bit can only be at one of two positions: stuck at the north or south pole of a sphere. In contrast, a single qubit's state can occupy any point on the sphere's surface. By applying quantum operators (the fundamental building blocks of a quantum circuit) we can move this point around the surface, enabling a continuum of states.

A register containing two classical bits can store four numbers: 00, 01, 10, and 11. Although both classical systems with n bits and quantum systems with n qubits have 2^n possible basis states, the key difference lies in how those states are used. A classical computer can only be in one state at a time, meaning it must process each possibility sequentially. In contrast, a quantum computer can hold a superposition of all 2^n states simultaneously, allowing operations to act on every state **in parallel**. This ability to manipulate the entire state space at once is what makes quantum computing so powerful compared to classical approaches.

We are all familiar with motherboards built on silicon-based chips, but a quantum computer requires far more than sand that has been *baked* in an industrial oven. Some of the earliest implementations of quantum computation used spin qubits realized through nuclear magnetic resonance devices. Today, researchers are exploring **multiple hardware platforms**, including photonic qubits for gate-based quantum computers, silicon-based spin qubits, and superconducting qubits—currently among the leading contenders for scalability.

It is critical to note that these engineered quantum states are extremely fragile and highly sensitive to environmental disturbances. For instance, superconducting qubits must be cooled to below 10 millikelvin (-273°C or -460°F) to minimize quantum fluctuations, making these chips some of the coldest places in the universe! To address this fragility, **quantum error correction** plays a crucial role in the design of quantum computers, as we will explore in the next section.

I.3. Key Complexities and Technological Barriers of Quantum Computing

One of the key points of the previous section is that there are many more operations one can perform on a qubit compared to a classical bit. This also means that there are more errors that can occur on a qubit! Concretely, the primary classical error is a **bit-flip error**. For example, imagine our classical 16-bit computer is in the following state:

1001 0010 0001 1111

This represents the number 37,407 in binary form. Now imagine that our computer chip is struck by a cosmic ray, which flips one bit. Suddenly, the computer is found in the state:

1**1**01 0010 0001 1111

The state is now 53,791—that is a very different number!

Once again, in quantum computers, errors occur frequently because qubits are extremely **fragile** and easily disturbed by their environment. This fragility, combined with the challenge of scaling up to large, stable quantum systems, remains one of the biggest obstacles to practical quantum computing.

How can we hope to correct errors that can affect a qubit's state? The answer lies in sophisticated error correction schemes, which are beyond the scope of this paper. Currently, a significant proportion of physical qubits are used redundantly for error correction, forcing quantum systems to scale drastically. But quantum hardware is costly even without these schemes, and every additional qubit only amplifies this challenge. Experts estimate that achieving **fully error-correcting (FEC)** quantum computers will require millions of qubits, whereas today's devices operate with only hundreds to a few thousand qubits. FEC technology is expected to remain several years away, likely into the 2030s.

Bit-flip error is just one illustrative example of the many hardware and software hurdles that quantum computers needs to overcome to become a stable and trustworthy technology. Indeed, as confirmed in a recently published report by the *National Energy Research Scientific Computing Center* (NERSC)—a high-performance computing (HPC) facility for the U.S. Department

of Energy's Office of Science—quantum hardware vendors face key challenges in delivering stable, useful, and affordable technology(Bard et al., 2025) that will shape how (and when) these benefits reach financial institutions. Beyond bit-flip error, some of these key challenges include:

i. **Scaling Up:** Current quantum computers operate with tens or hundreds of qubits, but meaningful financial applications will require **thousands** or even **millions**. Scaling up introduces engineering challenges in manufacturing, controlling, and connecting vast numbers of qubits, each with precise requirements for stability and communication.

ii. **Technology Diversity and Integration:** There are different hardware avenues to realise the technology (e.g., superconducting circuits, trapped ions, neutral atoms, photonics), each with unique **strengths** and **weaknesses**. The financial exchanges industry must monitor which technologies mature fastest, as integration with existing IT infrastructure and regulatory compliance will depend on the chosen platform.

iii. **Speed and Throughput:** Quantum computers must execute operations ("gates") quickly and accurately. Slow or **error-prone gates** can make even theoretically powerful quantum computers impractical for real-world financial tasks, where latency and accuracy are paramount. As hardware scales up, maintaining high gate fidelity and fast execution becomes more challenging, especially when error correction overhead increases. Vendors are working to improve both the speed and reliability of gate operations, but progress remains uneven across platforms, as noted in the NERSC report issued in September 2025 (Bard et al., 2025).

Beyond these hardware hurdles, programming quantum computers introduces its own set of complexities. Unlike classical systems, coding for quantum machines requires deep knowledge of quantum mechanics and linear algebra. While some tools simplify access, creating efficient quantum algorithms remains an immense challenge, making the leap from concept to implementation far from trivial.

I.4. Main Applications

If we bought a quantum computer online today, after paying a six or seven-figure sum, what could it actually do?

One of the most promising areas is **quantum simulation**, particularly in chemistry. Classical supercomputers already model molecular structures to develop new materials and drugs, but quantum systems could push this further, enabling simulations that were previously impossible—echoing Feynman's remark at the beginning of section I.2: what better than a quantum computer to model a quantum system! Early research partnerships, including work by a prominent pharmaceutical company, are exploring hybrid quantum-classical approaches for drug discovery (Soller et al., 2025a).

Another key theorised application is **optimization**, which is critical for industries tackling complex problems like delivery routing. One approach, **quantum annealing**, uses quantum effects to efficiently search for the lowest-energy solution among many possibilities, making it well-suited for certain optimization tasks. Another promising direction involves variational algorithms such as the *Quantum Approximate Optimization Algorithm* (QAOA), which aim to provide speedups for specific problem classes. Together, these techniques represent a theorised frontier for logistics, finance, and beyond (Farhi et al., 2014).

Although proven use cases in financial systems remain elusive today, the potential impact as the technology matures is undeniable. In section IV.2 we provide an overview of the prospective effects of quantum technology on global markets.

SECTION II

THE INEVITABLE HORIZON: CRYPTOGRAPHY AND Q-DAY

With the scientific foundations in place, we now turn to the pressing risks posed by quantum computing—particularly those with real-world urgency. While many use cases remain exploratory, one area where quantum capabilities are already reshaping strategic priorities is **cybersecurity**.

Quantum computers threaten to break widely used encryption protocols, posing a risk that could materialize within the next five to ten years. This looming milestone, often referred to as *"Q-Day"*, has prompted a global push toward **post-quantum cryptography**. For financial exchanges, where secure data transmission is critical, preparing for this transition is not optional.

In this section, we explore how quantum computing is driving change in cybersecurity and why industry readiness must begin now.

II.1. Cryptography Fundamentals

Suppose Alice, after her strange encounter with quantum entanglement earlier, wants to send a private message to Bob over the internet. Along the way, Alice's message could be intercepted by a malicious eavesdropper, Charlie. This is where **cryptography** comes in: the science of making and breaking secret codes. One of the most widely used protocols is **RSA** (named after Rivest, Shamir, and Adleman), which secures information transfer across the internet. RSA uses two keys: a **public key** for encryption and a **private key** for decryption. These keys are derived from large prime numbers and their product, which forms the basis of RSA's security. Heuristically speaking, RSA relies on a **trapdoor function**: multiplying two large prime numbers is easy, but factoring the product back into its original primes is extremely hard. For example:

$$p = 61, \quad q = 53 \quad \Rightarrow \quad n = p \times q = 3233 \tag{4}$$

Imagine Charlie only knows $n = 3233$ and needs to find its prime factors to access the individual keys of Alice and Bob. For small numbers, this is doable by trial division, but if p and

q were each hundreds of digits long, factoring n would take classical computers an astronomical amount of time.

Quantum computers pose a serious threat to RSA because of **Shor's algorithm**, which can factor large integers exponentially faster than the best-known classical algorithms. This means that once sufficiently powerful quantum computers exist, they could break RSA encryption by efficiently finding the prime factors of its large composite keys, allowing Charlie to decipher Alice's private message and rendering much of today's internet security obsolete.

To prepare for this risk, researchers are developing **post-quantum cryptography**: new cryptographic schemes based on mathematical problems believed to be resistant to quantum attacks II.2. To keep her secrets secure, Alice (and the entire industry) will need to transition to quantum-safe protocols to protect data in the coming quantum era.

II.2. Q-Day and Cybersecurity

Technological advancement is exciting, but it inevitably represents change and carries inherent risks. Most exchanges recognize the significant risks associated with rapidly emerging new technologies, such as quantum technology, but remain committed to both adhering to industry standards and actively contributing to the field.

Cybersecurity represents a significant and fundamental risk for any organization managing digital information, and is mainly focused on the weakness of classical encryption in front of quantum computers' capabilities. One of the main conclusions of the previous section is that quantum computers have the potential to **compromise** these systems by applying Shor's algorithm to factor RSA or Grover's algorithm to **speed up key searches** for other forms of encryption. According to the *Global Risk Institute's 2023 Quantum Threat Timeline Report* (Global Risk Institute, 2023), quantum computers capable of breaking current encryption could emerge sooner than expected. To mitigate this risk, transitioning to quantum-safe encryption methods before the widespread adoption of this technology is **essential** for all financial exchanges.

In preparation for Q-Day, mathematicians around the world are developing post-quantum cryptography: new encryption, digital certificate, and hashing algorithms based on mathematical problems that are difficult to solve by both quantum and classical computers. Once finalized, these algorithms will become the new encryption standards set by the *National Institute of Standards and Technology* (NIST) and the *International Organization for Standardization* (ISO).

Reflecting this effort, NIST issued an initial report **IR 8547** in November 2024 that outlined its expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes. The report identified existing quantum-vulnerable cryptographic standards and the quantum-resistant standards to which information technology products and services would need to transition. Moreover, the report refers to the deadline specified in the *White House's National Security Memorandum 10* for completing the transition to **quantum-resistant algorithms** for National Security Systems by 2035 (The White House, 2022).

NIST has assigned a post-quantum security category to each variant of its standardized *Post-Quantum Cryptographic* (PQC) asymmetric algorithms, with *Category 1* indicating the lowest security strength[4] and *Category 5* indicating the highest security strength. See Table 1 for an overview of these categories.

Table 1: Post-Quantum Security Categories from NIST

Category	Attack Type	Example Primitive
1	Key search on a 128-bit block cipher	AES-128
2	Collision search on a 256-bit hash	SHA-256
3	Key search on a 192-bit block cipher	AES-192
4	Collision search on a 384-bit hash	SHA3-384
5	Key search on a 256-bit block cipher	AES-256

In essence, NIST concludes that:

1. Algorithms that provide approximately 112-bit classical security will be deprecated after 2030 and fully disallowed after 2035.

2. Algorithms that provide 128-bit or higher classical security will also be disallowed after 2035 because they remain vulnerable to quantum attacks.

While NIST is working with industry leaders to refine the transition timeline and approach, ensuring all stakeholders are adequately protected by post-quantum cryptography before the technology's arrival, exchanges, through their **information security teams**, must proactively lead internal efforts to achieve timely compliance with NIST's recommendations.

Given the global nature of an exchange's operations, the security of **VPN connections**, which is widely used by staff for remote work and to access sensitive internal resources, demands particular attention. These VPN connections typically rely on public-key encryption for the authentication of both users and devices, rendering them susceptible to the same potential vulnerabilities that threaten broader business-to-business communications in the quantum era.

In this regard, recent research (Bank for International Settlements, 2023) outlined preliminary guidelines and prospective approaches to securing VPN technologies against emerging threats, with central banks and other financial institutions already commencing investigations into quantum-safe cryptographic solutions. In addition to VPN vulnerabilities, encryption protecting payment and **settlement transaction networks** represent another significant risk area for exchanges, warranting close monitoring. In anticipation of these risks, regulatory bodies underscore the importance of proactive adaptation to safeguard the financial sector's integrity as quantum computing advances.

[4]The NIST report highlights that "[t]ransition schedules are primarily driven by the level of cryptographic protection that a given algorithm and associated parameter set can provide, which is described as a rough measure known as security strength. Historically, the security strength that an algorithm could provide was defined in terms of the amount of work (i.e., the number of operations) that is required to break the algorithm (i.e., an algorithm has s bits of security strength if breaking the algorithm requires 2^s operations of some kind, where s = 112, 128, 192, or 256). However, there are significant uncertainties in estimating the security strengths of post-quantum cryptosystems given the difficulty of accurately predicting the performance characteristics of future quantum computers, such as their cost, speed, and memory size" (Moody et al., 2024).

SECTION III

RISKS OF QUANTUM COMPUTING FOR EXCHANGE OPERATORS

Financial infrastructures need to actively participate in both the growth and practical application of quantum technology if they want to maintain a leading position in innovation for three key reasons:

i. Ensure comprehensive readiness for **Post-Quantum Cryptography**[5] while actively engaging with industry stakeholders to facilitate timely and appropriate decisions that guarantee robust data protection.

ii. Attain a competitive edge by pioneering the adoption of technology in market operations, while simultaneously implementing robust controls to effectively manage associated risks.

iii. Demonstrate leadership within the legal and regulatory domains by advocating for the establishment of appropriate frameworks that uphold safe, reliable, and equitable market conditions.

It is important that **all three objectives** are balanced to support risk-based decisions related to investment, usage, and advocacy for or against this technology. By systematically evaluating and integrating quantum technology across critical domains, exchange operators are not only exploring but also critically assessing the appropriate use of these technologies to maintain efficient, fair, and secure market operations. It is essential that these organizations ensure quantum technologies align with their operational goals and overarching strategic mission, which should emphasize investor interests, market stability, and equitable access.

Cybersecurity risk is the most obvious and imminent concern for most organizations. However, it is equally important to identify other specific risks, such as regulatory, operational, reputational, and ethical risks associated with the emergence and availability of quantum technology, to which exchanges could be exposed even if they do not adopt it.

III.1. Exposure to Conventional Risks of Emerging Technologies

Beyond cryptography related risks, new technologies also pose challenges such as, data integrity, dependencies and interconnectedness, misunderstandings of technology, operational issues, and regulatory compliance(Freund, 2024).

[5]The *Global Risk Institute* recommends a six-phase approach: (1) Identify and document information assets and their current cryptographic protection; (2) Research the state of emerging quantum computers and quantum-safe cryptography, estimate timelines for availability, and influence development and validation; (3) Identify threat actors and estimate their time to access quantum technology "z"; (4) Identify the lifetime of your assets "x" and the time required to transform the organization's technical infrastructure to a quantum-safe state "y"; (5) Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them ($x+y > z$?); (6) Identify and prioritize activities required to maintain awareness and migrate the organization's technology to a quantum-safe state.

i. **Data Integrity:**

Data integrity represents a fundamental component of the **information security framework**, ensuring that digital information remains "accurate, complete and consistent at any point in its lifecycle. Maintaining data integrity involves safeguarding an organizations' data against loss, leaks and corrupting influences" (IBM).

Quantum technology's advancement introduces specific risks impacting these core components directly. One notable risk is the **facilitation** of **forging digital signatures**, which is significantly easier with the advent of quantum technology. Such capabilities would directly compromise the **accuracy** and **completeness** of digital documents and transactions, resulting in potential unauthorized modifications. Additionally, there is a severe threat of decrypting sensitive data—the risk known as "Harvest Now, Decrypt Later" (HNDL), mentioned earlier, as this involves the potential decryption of currently encrypted data when quantum computers become sufficiently advanced. This threat **jeopardizes** the consistency of data throughout its lifecycle, enabling the future decryption of currently secured information and exposing sensitive data that was once protected. All stakeholders in the financial system should recognize these quantum-enabled risks and begin reviewing and planning appropriate mitigation strategies.

It is worth noting that cryptography is used worldwide to protect military secrets and nation-states have already adopted the harvest-and-decrypt approach, intercepting adversary data they hope to decrypt after Q-Day. Unlike nation-states, financially motivated cyber actors are not known to be harvesting encrypted data, as paying for storage for decades precludes monetization. There is no evidence of dark web chatter about quantum yet.

Some advanced cybercrime groups are now encrypting their malicious network traffic using quantum-resistant algorithms. This makes the traffic extremely hard to analyze and hides its true purpose; a tactic known as obfuscation. Today, these methods work just like traditional encryption, but with one critical difference: even when quantum computers arrive (Q-Day), defenders will not be able to decrypt this stored traffic because it was encrypted with algorithms designed to resist quantum attacks. In contrast, hacktivists are far less sophisticated and will likely be the last to adopt quantum technologies.

ii. **Dependencies and Interconnectedness :**

New technologies do not exist in **isolation**; they must be integrated and updated to function smoothly alongside one another. Similarly, a particular technology risk can rapidly proliferate throughout all products that depend upon it. **Blockchain** serves as a prime example of this phenomenon. The combination of weak classical cryptography, such as outdated encryption algorithms that are vulnerable to attack and the potential for malicious actors to alter existing data, can be particularly detrimental to blockchain platforms and cryptocurrencies. These vulnerabilities could threaten the security and integrity of digital assets.

Market operators that may be interested in entering or expanding in the digital asset space (through **tokenization** or **crypto**

exchanges), must take these risks into account and be prepared to invest in implementing adequate controls, like quantum-safe encryption methods and robust data integrity protocols.

iii. **Misunderstanding of the Technology:**

At first glance, this may seem like a minimal risk, as a broader understanding of the technology will eventually emerge. However, industry leaders often face significant exposure when making **unchecked decisions** in their race to stay ahead. While higher risks can lead to greater rewards, it is essential to determine whether emerging technologies truly align with and advance the organization's strategic objectives. A thorough evaluation of the benefits versus the costs of early quantum adoption is critical. Success depends on ensuring both technological expertise and business acumen are present—and that these capabilities work together to identify practical, high-impact use cases for quantum technology within market operations.

iv. **Operational Challenges:**

In close relation to the risks mentioned above, evaluating **operational constraints** when implementing new technologies is an essential consideration. Clearly defined operational requirements are critical for successfully transitioning an idea into practice. However, these requirements are frequently determined too late in the development process. Quantum technology, as previously discussed, is highly sensitive to environmental fluctuations and demands bespoke and advanced infrastructure (such as large form factors, the need for cryogenic cooling, and specialized networking equipment for networking between quantum chips), plus the sophisticated ongoing maintenance.

Considerable investments are currently directed toward advancing this technology, which is expected to result in elevated initial market costs. Therefore, existing infrastructures may need to be updated or adjusted to integrate quantum components, either to utilize their capabilities or to address potential risks such as vulnerabilities to classical encryption methods. For market operators, it will be necessary to objectively evaluate the advantages and costs of implementing quantum technology in market operations, taking into account their mission to provide fair and equitable markets for investors.

v. **Regulatory Compliance:**

As is typical with emerging technologies, regulatory bodies have yet to engage **extensively** in discussion or issue comprehensive rulings regarding quantum technology. The complexity arises largely because many assessments and analyses rely on **assumptions** concerning the feasibility of quantum advancements. Presently, international competition is driving both nations and private enterprises to accelerate investment and development efforts in an attempt to secure early advantages in this field. There is significant motivation to file numerous patents to obtain privileged access to new technologies.

In the United States, the *National Quantum Initiative Act*, enacted in 2018, aims to bolster economic growth and national security. The European Union's *Quantum Flagship*, also launched in 2018, seeks to reinforce European leadership and scientific excellence, while explicitly considering the societal and ethical implications of quantum technologies. Meanwhile, the Chinese government has designated quantum technology as a national priority, committing substantial resources to research and development, and targeting notable breakthroughs by 2030.

III.2. Distinct or Heightened Risks in Quantum Technology

In addition to the conventional risks mentioned above, quantum technology's novelty and complexity introduce new risks or heightens existing risks that go beyond the technology itself and focus on the resources needed to build, operate and maintain it, such as **talent** and **vendors**.

III.2.1. Enhanced Talent Risk: Specialized Skillset Requirements

The skills needed to work with different quantum computing vendors vary depending on their hardware architecture and software development environments. Most vendors use Python-based SDKs, but the specific tools and programming models differ. For example, *IBM* and *Google* use gate-based systems and require familiarity with quantum circuits and libraries like Qiskit or Cirq. On the other hand, *D-Wave*, uses quantum annealing and requires knowledge of optimization theory and QUBO/Ising models through its Ocean SDK (Software Development Kit). *Rigetti* uses its own Quil language via pyQuil, while *Quantinuum* offers TKET, a compiler that supports multiple platforms. *IonQ* and *PsiQuantum* also introduce unique hardware considerations, such as trapped ions or photonic qubits, which may require additional domain-specific knowledge.

As a result, quantum developers often need to tailor their skills to the specific vendor ecosystem they are working with. There is a risk of a **talent** and **skill gap** but also **vendor lock-in** if we get too familiar with a specific hardware architecture (as we discuss in subsection III.2.2).

To effectively engage with this emerging technology, exchanges will need to adapt and build new capabilities. This includes developing a working understanding of quantum algorithms and their practical applications—such as optimization, simulation, and cryptography—as well as gaining familiarity with different qubit technologies like superconducting, trapped ion, and photonic systems. Teams should also be equipped to analyze the vendor landscape, benchmark performance, and model cost-effectiveness between quantum and classical systems. Additionally, knowledge of integration strategies for hybrid quantum-classical workflows and awareness of regulatory and intellectual property considerations will be essential for informed decision-making and strategic alignment.

III.2.2. Vendor Risk: Tight Roadmap & Heightened Concentration Risk

As quantum computing continues to evolve, the path to practical deployment in the financial sector remains complex and uncertain. Beyond technical hurdles related to reliability, scalability, and integration, vendors and financial institutions alike must grapple with the **unpredictability** of **development timelines** and the challenge of assessing real-world system performance.

i. **Roadmap Uncertainty:** Vendor technology roadmaps are ambitious, projecting exponential improvements in qubit count and performance over the next five to ten years. However, these projections are subject to **frequent revision** due to the unpredictable nature of quantum research and development. Financial institutions should expect timelines to shift and plan for gradual adoption.

ii. **Practical Performance:** Even as hardware improves, quantum computers must deliver results within reasonable timeframes and support multiple users and workloads. Vendors are developing **new metrics**—such as *Sustained Quantum System Performance (SQSP)*—to measure throughput, but real-world performance will depend on advances in both hardware and software.

iii. **Enterprise Integration:** Financial institutions require systems that can handle multiple users and diverse workloads simultaneously. Early quantum computers are often single-user or batch-oriented, limiting their utility for enterprise-scale operations.

iv. **Hybrid Workflows:** Quantum computers will not operate in **isolation**. For practical performance, they must integrate seamlessly with existing high-performance computing (HPC) infrastructure, data lakes, and analytics platforms. Hybrid workflows—where quantum and classical systems collaborate—will introduce additional complexity in data transfer, latency, and orchestration.

v. **Concentration Risk:** The pace at which this technology stabilizes is closely tied to investment levels, suggesting that only organizations with sufficient capital may succeed, while smaller startups could be absorbed by major tech corporations. It is well-established that a limited number of technology providers dominate the industry; however, this risk becomes more pronounced for technology-specific requirements, such as ultra stable or ultracold environments, specialized chips, or rare materials. Should any critical component be scarce, the concentration risk will further intensify.

vi. **Vendor Lock-in** happens when organizations have limited choices and complex technologies, causing them to depend on a single provider's products or services. This reliance often makes changing vendors both challenging and costly. While some regulators ask market platforms to support measures against vendor lock-in by requiring a well-defined *Exit Strategy*, implementing these requirements is difficult with certain technologies; similar to the obstacles faced when transferring applications between different cloud infrastructure providers (for example, moving from one Cloud brand to another can be tough because some code may need to be rewritten for specific features of the Cloud Service Providers).

Tables 2 and 3 provide an overview of the quantum technology ecosystem as of June 2026, highlighting the principal technology layers, hardware modalities, infrastructure providers, networking and security capabilities, application domains, and key investment participants shaping the industry's evolution. The classification is based on industry analyses from *The Quantum Insider* and *Quantum Zeitgeist* (The Quantum Insider, 2026; Quantum Zeitgeist, 2025).

SECTION IV

THEORISED, LONG-TERM APPLICATIONS OF QUANTUM COMPUTING FOR EXCHANGE OPERATORS

After reviewing the theoretical and technical foundations of quantum computing, and examining its immediate implications, particularly in the realm of cybersecurity, we now turn our attention to the long-term, theorized applications of this emerging technology.

Quantum computing is often portrayed as transformative, with the potential to reshape industries through unprecedented computational capabilities. However, it remains in an embryonic stage, and many of its most ambitious promises have yet to be realized.

Technological progress is notoriously difficult to predict. Few could have foreseen that just 60 years after the Wright brothers' first powered flight in 1903, there would be humans in the low-Earth orbit. Exchanges must nonetheless look beyond encryption threats and begin to theorize how quantum capabilities might eventually unlock new efficiencies, insights, and competitive advantages across its exchanges and broader business operations.

In this section, we explore speculative use cases for quantum computing at financial exchanges. These scenarios are not imminent, nor are they guaranteed. Rather, they represent a forward-looking perspective on how quantum advancements (should they materialize) might shape the future of financial infrastructure and data-driven decision-making.

This exploration is intended to inform strategic foresight, not immediate investment or implementation.

*IV.1. **Applications for Exchange Operators***

Quantum technology is exponentially gaining popularity, especially over the past couple of years. As per the fourth annual *Quantum Technology Monitor* report from *McKinsey* published in June 2025 (Soller et al., 2025b), *"the surging investment and faster-than-expected innovation could propel the quantum market to $ 100 billion in a decade"*. The report also mentions that "*In 2024, the Quantum Technology industry saw a shift from growing quantum bits (qubits) to stabilizing qubits—and that marks a turning point. It signals to mission-critical industries that QT could soon become a safe and reliable component of their technology infrastructure*".

It is essential to understand the distinct advantages quantum technology may offer to different stakeholders within the trading ecosystem. Market participants, such as traders and institutional investors, may harness quantum computing to develop more advanced trading strategies, optimize portfolio management, and improve risk assessments. These direct applications could provide substantial competitive advantages. However, a relevant

Table 2: Quantum Computing Value Chain (2026) - Core Technology and Ecosystem

Layer	Category	Leading Players	Country	Description	Strategic Relevance
Core Hardware	Superconducting	IBM, Google, Rigetti, IQM, OQC	US, Finland, UK	Supercooled circuit-based processors	Most mature modality with leading roadmaps and ecosystems
	Trapped-ion	IonQ, Quantinuum, AQT, Universal Quantum	US, UK, Austria	Ion-based qubits with high fidelity	Leading performance in accuracy and error correction
	Neutral atom	QuEra, Pasqal, Atom Computing, Infleqtion	US, France	Atom arrays using optical trapping	Strong scalability potential (large qubit systems)
	Photonic	PsiQuantum, Xanadu, Orca, Quandela	US, Canada, UK, France	Light-based quantum systems	Room-temperature potential and semiconductor alignment
	Silicon / spin	Intel, Quantum Motion, Diraq, Qubly	US, UK, Australia, France	CMOS-compatible architectures	Leverages established semiconductor manufacturing
	Diamond / NV-center	Quantum Brilliance, SaxonQ, SBQuantum	Australia, Germany, Canada	Diamond-based systems and sensors	Enables room-temperature and edge deployments
	Topological	Microsoft	US	Topological qubits	Long-term potential for intrinsic error resistance
	Quantum annealing	D-Wave	Canada	Optimization-based quantum computing	Only commercially deployed alternative architecture
Networking & Security	Quantum networking	NTT, SK Telecom, Cisco, Deutsche Telekom, QuantumCTek	Japan, Korea, US, Germany, China	Quantum communication and entanglement networks	Enables quantum internet and distributed computing
	Post-quantum security	PQShield, SandboxAQ, ID Quantique, QuintessenceLabs	UK, US, Switzerland, Australia	Quantum-resistant cryptography	Earliest and fastest commercial adoption pathway
Infrastructure	Components & control	Bluefors, Zurich Instruments, Qblox, Kiutra, Keysight	Finland, Switzerland, Netherlands, Germany, US	Cryogenics, control, and measurement systems	Key scaling constraint across all hardware modalities
	Software & cloud	AWS, NVIDIA, Classiq, Riverlane, QC Ware	US, UK, Israel	Programming, orchestration, and hybrid compute	Enables usability and abstracts hardware complexity
Applications & Adopters	Quantum sensing	Q-CTRL, Exail, Nomad Atomics	Australia, France	Precision sensing and timing solutions	Most commercially advanced quantum applications
	Enterprise adoption	Accenture, Capgemini, Goldman Sachs, Booz Allen	US, France, Global	Use-case development and integration	Bridges technology and commercialization
	Emerging approaches	Multiverse Computing, C12 Quantum, EeroQ	Spain, France, US	Novel and quantum-inspired methods	Potential disruptive or complementary solutions

Table 3: Quantum Computing Value Chain (2026) - Capital and Ecosystem Support

Category	Leading Players	Country	Description	Strategic Relevance
Sovereign investors	Mubadala, Temasek, Qatar Investment Authority	UAE, Singapore, Qatar	National strategic investment funds	Anchor capital shaping global quantum competition
Specialist quantum funds	Quantonation	France	Dedicated quantum venture capital	Early-stage innovation and technical validation
Institutional investors	BlackRock, Baillie Gifford	US, UK	Large-scale asset managers	Validate quantum as a long-term infrastructure asset
Corporate venture	NVentures (NVIDIA), Airbus Ventures	US, France	Strategic industry investors	Link technology development to commercial use cases
Government-backed investors	In-Q-Tel	US	National security-focused investment arm	Accelerates defense and intelligence adoption
Venture capital	Andreessen Horowitz, Lux Capital	US	Generalist deep-tech investors	Support ecosystem growth and commercialization

question emerges as to whether the *Market Service Providers* will benefit from quantum computing technology as strongly as market participants themselves?

Market Service Providers, such as exchange operators and infrastructure vendors, prioritize **investor interests**, **market stability**, and **equitable access**. Accordingly, the application and advantages of quantum computing within this sector are likely to be distinct. The main emphasis would be on utilizing quantum technologies to advance the **core trading infrastructure**, thereby reinforcing the foundation of the financial system.

IV.1.1. ***Potential Benefits for Exchange Operators***

The core objective of an exchange operator is to guarantee fair and orderly markets for all investors. To achieve this, in addition to state-of-the art cybersecurity measures, they prioritize the delivery of best-in-class technology, centered around:

i. **Trading systems**.

ii. Ultra-low **latency**.

iii. Effective **surveillance**.

A review of how these technological advances could be applied to each of these critical areas is essential.

i. **Matching Engine:**

The matching engine is the core system responsible for pairing buy and sell orders. Any improvement in this area must uphold the principles of speed, fairness, and determinism. Quantum technology could offer enhancements by optimizing complex processes such as **order scheduling** and **computational resource allocation**, especially during periods of peak market activity. In addition to the matching function, overall trading systems, which include surrounding systems and configurations, enforce critical controls such as risk checks, credit limits, and compliance rules. Although these checks are executed in parallel with the matching workflow, quantum computing could accelerate the underlying computations for these validations, making them available in **real time**. This would help maintain the speed of the matching process and allow transactions to be completed more efficiently, even under peak load conditions.

ii. **Low Latency:**

While matching engines already operate at superfast latencies (often in the sub-millisecond range), quantum computing is **not** expected to deliver dramatic improvements for these individual ultra-low-latency tasks. Instead, the true strength of quantum technology lies in its ability to tackle **large**, complex problems that are computationally intensive and data-heavy.

Quantum computers excel when the challenge is so **vast** that classical systems would require months or years to solve it. In such cases, quantum algorithms have the potential to reduce solution times to seconds, fundamentally changing how exchanges can process and leverage **massive datasets**. Rather than focusing on shaving microseconds off existing processes, quantum computing opens new possibilities for optimizing large-scale operations and rethinking how data and information used by exchanges can be leveraged more optimally.

While quantum algorithms can dramatically accelerate certain classes of computations (e.g., optimization, cryptography), these gains apply to **computational throughput**, not network-level latency. In traditional systems, certain computational problems, such as routing orders, managing network traffic, and optimizing resource allocation, can introduce delays, even if measured in fractions of microseconds. Quantum computing, leveraging the principles of superposition and entanglement, offers extraordinary parallel processing capabilities by evaluating multiple scenarios simultaneously and delivering efficiencies that classical methods cannot match. In particular, quantum algorithms like **quantum annealing** or **variational optimization** are designed to solve complex optimization problems, such as finding the most efficient arrangement, path, or allocation. For example, quantum technology could enable the dynamic optimization of **queue management**, **network routing**, or resource allocation at large scales and in real time—tasks that may be difficult or inefficient for classical computers.

iii. **Surveillance:**

The seamless operation of an exchange relies on a set of critical controls that demand both high-speed computing and advanced algorithmic capabilities. Among these, **real-time surveillance** and **post-trade surveillance** play a vital role in maintaining market integrity and ensuring compliance with regulatory standards. Quantum computing has the potential to significantly elevate the effectiveness of these surveillance mechanisms. By harnessing its computational power, quantum technology could exponentially increase the speed and complexity of pattern recognition, enabling extensive analysis of historical data at scales unattainable with classical systems.

For instance, the combined strengths of quantum computing and Artificial Intelligence, through **quantum machine learning** (QML), offer **new possibilities** for surveillance. QML utilizes quantum circuits as trainable machine learning models, enhancing computational efficiency and the performance of machine learning tasks. This synergy could drive advancements in data-driven decision-making, particularly within surveillance functions in trading environments.

Utilizing larger datasets spanning multiple years would enhance the accuracy of pattern detection and allow for simultaneous consideration of numerous scenarios. This would enable exchanges to detect **unusual trading activities**, **market manipulation**, or **compliance violations** more rapidly and with greater accuracy than is currently achievable. Quantum computing could introduce a transformative shift in regulatory intelligence, moving beyond static market abuse frameworks and retrospective testing to dynamic identification of emerging trading patterns in real time.

This opens the door to adaptive rule discovery that evolves with market behavior, allowing risk and compliance teams to anticipate and respond to anomalies before they materialize into threats. Organizations should explore how quantum-driven models can be integrated into surveillance and governance architectures to stay ahead of increasingly complex regulatory landscapes.

As automation and reliance on technology continue to expand—particularly in adapting to real-time trading patterns—maintaining a robust and consistent governance and controls framework will become increasingly critical. Such a framework ensures that changes in the operating environment, trading behaviors, and surveillance decision rules are not only well **understood** and **relevant** but also that every decision remains **explainable** and **transparent**.

IV.2. Prospective Effects on Global Markets

This section examines prospective effects of quantum computing on volatility, Quantum Networks and IPOs landscape, highlighting both opportunities and systemic risks that may arise during the transition from research to practical deployment of the technology.

*IV.2.1. **Market Volatility***

Before exploring additional applications of **quantum technology** within market services, it is essential to assess its potential influence on **market volatility**. Volatility serves as an indicator of investor sentiment and reflects the degree of price fluctuations within a specified timeframe. This is an intrinsic aspect of financial markets.

Volatility arising from the advent of quantum technology can be expected on two distinct fronts: **investor sentiment** and **structural inequality**.

Firstly, as quantum computing transitions from research to practical deployment, the early phase is expected to bring about significant **disruption** and volatility, primarily due to investor reactions to announcements and breakthroughs rather than immediate structural changes. Any new development—whether positive or negative—can prompt abrupt price movements as investors respond to emerging information. In this respect, investor behavior toward quantum technology would follow similar pattern of reaction than when previous ground breaking innovative technologies were introduced to the market. For example, last fall's announcement of a collaborative experiment between **HSBC** and **IBM** IBM Quantum Blog (2025), which reportedly enhanced prediction accuracy for bond orders in the European corporate bond market by up to 34%, resulted in a 5% increase in IBM's stock price. Such volatility is typical during the evolution and market integration of new technologies.

Secondlly, beyond sentiment, structural factors may amplify volatility as quantum capabilities become unevenly distributed. Trading firms with early access to quantum computing may gain a **competitive edge**, potentially creating market imbalances and compressing arbitrage windows. These firms could leverage quantum-enabled trading to identify and exploit **mispricing** more effectively, which may reduce **market liquidity** and incentivize other participants to adopt faster or riskier strategies. This dynamic introduces risks of a **Quantum Digital Divide**, similar to F1 racing where top teams benefit from superior engines, data, and engineering talent. In practice, this divide would manifest along several fronts:

a. **Access Inequality** in the financial ecosystem where only large institutions such as JPMorgan, HSBC, Goldman Sachs, and hedge funds like Renaissance Technologies—known for their culture of successfully utilizing sophisticated mathematical and computational strategies—can afford early access to quantum systems or partnerships with companies like IBM, Google, or Rigetti.

b. **Algorithmic superiority** may emerge as proprietary quantum algorithms become trade secrets, giving firms a competitive edge in arbitrage, pricing, and risk management. This could also lead to market manipulation risks, where faster and more accurate predictions allow quantum-equipped firms to front-run trades or exploit inefficiencies before others can even detect them.

Additionally, **disparities** may arise regarding information access and processing efficiency. Firms equipped with advanced quantum computational resources may price derivatives and hedge risks more efficiently than those relying on conventional systems, further influencing market dynamics. This could potentially lead to a **herding effect** where non-quantum powered trading firms could just follow the strategies executed by those having the technology, without understanding their rationales. This could lead to **unexpected price shocks** as competitors without quantum computing would not be able to adjust their positions fast enough when necessary.

Markets will stabilize as access to comparable computational capabilities percolates through the market, supporting fair competition in the long run. Technological advancements inevitably lead to changes, opportunities, temporary gaps, and transitional phases within the environment. These are common occurrences during the initial stages of any major technological shift and are well understood by regulators, industry players, and consumers. Market exchanges have a unique opportunity to guide this transformation in a constructive and secure manner.

*IV.2.2. **Quantum Networking***

If we're building computers that operate with qubits, wouldn't it be great if these systems could also "talk" to each other? This is the long-envisioned goal of *quantum networking*.

A quantum network enables the transmission of qubits across an infrastructure while preserving their entanglement, which is a critical requirement for *true* quantum communication. Importantly, this does not imply faster-than-light signaling (see Section I.1); rather, it allows quantum states to be shared securely and coherently. While classical and quantum processors can communicate using conventional NICs[6], quantum networking and entanglement make clustering quantum compute far more efficient. Once this technology becomes stable and practical, a range of transformative applications could emerge.

According to the *Center for Quantum Networks*, these include **Quantum Key Distribution** (QKD)[7], secure quantum communications, and clustered or distributed quantum computing. While QKD enables secure key exchange, **distributed quantum computing** allows multiple quantum processors to work together across a network, effectively pooling resources for larger or more complex computations. Such capabilities could benefit clients operating servers across multiple locations who need to share updates securely and efficiently. Exchanges could, therefore, leverage these technologies, offering improved **coordination** between stakeholders.

However, the promise of these capabilities is counterbalanced by a fundamental constraint: maintaining entanglement across large networks with multiple point-to-point connections remains challenging without resilient quantum hardware. This limitation is closely tied to the physical constraints of quantum communication, where researchers are actively seeking solutions to extend transmission distances. Currently, photons traveling through fiber optic cables experience loss and scattering, which restricts

[6] NIC: Network Interface Card, a hardware component that connects a computer to a network.

[7] Quantum Key Distribution (QKD) is a secure communication method that uses quantum mechanics to generate and share encryption keys between parties, ensuring that any attempt to eavesdrop can be detected.

direct quantum signal transmission to roughly 100-200 kilometers.

Why does this limitation emerge in quantum communication? In classical systems, each bit is encoded in many photons. If some photons are lost during transmission, it's not critical (classical repeaters can amplify the signal by injecting additional photons). In quantum networking, however, we deal with **individual**, **entangled photons** whose quantum states are unknown and *uncloneable*, due to the *No-Cloning Theorem*.

To overcome this limitation, **quantum repeaters** are being developed. These devices link short quantum connections incrementally using techniques such as **entanglement swapping**, which allows two distant network nodes to become entangled via intermediate pairs of photons, and **entanglement purification**, which improves fidelity by combining multiple imperfect copies. Unlike classical repeaters that amplify signals, quantum repeaters form extended chains that enable quantum information transfer over greater distances, potentially even across continents. Developing reliable quantum repeaters remains a significant technical and scientific challenge. Laboratories worldwide, including *NIST* and *Cisco*, are **actively** building and evaluating early models.

In summary, quantum networking presents tangible opportunities for improving co-location and secure communications, with its implementation currently regarded as **promising**. especially in financial services. A notable example is JPMorgan Chase's successful launch of one of the world's fastest quantum-secured networks in Singapore (Alia et al., 2024), shifting quantum security from theory to practice in a financial setting. Initiated in 2018 with technology partners and researchers, the project reached full deployment by 2023, linking the main data center, trading floor, and four branches. The system uses the aforementioned QKD technology, which detects interception attempts through changes in quantum states. Notably, JPMorgan achieved 100 Gb/s speeds on QKD-secured connections, supporting real-time operations without compromising security or performance—a benchmark for post-quantum readiness in finance.

Recent advancements in academia and technology further highlight the momentum in quantum networking. For instance, an experimental quantum network was established between the campuses of *Rochester Institute of Technology* and *University of Rochester* utilizing optical fiber technology. In addition, Cisco has inaugurated a *Quantum Networking Lab* in Santa Monica and, in collaboration with *UC Santa Barbara*, developed a prototype quantum entanglement chip. Cisco aims to accelerate the realization of practical quantum computing from decades to merely **a few years**.

IV.2.3. New Listings and IPOs

The pursuit of quantum supremacy has led to the emergence of numerous new companies and startups seeking investment to advance their research efforts. Within the technology sector, this trend is expected to continue, with new entrants establishing themselves as key contributors to the field, while established industry leaders strive to enhance their market position through quantum technologies. Exchanges are and will continue to play a key role in providing access to capital to these companies that are looking for investors.

For example, Nasdaq is already home to several quantum computing companies like Rigetti (RGTI), Arqit (ARQQ), and Quantum Computing Inc. (QUBT). There are over 28 notable U.S.-based quantum startups with $2.7B in aggregate funding, many of which could pursue IPOs. While this sector is still early-stages, IPO activity will only increase. This development presents an opportunity for all exchanges to attract additional companies to undertake IPOs on its exchange, as many **startups** are expected to seek capital through market listings. Comparable patterns were observed during the internet bubble and the recent interest in companies specializing in Artificial Intelligence.

Conclusion

Quantum technology is widely regarded as the next significant development in the technological landscape. However, as extensively discussed in this paper, quantum technology remains in its nascent stages, with many applications still theoretical. The most immediate and probable impact will be on **cybersecurity**, highlighting the necessity for organizations to prepare for quantum advancements before these technologies become widely accessible. The 2030 target date set by NIST for **Post-Quantum readiness** has prompted industries to begin addressing the vulnerabilities of classical encryption methods in preparation for quantum-based encryption.

Furthermore, it is important to recognize that, **unlike sectors such as pharmaceuticals** where quantum technology may drive transformational change, the primary benefits for the financial industry—particularly within financial markets infrastructure—will likely focus on **improving existing processes and services**. Quantum computing is expected to enhance market operations, surveillance, and communication efficiency rather than introducing entirely new paradigms.

These advantages are expected to emerge within the next decade to fifteen years. Nevertheless, the quantum technology ecosystem is **advancing at a rapid pace**, and projected timelines and industry milestones may accelerate or change as scientific and engineering breakthroughs continue to emerge. As a result, organizations should **closely monitor developments across the quantum landscape** and adopt a **proactive readiness approach**, regularly evaluating potential opportunities, risks, and strategic implications. Consequently, it is advisable to maintain steady but measured initiatives to ensure successful adoption and preparedness for the quantum transition.

While enthusiasm for participating in the quantum technology race remains high, it is crucial that financial infrastructure providers exercise **prudent oversight** regarding the dissemination, application, and accessibility of this technology. It is critical for the financial industry to establish and uphold **comprehensive frameworks**, **regulations**, and **controls** to preserve market integrity and ensure **equal access to capital** for all stakeholders. In particular, exchanges should maintain close collaboration with NIST, global governmental agencies, and strategic partners such as the main cloud technology providers to develop a coordinated strategy for integrating quantum technology.

Although competition fosters innovation and advancement, collaboration among essential entities—including technology providers, regulators, and financial infrastructure organizations—is vital to achieving efficient and effective adoption of quantum technology.

Acknowledgements

We would like to express our gratitude to John Gardiner for his valuable scientific and technological comments and thoughtful revisions, which improved the clarity and quality of this manuscript. We also extend our sincere thanks to Natalia Hanson for her expert review of the cryptographic considerations, which enhanced the technical accuracy and depth of this paper.

Disclaimer

References

Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M., Lim, C., 2024. 100 gbps quantum-safe ipsec vpn tunnels over 46 km deployed fiber. URL: https://arxiv.org/abs/2405.04415, arXiv:2405.04415.

Bank for International Settlements, 2023. Project Leap: Quantum-proofing the financial system. Technical Report. BIS Innovation Hub Eurosystem Centre. URL: https://www.bis.org/publ/othp67.pdf. accessed: 2025-10-08.

Bard, D., Canon, S., Deslippe, J., et al., 2025. Quantum computing for scientific applications: A report from the nersc quantum computing program. URL: https://arxiv.org/abs/2509.09882, arXiv:2509.09882.

Farhi, E., Goldstone, J., Gutmann, S., 2014. A quantum approximate optimization algorithm. arXiv preprint arXiv:1411.4028 URL: https://arxiv.org/abs/1411.4028, doi:10.48550/arXiv.1411.4028. accessed: 2025-10-08.

Freund, J., 2024. The role of the risk sin-eater. ISACA Newsletter 9. URL: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-9/the-role-of-the-risk-sin-eater. accessed: 2025-10-10.

Global Risk Institute, 2023. 2023 Quantum Threat Timeline Report. Technical Report. Global Risk Institute. URL: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/. accessed: 2025-10-10.

Hidary, J.D., 2021. Quantum Computing: An Applied Approach. 2 ed., Springer. URL: https://link.springer.com/book/10.1007/978-3-030-83274-2, doi:10.1007/978-3-030-83274-2.

IBM Quantum Blog, 2025. Hsbc and ibm demonstrate quantum-enabled algorithmic bond trading. URL: https://www.ibm.com/quantum/blog/hsbc-algorithmic-bond-trading. accessed November 17, 2025.

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., Cooper, D., 2024. Transition to Post-Quantum Cryptography Standards. NIST Internal Report (IR) NIST IR 8547 ipd. National Institute of Standards and Technology. Gaithersburg, MD. URL: https://doi.org/10.6028/NIST.IR.8547.ipd, doi:10.6028/NIST.IR.8547.ipd. accessed: 2025-10-08.

Quantum Zeitgeist, 2025. Quantum computing companies. URL: https://quantumzeitgeist.com/quantum-computing-companies/. accessed June 29, 2026.

Soller, H., Bogobowicz, M., Zhang, A., Heid, A., Raschke, R., 2025a. The quantum revolution in pharma: Faster, smarter, and more precise. URL: https://tinyurl.com/54eeyjpx. accessed: 2025-10-08.

Soller, H., Gschwendtner, M., Shabani, S., Svejstrup, W., 2025b. The year of quantum: From concept to reality in 2025. URL: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025. quantum Technology Monitor 2025, accessed 2026-06-29.

The Quantum Insider, 2026. How many quantum chip companies are there? URL: https://thequantuminsider.com/2026/06/05/how-many-quantum-chip-companies-are-there/. accessed June 29, 2026.

The White House, 2022. National security memorandum on promoting u.s. leadership in quantum computing while mitigating risks to vulnerable cryptographic systems. https://tinyurl.com/y9e3krtk. Accessed: 2025-10-10.