FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN

Quantum: Shaping The Next Decade of Financial Technologies

Nov 2025

About

The Global Finance & Technology Network (GFTN) is a Singapore-headquartered organisation that leverages technology and innovation to create more efficient, resilient, and inclusive financial systems through global collaboration. GFTN hosts a worldwide network of forums (including its flagship event, the Singapore FinTech Festival); advises governments and companies on policies and the development of digital ecosystems and innovation within the financial sector; offers digital infrastructure solutions; and plans to invest in financial technology startups through its upcoming venture fund, with a focus on inclusion and sustainability.

GFTN
Innovating Finance. For Everyone.

For more information, visit www.gftn.co

The Singapore FinTech Festival is a global nexus where policy, finance, and technology communities converge. Designed to foster impactful connections and collaborations, SFF is a platform to explore the intersections of cutting-edge financial solutions, evolving regulatory landscapes, and the latest technological innovations.

SINGAPORE FINTECH FESTIVAL™ CELEBRATING 10 YEARS

Through insightful sessions, roundtables, workshops, exhibitions and much more, SFF is an immersive discovery and dialogue of the future trajectories of financial services and the overarching digital transformation reshaping global economies.

For more information, visit www.fintechfestival.sg

Contents

Executive Summary

The 2025 Nobel Prize in Physics was awarded to John Clarke, Michel Devoret, and John Martinis for their experiments revealing macroscopic quantum mechanical tunnelling in electrical circuits, a discovery that demonstrates quantum physics on a larger macroscopic scale. This work is a foundational achievement for developing quantum technologies like quantum computers, quantum sensors and quantum cryptography.[1]

Quantum technologies have evolved from a theoretical curiosity into a strategic imperative for the financial services industry, marking a pivotal shift from experimental research to tangible pilot deployments. The past decade had seen the technology mature from a laboratory concept into a credible domain for financial research and development, with nearly 80% of the world's 50 largest banks now exploring quantum applications.[2] This acceleration is driven by the dual nature of quantum technology: it presents both unprecedented opportunities for computational advantage and an imminent threat to global cryptographic security.

The central challenge is "Q-day" - the point at which a quantum computer will be capable of breaking current encryption standards that protect everything from financial transactions and blockchain networks to critical infrastructure. In response, regulations such as the United States (US) National Security Memorandum 10[3] and United Kingdom's National Cyber Security Centre guidance[4] have set a 2035 deadline for migrating to post-quantum cryptography (PQC), creating a clear timeline for institutional action. Financial institutions are not only preparing defences but also actively seeking a "quantum advantage" through near-term applications. These include hybrid quantum-classical systems for risk modelling, quantum-inspired algorithms for trade optimisation, and quantum machine learning for fraud detection.

Global investment reflects the potential of quantum technologies, with cumulative public funding surpassing US$54 billion (B) and private investment in quantum firms reaching over US$1.25B in Q1 2025[6] alone. Governments and financial authorities are fostering this growth through strategic initiatives. Singapore, for instance has committed over S$300 million through its National Quantum Strategy[7] and an additional S$100 million via the Monetary Authority of Singapore (MAS)[8], to establish itself as a quantum hub.

Despite this momentum, significant technical barriers remain, including quantum bits (qubit) stability, error correction, and hardware scalability, which currently limit quantum computing to specialised use cases rather than mission-critical operations. However, the trajectory is clear: quantum technology is poised to reshape finance, and proactive engagement is no longer optional but essential for future competitiveness and security.

1. Nobel Prize (2025), Press release: Nobel Prize in Physics 2025
2. Tech Informed (2025), JPMorgan and HSBC lead global banks in quantum technology race
3. SEC (2025), Post-Quantum Financial Infrastructure: A Roadmap for the Quantum-Safe Transition of Global Financial
4. Quantum Computing Report (2025), UK's NCSC Sets 2035 Deadline for National Migration to Post-Quantum Cryptography
5. McKinsey (2025), Quantum Technology Monitor 2025
6. Future Markets (2025), The Global Quantum Technology Industry 2025: Technologies, Markets, Investments and Opportunities
7. NQO (2024), National Quantum Strategy
8. MAS (2024), Quantum Computing Programme

1 Celebrating a Decade of Progress

1.1. Introduction: Quantum at the Frontier of Finance

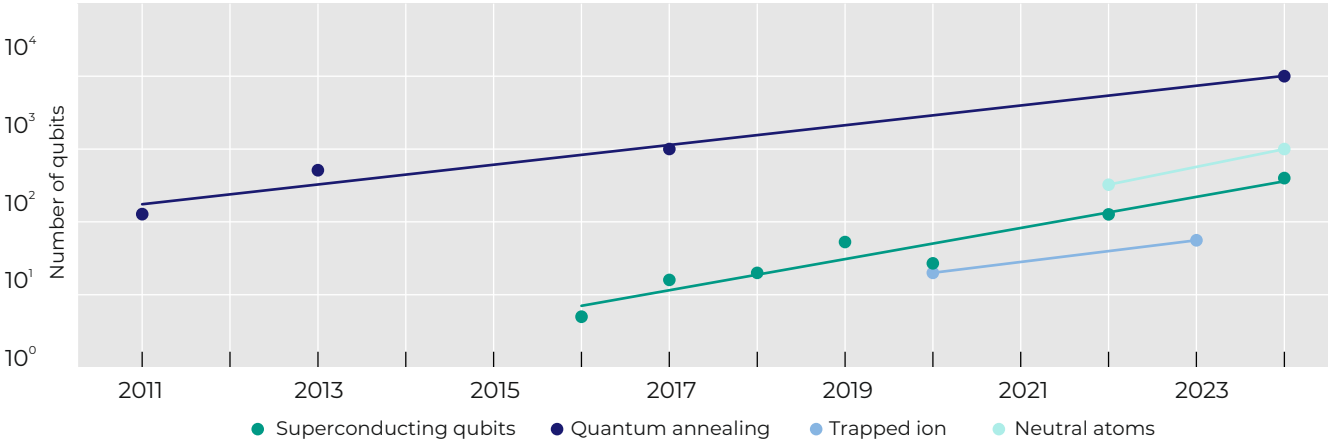
The last decade has been defined by the acceleration of emerging technologies in finance. Artificial intelligence (AI), digital assets and distributed infrastructure such as cloud computing and blockchain have started to reshaped markets, yet quantum technologies have consistently held a unique position: a frontier, highly complex, but deeply transformative technology whose commercial promise for financial services has steadily matured. From 2016's laboratory curiosity, quantum technologies are now increasingly part of strategic roadmaps. The Monetary Authority of Singapore (MAS) and Global Finance & Technology Network (GFTN) have posited quantum computing alongside AI and tokenisation as cornerstone technologies that will shape the next decade of financial services.[9]

McKinsey has estimated quantum computing use cases in financial services could generate up to US$400-600 billion in economic value by 2035.[10]

The urgency of quantum adoption is underscored by the dual nature of quantum impact: **quantum opportunity** and **quantum threat**. While quantum computers promise unprecedented computational capabilities for portfolio optimisation and risk modelling, they simultaneously threaten current cryptographic standards protecting financial systems. The United States (US) National Institute of Standards and Technology (NIST) has required the adoption of post-quantum cryptography within the next 10 years.[11]

In 2016, quantum hardware was largely confined to research institutions with limited quantum bit (qubit) counts, high noise, and low coherence. By 2025, higher qubit counts, hardware improvements, error mitigation techniques, quantum cloud access, and hybrid algorithmic frameworks have made quantum a credible domain for financial research and development and pilot deployment. Google and IBM both claim the decades-long quantum race towards building a full scale industrial-grade machines are near completion with such machines being potentially available before 2030.[12]

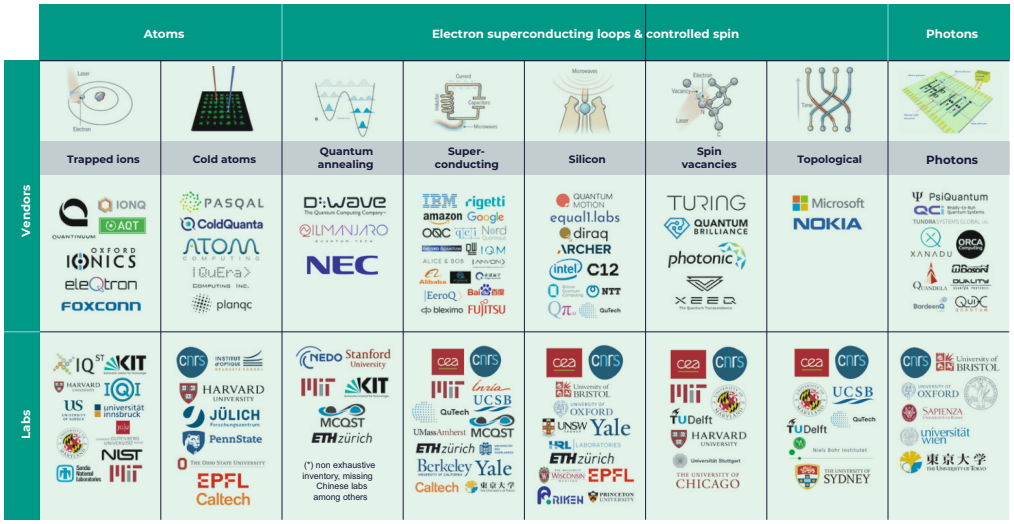
Fig. 1: Evolution of Quantum Computing capabilities



Source: BIS (2025), Quantum-readiness for the financial system: a roadmap
BIS authors' elaborations based on companies' communication

9. MAS (2025), Singapore FinTech Festival Celebrates its 10th Anniversary
10. McKinsey (2025), Quantum Technology Monitor 2025
11. Keyfactor (2025), NIST Drops New Deadline for PQC Transition
12. Computing (2025), Google and IBM latest to claim quantum race is nearing end

Fig. 2: Landscape of Quantum Computing players



Source: Arthur D. Little (2022) Unleashing the business potential of quantum computing

1.2. Early Experimentation to Strategic Investment

In 2016, IBM made a 5-qubit computer accessible via the internet, aiming to stimulate interest and experimentation with quantum technology.[13] Before the 2020s, financial institutions took early interest to experiment with quantum use case, partnering tech incumbents and quantum startups, linking up with academia and government agencies, and even made early investments in quantum computing players.[14]

By the early 2020s, quantum began crossing a perception threshold. Improvements in coherence times, gate fidelities[15], error mitigation, and modular architectures gave credence to medium term fault-tolerant quantum computing (FTQC) that are designed to perform accurate calculations despite the errors inherent in its physical components. Cloud-based quantum access also lowered the barrier to experimenting with quantum systems[16] without needing full in-house infrastructure.

These early years established the foundational understanding that quantum computing could address financial services' most computationally intensive challenges. This includes optimising market trading and investment processes, risk management, enhancing the efficiency of payment processing, dynamic optimisation of portfolio holdings, and enhancing the security of firms' digital communication systems (through quantum key distribution).[17]

By 2023 - 2025, experimentation in finance moved from theory to testing use cases. Some major financial services quantum initiatives are listed below.

- **HSBC** piloted quantum-secure technology including post-quantum cryptography for tokenized gold transactions in September 2024.[18] HSBC also demonstrated the first known quantum-enabled algorithmic bond trading with IBM in September 2025, providing empirical evidence of current quantum computers' potential value.[19]
- **Turkish bank Yapı Kredi** used quantum computing to model and identify failure points in its Small and Medium sized Enterprises (SME) networks, completing analysis in seconds that would traditionally take years.[20]
- **Italian bank Intesa Sanpaolo** explored quantum machine learning (using variational quantum circuit-based classifiers) for fraud detection, achieving better accuracy than traditional methods with quantum-enhanced algorithms.[21]
- **Santander** investigated quantum-inspired algorithms for bond-hedging strategies, demonstrating faster execution and improved scalability.[22]

These case studies represent the transition from theoretical research to tangible applications that could deliver value to financial institutions worldwide.

As of 2025, **nearly 80% of the 50 largest banks worldwide were exploring or engaging quantum technology,** signalling the shift from experimentation to strategic investment.[23]

13. TechTarget (2025), The History of Quantum Computing: A Complete Timeline
14. BCG (2020), Time for Financial Institutions to Place Quantum Bets
15. IQM (2024), IQM Quantum Computers achieves new technology milestones with 99.9% 2-qubit gate fidelity and 1 millisecond coherence time
16. WEF (2022), State of Quantum Computing
17. G7 Cyber Experts Group (2024), G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quant
18. HSBC (2024), HSBC pilots quantum technology for tokenised gold
19. HSBC (2025), HSBC demonstrates world's first-known quantum-enabled algorithmic trading with IBM
20. WEF (2025), Quantum Technologies Key Strategies and Opportunities for Financial Services Leaders 2025
21. WEF (2025), Quantum Technologies Key Strategies and Opportunities for Financial Services Leaders 2025
22. WEF (2025), Quantum Technologies Key Strategies and Opportunities for Financial Services Leaders 2025
23. Tech Informed (2025), JPMorgan and HSBC lead global banks in quantum technology race

Spotlight Regional Leadership: Singapore's Quantum Strategy

Singapore seeks to establish itself as Asia's quantum technologies hub through decisive government action and public-private collaboration.

In May 2024, **Singapore's National Quantum Strategy** was launched with S$300 million allocated over five years for quantum research and talent development. This strategy included four key initiatives: advancing scientific excellence by upgrading the Centre for Quantum Technologies (CQT) to a flagship national centre, building critical engineering capabilities by establishing a National Quantum Processor Initiative (NQPI) to design and build local quantum processors, and expanding the Quantum Engineering Programme (QEP) with a new National Quantum Sensor Programme. It also sought to foster a vibrant innovation and enterprise ecosystem and nurture a pipeline of deep tech talent via the National Quantum Scholarships Scheme (NQSS) to support talent development.[24]

The Monetary Authority of Singapore (MAS) also launched the **Quantum Computing Programme** in July 2024 to advance quantum-related innovation and adoption in financial services and committed up to S$100 million through the Financial Sector Technology & Innovation Scheme (FSTI 3.0) Quantum Track, specifically supporting quantum capabilities in financial institutions.[25]

OCBC Bank partnered with the National University of Singapore, Nanyang Technological University, and Singapore Management University for quantum research in derivative pricing by accelerating Monte Carlo simulations, post-quantum cryptography to enhance data security, and quantum machine learning techniques to enhance fraud detection respectively.[26] HSBC selected Singapore for its second global Quantum Centre of Excellence, focusing on quantum-safe security including post-quantum cryptography, quantum key distribution, and hybrid cryptographic frameworks.[27] These institutions also participated in MAS's industry-wide Quantum Key Distribution sandbox alongside DBS, UOB, SPTel, and SpeQtral, testing secure financial communications infrastructure and publishing a technical report to share their learnings.[28]

This was in addition to MAS' groundbreaking joint experiment in post-quantum cryptography with Banque de France (BdF) in November 2024 where they successfully exchanged digitally-signed and encrypted emails using PQC algorithms, namely CRYSTALS-Dilithium (Module-Lattice-Based Digital Signature Standard, ML-DSA) and CRYSTALS-Kyber (Module-Lattice-Based Key-Encapsulation Mechanism Standard, ML-KEM) across continents using current Internet technologies. For next stage of experimentation, MAS and BdF aim to extend PQC to critical financial transactions, particularly cross-border transactions on payment networks.[29]

MAS has also published an advisory on addressing cybersecurity risk associated with quantum to financial institutions in February 2024 which required them to (i) actively monitor advancements in quantum technology and associated cybersecurity risk, (ii) maintain a record of all cryptographic assets within their systems, prioritise the migration of critical assets to quantum-resistant encryption and key distribution, and (iii) develop strategies and build capabilities to counter cybersecurity risks associated with quantum.[30]

This coordinated approach positions Singapore as both innovator and implementer, creating an ecosystem where research advances translate to commercial applications while maintaining robust security standards.

24. NQO (2024), National Quantum Strategy
25. MAS (2024), Quantum Computing Programme
26. CQT (2025), CQT researchers to collaborate with OCBC on quantum computing
27. HSBC (2025), HSBC selects Singapore for its second Quantum Centre of Excellence
28. MAS (2025), MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications within the Financial Sector
29. MAS (2024), Banque de France and Monetary Authority of Singapore Conduct Groundbreaking Post-quantum Cryptography Experiment to Enhance Communication Security
30. MAS (2024), MAS Quantum Advisory

2 Building Pathways for Growth

Within the next decade, growth in quantum technologies for financial services will be driven by proactive cybersecurity, near-term applications like quantum-inspired optimisation, and the long-term integration of fault-tolerant quantum computing. Financial institutions are already exploring hybrid approaches and investing to prepare for both the opportunities and risks posed by this emerging technology.

2.1. Key Quantum Breakthrough Announcements

Several major companies announced landmark quantum breakthroughs in late 2024 and 2025 listed below, marking a pivotal inflection point for the industry. The most significant contributions came from a mix of tech giants, deep-tech startups, and research-driven firms focused on scaling qubits, improving error correction, and commercialising hybrid quantum systems.

Company	Breakthrough	Details
Microsoft	Majorana 1 topological qubit chip	Microsoft introduced the world's first Majorana 1 processor based on topological superconductors. This design embeds fault tolerance at the hardware level, reducing the need for complex software corrections and paving the way to million-qubit scalability.[31]
Google (Alphabet)	Willow quantum chip and Quantum Echoes algorithm	Google's 105-qubit Willow chip demonstrated real-time quantum error correction[32] and claims to run its new verifiable Quantum Echoes (out-of-order time correlator) algorithm 13,000 times faster than classical supercomputer.[33]
IBM	Condor and Nighthawk processors	IBM announced Nighthawk and expanded its 1,121 qubits Condor processor[34] with advanced error-correction capabilities. These milestones strengthen IBM's roadmap toward a large-scale, fault-tolerant quantum computer called Quantum Starling.[35]
Amazon Web Services	Ocelot bosonic chip	AWS introduced Ocelot, the company's first bosonic cat qubit architecture, supporting error correction. Enhancing AWS's integrated quantum-classical infrastructure.[36]
IonQ	Record two qubit-gate fidelity	IonQ expanded into quantum sensing and achieved 99.99% two-qubit gate fidelity on a trapped-ion platform, among the highest reported for quantum systems.[37]

2.2.The threat of Q-day

Q-day is the anticipated date when large-scale quantum computers become powerful enough to break the public-key encryption methods that currently secure most of our sensitive digital data. This event represents a significant cybersecurity threat that necessitates a transition to new, quantum-resistant security standards.

Modern public-key encryption, such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC), relies on mathematical problems that are currently very hard for classical computers to solve in a reasonable amount of time. However, a sufficiently powerful quantum computer, using algorithms like Shor's, could solve these problems quickly. This would fundamentally compromise today's cryptographic infrastructure:

- **Encrypted Transport Layer Security (TLS) communications**, including financial transactions, secure web browsing (HTTPS), and virtual private networks (VPNs) by deriving private keys from public ones, undermining core internet security protocols.[38]
- **Blockchain systems** including Bitcoin and Ethereum, which rely on Elliptic Curve Digital Signature Algorithm (ECDSA) encryption are susceptible to Shor's Algorithm; by the early 2030s, these digital signatures and private keys could be reverse-engineered, unless networks migrate to quantum-resistant schemes.[39]
- **Critical infrastructure**, including government, healthcare, financial, security and defence information will be exposed to quantum threats given that they rely on encryption for secure communication and system integrity.[40]

A new global study from the Capgemini Research Institute released in July 2025 showed nearly two-thirds (65%) of 1,000 global organisations they surveyed now see quantum computing as the most critical cybersecurity threat they will face within the next three to five years. 70% of respondents say they are currently working on or planning to use quantum-safe solutions in the next five years.[41]

31. Quantum Insider (2025), Quantum Computing Roadmaps & Predictions of Leading Players
32. Google (2024), Meet Willow, our state-of-the-art quantum chip
33. Google (2025), The Quantum Echoes algorithm breakthrough
34. Techfunnel (2025), Quantum Computing in 2025: Real-World Industry Breakthroughs and the Next Digital Revolution
35. CNBC (2025), IBM announces new quantum processor, plan for Starling supercomputer
36. Amazon Science (2025), Amazon announces Ocelot quantum chip
37. IonQ (2025), IonQ Achieves Landmark Result, Setting New World Record in Quantum Computing Performance
38. IBM (2024), Quantum Safe IBM MQ. Actions you can take now.
39. CoinCentral (2025), Quantum Computing Threatens Bitcoin and Ethereum Security, Mysten Labs Warns
40. European Parliament Research Service (2024), Cryptographic security: A question for Europe's digital sovereignty
41. Capgemini (2025), CRI PQC Research

2.3. Near Term Focus

The near term focus is on mitigating risks, building knowledge, and leveraging hybrid approaches that combine classical computing with early quantum systems.

Post-quantum cryptography (PQC) transition: Financial institutions are starting to transition to new encryption standards such as NIST Federal Information Processing Standards (FIPS) 203 (for general encryption using ML-KEM), FIPS 204 (for digital signatures using ML-DSA), FIPS 205 (for stateless hash-based digital signatures SLH-DSA) to defend against future quantum attacks[42], in which encrypted data is harvested now for later decryption ("harvest now, decrypt later"). US NIST has announced it would depreciate traditional public key cryptography (RSA and ECDSA) by 2030 where data owners must examine security risk potential and decide whether to continue using these algorithm and key strength, and it would disallow them by 2035. 2035 is also the primary target year for completing the migration to PQC across US Federal systems.[43]

United Kingdom's National Cyber Security Centre (NCSC) has also formalised a 2035 PQC migration roadmap for financial institutions.[44]

European Union (EU) roadmap recommends member states to start transition to post-quantum cryptography by the end of 2026, complete transition for critical infrastructure before 2030 and as many systems as possible before 2035.[45]

48% of banks surveyed by Capgemini intend to adopt PQC in the next 2 years while a further 33% plan to adopt it within 3 to 5 years.[46]

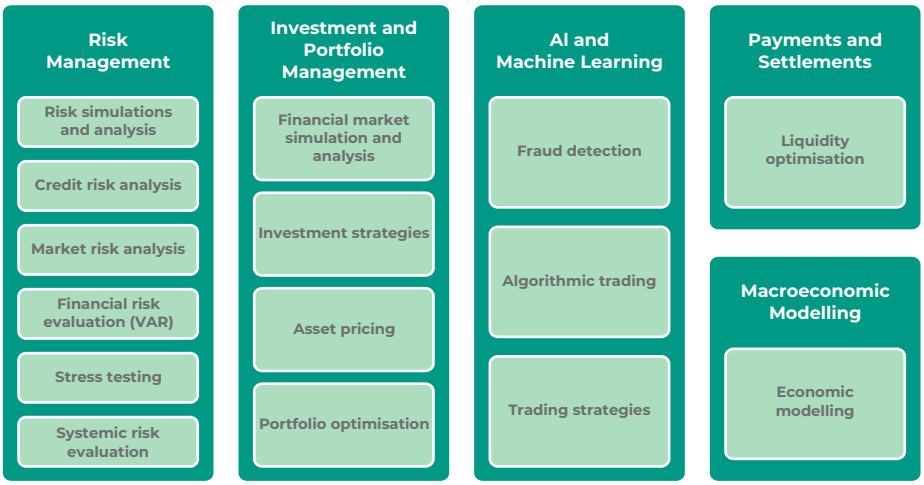
PQC however faces implementation challenges. New algorithms require more processing power, memory, and bandwidth than today's cryptography. PQC is not a simple replacement for current encryption. It requires substantial work to integrate with existing systems and software. The new algorithms must also be rigorously tested to ensure they meet security and performance standards. Larger key sizes, more intensive computations, and higher precision requirements also mean PQC algorithms are not a straightforward substitution.[47]

Quantum Key Distribution (QKD): Experiments with QKD, a method for generating unbreakable encryption keys using quantum mechanics, are underway to protect sensitive communications, including trials by central banks like MAS.[48] Financial infrastructures will increasingly depend on QKD and quantum-secure communications. Building quantum communication networks integrated with next-generation financial market infrastructures can help ensure transaction integrity and shield critical assets from post-quantum threats. Singapore's Infocomm Media Development Authority (IMDA) launched Southeast Asia's first quantum-safe network infrastructure, National Quantum-Safe Network Plus (NQSN+) in 2023.[49]

Quantum-inspired optimisation (QIO): As a stepping stone to full quantum computing, financial firms are using classical algorithms that are inspired by quantum principles. These are already being used to improve optimisation problems like fraud detection, portfolio modelling, and trading algorithms. Microsoft Azure Quantum has demonstrated measurable improvements in anomaly detection for payment systems using QIO.[50]

Hybrid quantum-classical applications: In the short term, quantum computing has been used to boost the accuracy

Fig. 3: Potential advantages of Quantum applications in Financial Sector



Source: BIS (2024), Quantum computing and the financial system: opportunities and risks
BIS authors' elaborations

42. NIST (2025), Post-Quantum Cryptography
43. NIST (2024), NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards
44. Quantum Computing Report (2025), UK's NCSC Sets 2035 Deadline for National Migration to Post-Quantum Cryptography
45. EC (2025), Roadmap for the Transition to Post-Quantum Cryptography
46. Capgemini (2025), CRI PQC Research
47. BIS (2025), Quantum-readiness for the financial system: a roadmap
48. MAS (2025), MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications within the Financial Sector
49. IMDA (2025), Singapore's National Quantum-Safe Network Plus (NQSN+)
50. Microsoft (2022), Improving financial services anomaly detection with Mphasis and Azure Quantum

and speed of classical calculations. These hybrid systems use quantum processors for computationally intensive tasks, offering a potential quadratic speedup over classical Monte Carlo methods, while classical computers handle other aspects of the workflow.[51]

Quantum AI Synergy

Quantum Computing (QC) and AI have significant synergies. QC could accelerate AI training and overcome computational limits, while AI could speed up QC development. Major players are pursuing synergies between AI and quantum computing.

- **Nvidia** announced its Accelerated Quantum Computing Research Center (NVAQC) in March 2025 to integrate quantum hardware with AI supercomputing infrastructure. The centre aims to move quantum development from research to real-world scaling, with dedicated facilities and industrial partnerships to scale quantum hardware by integrating with conventional AI supercomputers at NVAQC, correct quantum errors through AI decoding and simulating new quantum processing units.[52]

- **Quantinuum** introduced Generative Quantum AI (GenQAI) in February 2025, which uses quantum-generated data to improve AI applications, such as financial modelling. This project shows a path toward hybrid AI-quantum systems for developing scalable, real-world solutions. The launch signals growing commercial readiness, moving beyond theory toward scalable, real-world AI solutions enhanced by quantum capabilities.[53]

Quantinuum's research team has also investigated quantum recurrent neural networks (qRNNs) as an alternative to traditional deep-learning models. These quantum-enhanced architectures could perform natural language processing (NLP) tasks more efficiently without sacrificing accuracy which represents a significant saving from the huge computational power that large language models such as GPT-4 demand.[54]

2.4. Regulatory Approaches

Bank for International Settlements (BIS) Innovation Hub's Project Leap initiative was designed to prepare the global financial system, and particularly central banks, for the cybersecurity challenges posed by future quantum computing capabilities. In 2023, BIS successfully demonstrated a quantum safe communication channel between Paris and Frankfurt, ensuring that highly sensitive payment data could be transmitted securely over a quantum resistant virtual private network (VPN).[55] Phase 2 focuses on quantum-proofing payment systems by exploring the implementation of post-quantum cryptography in a European payment system.[56]

BIS also reiterated in its "Quantum-readiness for the financial system: A roadmap" report that Q day represents an imminent threat to the financial system and preparedness is an urgent priority for all financial authorities. A phased transition plan combining cryptographic agility, migration pilots, and international coordination is essential to maintaining financial stability in the quantum era.[57]

The US Securities and Exchange Commission (SEC) has also proposed a Post-Quantum Financial Infrastructure Framework (PQFIF)[58] to enable a secure, orderly, and verifiable transition to post-quantum cryptographic standards, supporting the SEC's mandate to protect investors and ensure the integrity of US financial markets. It has particular focus to address the unique vulnerabilities of the digital asset ecosystem.

In the European Union, the Digital Operational Resilience Act (DORA) draft technical standards require financial entities to prepare for the security threat posed by future quantum advancements.[59]

The Bank of England has adopted a proactive policy of engagement with the quantum technology ecosystem as part of its innovation roadmap. Through its collaboration with the Financial Conduct Authority (FCA) and the Cross Market Operational Resilience Group (CMORG), it is studying the systemic and supervisory impacts of quantum computing, particularly on market integrity and data security.[60]

MAS meanwhile adopts a multiprong approach of industry guidance through advisory[61], support through dedicated quantum capabilities grants[62] and industry partnerships[63]. The Cyber Security Agency of Singapore (CSA) has also announced in Oct 2025 a quantum readiness index (QRI) and quantum-safe handbook. QRI is a self-assessment tool for system owners and security practitioners to gauge their readiness for quantum threats and prioritise key actions for their migration journey while the quantum-safe handbook provides detailed guidance on transition to quantum-safe cryptography for organisations, particularly critical information infrastructure (CII) owners and government agencies.[64]

51. World Quantum Summit (2025), Portfolio Stress Testing with Quantum Monte Carlo: Revolutionizing Financial Risk Management
52. Nvidia (2025), NVIDIA Accelerated Quantum Computing (NVAQC) Research Center
53. Quantinuum (2025), Announces Generative Quantum AI Breakthrough with Massive Commercial Potential
54. Quantum Insider (2025), Quantinuum Touts Generative Quantum AI's Massive Commercial Potential
55. BIS (2023), Press release: Project Leap proves the viability of a quantum-safe financial system
56. BIS (2025), Project Leap: quantum-proofing the financial system
57. BIS (2025), Quantum-readiness for the financial system: a roadmap
58. SEC (2025), Post-Quantum Financial Infrastructure: A Roadmap for the Quantum-Safe Transition of Global Financial
59. ESMA (2024), JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework
60. BoE (2025), The Bank of England's approach to innovation in artificial intelligence, distributed ledger technology, and quantum computing
61. MAS (2024), MAS Quantum Advisory
62. MAS (2024), MAS Commits up to S$100 Million to Support Quantum and Artificial Intelligence Capabilities in the Financial Sector
63. MAS (2025), MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications within the Financial Sector
64. GovInsider (2025), Agentic AI, quantum represent extraordinary moment in tech, says Singapore's Digital Minister

Public - Private Innovation Partnership

The expansion of public-private alliances among central banks, Fintechs, academia, and technology firms is becoming critical for shaping the future of quantum finance. These partnerships are driving global efforts to define standards, interoperability frameworks, and responsible innovation guidelines for emerging quantum technologies in the financial sector. The 2025 "US National Quantum Initiative Annual Report" by the National Science and Technology Council highlighted increasing collaboration between industry, academia, and federal agencies to harmonise regulatory standards and strengthen post quantum resilience across financial infrastructures.[65]

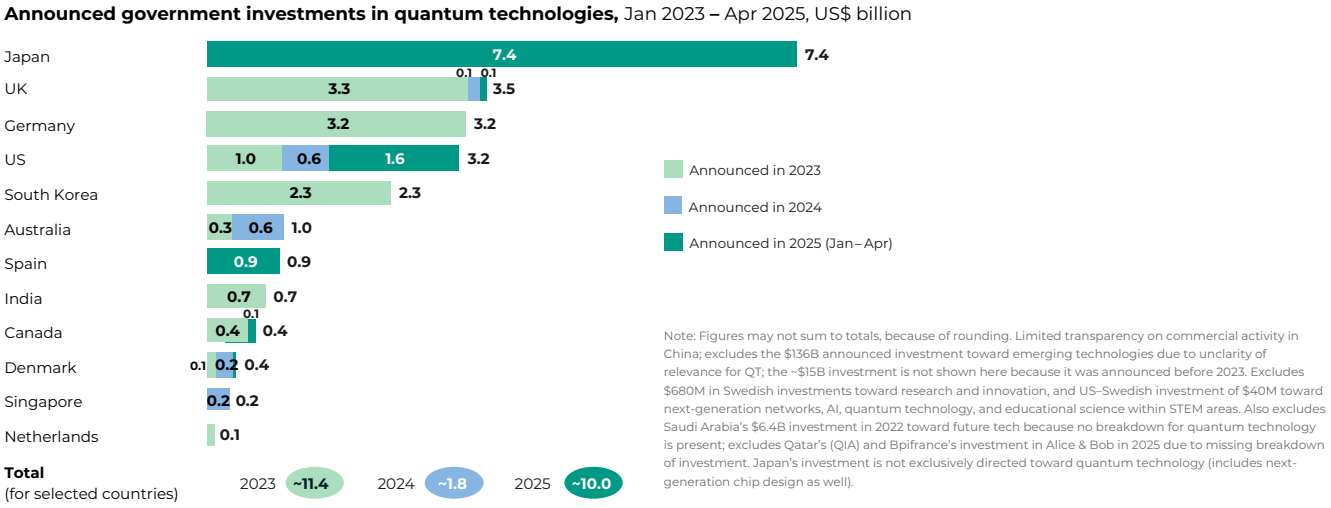
2.5. Investments

Public investments in quantum technology worldwide have surpassed **US$54 billion** cumulatively. While another US$10 billion of public investments have been announced as of April 2025 after dropping to around US$1.8 billion in 2024 from US$11.4 billion in 2023 (Figure 4).[66]

The quantum computing industry has also attracted significant private funding growth, Q1 2025 investments in quantum computer companies exceeded **US$1.25 billion**, a 125% increase from Q1 2024. Major funding rounds included IonQ (US$360 million), QuEra Computing (US$230 million), Quantum Machines (US$170 million), and D-Wave Systems (US$150 million).[67]

Quantum computing was one of 27 specified sub-areas that JPMorgan plans to invest in as part of its decade long Security and Resiliency Initiative.[68]

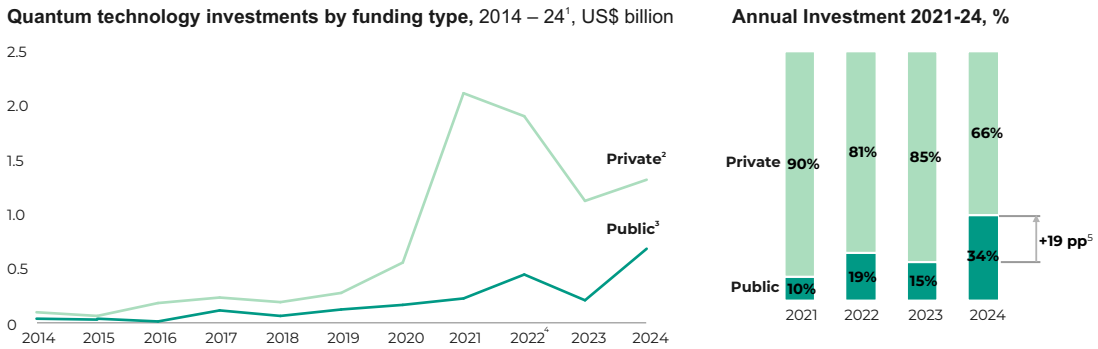
Fig. 4: Public Investments in Quantum Technologies



Note: Figures may not sum to totals, because of rounding. Limited transparency on commercial activity in China; excludes the $136B announced investment toward emerging technologies due to unclarity of relevance for QT; the ~$15B investment is not shown here because it was announced before 2023. Excludes $680M in Swedish investments toward research and innovation, and US–Swedish investment of $40M toward next-generation networks, AI, quantum technology, and educational science within STEM areas. Also excludes Saudi Arabia's $6.4B investment in 2022 toward future tech because no breakdown for quantum technology is present; excludes Qatar's (QIA) and Bpifrance's investment in Alice & Bob in 2025 due to missing breakdown of investment. Japan's investment is not exclusively directed toward quantum technology (includes next-generation chip design as well).

Source: McKinsey (2025), Quantum Technology Monitor

Fig. 5: Public and Private investments in Quantum Technology start ups



[1]Based on investment data recorded in PitchBook; actual investment likely higher (excluding investments with missing details on investment types); data availability on start-up investment in China is limited. [2]Including investments from venture capital funds, hedge funds, corporations, angel investors, and accelerators. [3]Including investments from governments, sovereign wealth funds, and universities. [4]Excluding other uncategorized funding data. [5]Percentage points.

Source: McKinsey (2025), Quantum Technology Monitor

65. US NSTC (2025), National Quantum Initiative supplement to the President's 2025 Budget request
66. McKinsey (2025), Quantum Technology Monitor 2025
67. Future Markets (2025), The Global Quantum Technology Industry 2025: Technologies, Markets, Investments and Opportunities
68. JPMorganChase (2025), Launches $1.5 Trillion Security and Resiliency Initiative to Boost Critical Industries

3 Addressing Unresolved Challenges

Technical Barriers to Scalability

Despite remarkable progress in hardware and algorithm design, fundamental technical challenges constrain quantum computing's near-term impact and long-term potential. Addressing these barriers requires sustained research investment and engineering innovation across multiple dimensions.

Qubit Stability and Coherence

Quantum bits (qubits) are extremely sensitive to external noise, vibration, and electromagnetic interference, losing quantum states through decoherence within microseconds or milliseconds due to environmental interference. IBM's superconducting qubits currently maintain coherence for roughly 100 - 200 microseconds, which limits level of complexity in computations. Error rates for basic quantum gate (building blocks of quantum circuits) operations, often 0.1-1% per gate, require extensive error correction consuming additional qubits. Currently creating a single stable "logical qubit" demands thousands of physical qubits, a threshold current hardware cannot meet.[69] IBM scientists proposed in March 2025 a new quantum error-correction Gröss code which they claim can protect 12 logical qubits for nearly a million cycles of error checks using just 288 qubits a 10 times reduction from 3,000 qubits need using current leading surface code, this they claim clears a major hurdle toward building practical, large-scale quantum computers.[70]

Scaling Challenges

While companies like IBM have built processors with 1,000+ qubits, these systems lack connectivity and uniformity needed for complex algorithms. Adding qubits increases unital noise and crosstalk (unwanted qubit interactions), degrading performance and accuracy. IBM's 433-qubit Osprey processor still battles with error rates preventing most real-world applications.[71] Engineering consistent performance across all qubits, critical for reliable computation, remains elusive.

Quantum Control System Constraints

Current control systems were engineered to manage small-scale quantum processors containing 1 to 1,000 qubits, where each qubit requires customied calibration procedures and dedicated control resources. Whereas a fault-tolerant quantum computer would need to control 100,000 to 1,000,000 qubits concurrently.[72] Scaling quantum computers to millions of qubits requires revolutionary control architectures. Current electronics would demand extremely large facilities with enormous power requirements if scaled without design changes. Miniaturisation through chip-level redesign, improved interconnectivity for real-time error correction, and reduced per-qubit control costs represent essential innovation frontiers.[73]

Environmental Requirements

Superconducting qubits require operation near absolute zero temperatures, necessitating sophisticated cryogenic systems whereas Trapped-ion systems need ultra-high vacuum chambers and precise laser control.[74] Maintaining quantum states demands extreme isolation from vibration, electromagnetic interference, and thermal fluctuations. These environmental constraints limit quantum computing accessibility and increase operational costs significantly.

Software and Algorithm Development

Hardware advances must be matched by software progress. Quantum algorithms for financial applications remain nascent, with limited libraries and development tools. Translating business problems into quantum-compatible formulations requires specialised expertise. The gap between quantum hardware capabilities and practical applications persists due to insufficient software maturity.[75]

Operational Reliability

Quantum systems remain operationally fragile, requiring frequent calibration, experiencing downtime for maintenance, and producing unreliable results when operating outside optimal conditions. Financial services applications demand high reliability and consistent performance, standards that current quantum computers struggle to meet. Until operational reliability improves, quantum computing will remain unsuitable for mission-critical financial processes requiring guaranteed uptime.

69. Milvus (2025), What are the limitations of current quantum computing hardware?
70. Quantum Insider (2025), IBM Reports 10 Times More Efficient Error-Correcting Method Brings Practical Quantum Computers Closer to Reality
71. Milvus (2025), What are the limitations of current quantum computing hardware?
72. McKinsey (2024), Quantum control's role in scaling quantum computing
73. McKinsey (2024), Quantum control's role in scaling quantum computing
74. Milvus (2025), What are the limitations of current quantum computing hardware?
75. Forbes (2025), Quantum Computing Faces 3 Major Barriers Before Going Mainstream

4 Conclusion

Seizing the Quantum Opportunity

Quantum technologies stand at a strategic inflection point, poised to reshape financial services over the next decade. The journey from 2016's early uncertainty feasibility to today's pioneering applications, such as HSBC's quantum-enabled algorithmic trading, demonstrates that the technology delivers potential value now while promising transformational capabilities for the future. For leaders in the financial sector, the path forward requires a dual strategy: building a robust defence against the inevitable quantum threat while simultaneously exploring the technology's vast commercial opportunities.

The primary imperative is defensive. The cryptographic foundations of the global financial system are vulnerable, and the transition to post-quantum cryptography is a matter of priority. Financial institutions must act decisively to manage this systemic risk by developing migration roadmaps, investing in cryptographic agility, and participating in industry-wide initiatives to ensure a smooth and secure transition. BIS has stated that preparedness for Q-day is an urgent priority for maintaining financial stability.

Concurrently, institutions must adopt an offensive strategy to harness quantum computing's potential for competitive advantage. The ability to solve complex optimisation and simulation problems far beyond the reach of classical computers will unlock new frontiers in portfolio management, risk analytics, and AI application in finance. Early adoption, through hybrid systems and quantum-inspired approaches, allows firms to build internal expertise and identify high-impact use cases.

The future of quantum finance will be defined by collaboration. Public-private partnerships and cross-industry alliances are critical for establishing standards, fostering innovation, and navigating this new technological era. While significant challenges in scalability and reliability persist, the momentum is undeniable. The financial institutions that embrace this dual mission will not only safeguard their operations but also lead the next decade of innovation in a quantum-enabled world.

Authors

GFTN Research & Advisory

Aanault Lee
Lead Author

For further information, please contact
aanault.lee@gftn.com

Contributors

Kaitlyn Thinn
Head of Strategy & Research

Production

Sachin Kharchane
Graphic Designer

Global Finance &
Technology Network (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com