In collaboration with Accenture

WORLD ECONOMIC FORUM

Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders

WHITE PAPER

JULY 2025

Images: Getty Images

Contents

Foreword

Adam Burden
Global Innovation Lead and Chief Software Engineer, Accenture

Jeremy Jurgens
Managing Director, World Economic Forum

David Parker
Global Financial Services Industry Practices Chair, Accenture

Drew Propson
Head, Technology and Innovation in Financial Services, World Economic Forum

As quantum technologies rapidly advance, they are attracting increasing attention across industries given their potential to solve highly complex problems and their deep interconnection with cybersecurity. The financial services industry, known for its early adoption of emerging technologies, is particularly well-positioned to be a leader in quantum integration. While the evolution of quantum is still in its nascent stages, it is essential that stakeholders throughout financial services share insights and lessons learned from experimentation. Such collaboration will be necessary to accelerate innovation and safeguard the integrity of the global financial system, benefitting all participants.

Case studies play a critical role in grounding this dialogue, offering real-world perspectives that can inform the strategy decisions of financial services executives. The identification of core pillars, or shared areas of focus, is equally important and can guide institutions in collectively building a resilient, future-ready quantum ecosystem.

In response to this need, the World Economic Forum and Accenture have been collaborating to assess the current state of quantum applications in financial services and explore representative case studies across key domains. Over the past seven months, we have conducted over 30 interviews and hosted four community meetings with quantum and financial-sector leaders to gather perspectives on where quantum technologies are being tested and where they are most likely to be deployed over the long term. This publication distils those insights and outlines strategic priorities that financial institutions should consider in the years ahead. The Quantum Economy Network's Quantum Applications Hub and Industry Track present additional use cases and insights on quantum technology applications.

We are deeply grateful to all who contributed to this paper. We hope it proves valuable for decision-makers in both the public and private sectors and that it helps cultivate continued exchange and collaboration in the fast-evolving field of quantum technologies in financial services.

Executive summary

As quantum technologies advance, emerging applications in financial services are offering valuable insights to public- and private-sector leaders.

This white paper examines emerging applications of quantum technologies in financial services and highlights prominent case studies. Building on previous World Economic Forum reports focused on the quantum economy,[1] quantum security[2] and technology and innovation in financial services,[3] this publication aims to support public- and private-sector leaders with insights that can help them navigate and prepare for quantum's rapid evolution.

FIGURE 1 **Key insights on quantum technologies for financial services**

Quantum computing

- Quantum computing offers the ability to solve highly complex optimization, simulation and data analysis challenges.
- Use cases include risk modelling, fraud detection and portfolio optimization, among many.
- Case studies from Yapı Kredi, Intesa Sanpaolo and Santander (among others) show early success in quantum and quantum-inspired applications.

Quantum sensing

- Quantum sensing excels in highly precise measurements of physical quantities such as time, magnetic fields or acceleration.
- Use cases are limited, though include infrastructure monitoring and precise timing for high-frequency trading.
- This may have long-term potential in environmental, social and governance (ESG) reporting and sustainability-focused investing.

Quantum security and quantum communications

- Quantum security can leverage post-quantum cryptography (PQC), quantum key distribution (QKD) and quantum random number generators (QRNG) to protect sensitive data.
- HSBC and Banco Sabadell (among others) are piloting quantum-secure infrastructure to mitigate future cyber threats.
- A defence-in-depth strategy – integrating quantum-resistant and quantum native technologies – is essential for long-term resilience.

Strategic imperatives for financial services

For quantum to reach its full potential, engagement from policy-makers, industry leaders and academics is needed in six core pillars:

- Research and development
- Public-private collaborations
- Education and workforce development
- Infrastructure enablement
- Entrepreneurship support
- Responsible quantum deployment

While quantum technologies are still evolving, they are beginning to show potential as strategic differentiators. Financial services decision-makers that take thoughtful, measured steps today may be well-positioned to lead future innovation, strengthen security and build resilience in an increasingly complex digital landscape.

Introduction

Quantum technologies are poised to transform the financial services industry by offering innovation and security.

The financial services industry is at a technological inflection point, driven by the advent of quantum technologies. These emerging technologies hold the potential to transform the financial sector by offering new computational paradigms, enhanced security and innovative solutions to complex problems. This white paper explores the strategic imperatives, opportunities and risks that quantum technologies present for financial services leaders, providing a roadmap for action and readiness.

Quantum technologies differ from classical ones, harnessing quantum mechanics principles like superposition, entanglement and interference to facilitate powerful new capabilities in computing, communication and sensing. These principles allow quantum systems to process information in parallel, link particles across distances and amplify correct outcomes while eliminating errors. While they promise breakthroughs in fields like cryptography, simulation and data analysis, practical implementation remains a significant scientific and engineering challenge.

Quantum applications within financial services are diverse. Quantum computing, for instance, has the potential to offer more accurate risk modelling, fraud detection and portfolio optimization.[4] Quantum security and communications technologies enable theoretically unbreakable encryption through methods such as quantum key distribution (QKD) and quantum random number generation (QRNG). Complementing this, classical approaches like post-quantum cryptography (PQC) algorithms can build resistance to quantum computer attacks, helping to protect sensitive financial data from emerging threats.[5] Meanwhile, quantum sensing provides precise measurement capabilities that may be used to heighten the synchronization of high-frequency trading (HFT) algorithms.[6]

To derive meaningful value from quantum technologies, financial institutions will need to go beyond experimentation and pilot phases. Strategic focus is required across several key pillars – sustained research and development (R&D) investment, infrastructure enablement, public-private collaboration, engagement with start-ups and private ventures, targeted education and workforce development, and responsible quantum deployment. Together, these pillars lay the foundation for scaling quantum innovations – translating nascent, isolated use cases into industry-wide transformation.

In this dynamic and evolving landscape, financial services leaders must remain agile and forward-thinking. The integration of quantum technologies requires a phased and strategic approach, continuous learning and collaboration with multiple stakeholders. By embracing quantum advancements, financial services leaders can improve operational efficiency, deliver greater value to customers and strengthen resilience against emerging challenges, paving the way for long-term growth and stability within the industry.

1 Benefits across financial services

By demonstrating clear, incremental business benefits, quantum technologies have the potential to contribute to the evolution of the financial sector.

“ Understanding the full spectrum of quantum’s impact requires a nuanced examination of the various domains within financial services.

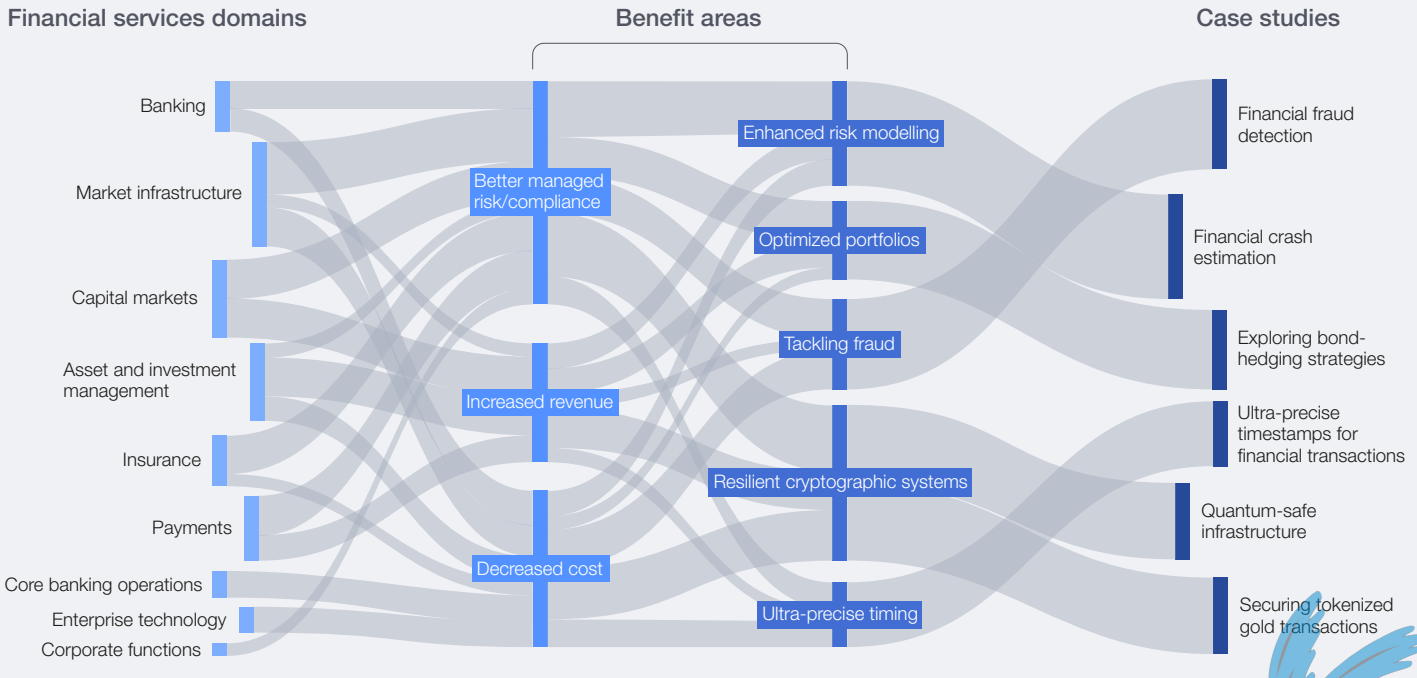
Quantum technologies are emerging as a powerful force with the potential to reshape the financial services industry. Understanding the full spectrum of quantum’s impact requires a nuanced examination of the various domains within financial services. As outlined in Figure 2, quantum technologies intersect with a wide array of domains, delivering tangible business benefits including revenue generation opportunities, increased operational efficiency and improved risk management. These benefits materialize when harnessing certain quantum use cases.

By implementing quantum technologies, financial institutions may be able to offer innovative, high-value services such as optimized portfolios, personalized products and ultra-secure transactions, attracting more customers and increasing revenue. Operational efficiency can also be achieved, for example, through the use of quantum algorithms that support faster and more accurate fraud detection and improvements in resource-intensive processes. Additionally, quantum technologies hold the potential to enhance risk management by providing more accurate models and simulations. Furthermore, they can reduce risk through improved cryptography methods.

Independent of quantum technology use in cryptography, PQC algorithms, also known as quantum-resistant cryptographic algorithms, can strengthen security and ensure compliance with regulatory requirements, reducing penalties and reputational risks.

Early adoption of PQC aligns with international regulatory directives – such as those outlined by the US National Institute of Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA) and the UK National Cyber Security Centre (NCSC) – supporting long-term compliance efforts.[7]

FIGURE 2 **Mapping of financial services domains to benefits and case studies**



The interconnected value of quantum technologies across the various financial services domains illustrated in Figure 2 demonstrates their contribution to distinct benefit areas and their translation into practical case studies, which are explained in detail in subsequent chapters.

Ultimately, quantum innovation extends beyond theoretical promise, offering a direct and multifaceted impact on the financial services ecosystem and driving greater security through quantum-resistant cryptography initiatives. Such initiatives include, among others, Mastercard's exploration of post-quantum encryption (which boosts operational efficiency via quantum-enhanced optimization of settlement processes and fraud detection), JP Morgan Chase's collaboration with QC Ware for credit risk simulations (which strengthens long-term resilience through robust risk modelling and scenario analysis enabled by quantum algorithms) and HSBC's trials in secure quantum communications.[8]

While the maturity of these quantum technologies varies, their strategic potential is notable. Early adoption may offer advantages, allowing financial institutions to gain access to scarce talent, develop critical infrastructure and establish partnerships ahead of broader industry uptake. By initiating this transformation early, industry pioneers can mitigate future risks and position themselves as leaders in an increasingly quantum-enabled landscape.[9] First movers must also remain mindful of the inherent risks associated with early adoption and should proceed with appropriate caution.

2 Quantum computing

Quantum computing stands to enhance capabilities and reshape the operations of financial institutions.

Quantum computing offers the ability to solve highly complex optimization, simulation and risk analysis problems at unprecedented speed and scale. As the technology matures, financial services firms must be proactive in integrating quantum solutions to ensure robust and strategic operational practices. Recent estimations suggest that quantum computing use cases in the financial services industry could generate up to $622 billion in value by 2035.[10] Some of the most promising use cases can be found in portfolio optimization, trading strategies, options pricing, risk management and fraud detection.

For example, quantum computing offers important advanced techniques for portfolio optimization. By efficiently analysing various investment scenarios and constraints, quantum algorithms have the potential to optimize asset allocations, thereby minimizing risk while maximizing returns. This capability is particularly beneficial in volatile markets where traditional methods may fall short.

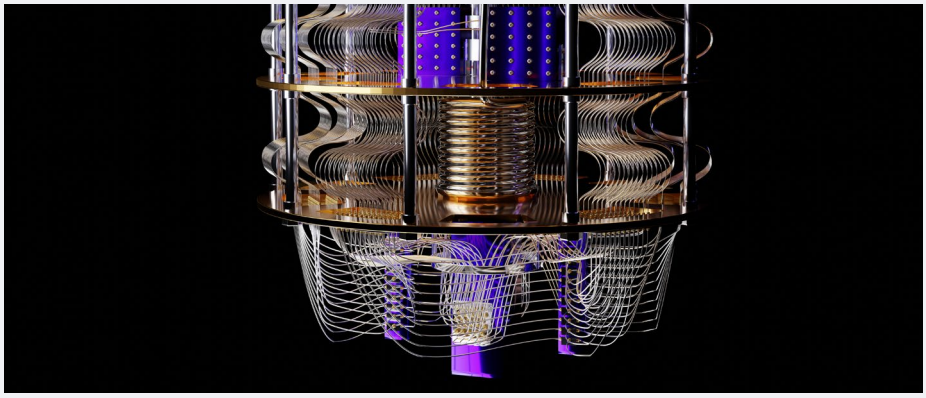
Quantum-enhanced Monte Carlo simulations also have the potential to improve the efficiency of options pricing predictions. The quadratic speedup provided by quantum algorithms will enable financial institutions to conduct these simulations more swiftly and accurately, resulting in faster and more precise pricing of complex financial derivatives.[11]

Similarly, in algorithmic trading, quantum computing has the potential to support the development of more advanced algorithms that react to market changes in real time. Quantum algorithms can evaluate numerous potential outcomes simultaneously, optimizing trading strategies based on complex market dynamics and improving overall trading performance.[12]

Moreover, quantum algorithms enable financial institutions to analyse complex models with greater efficiency, enhancing predictive analytics to improve anticipation of market trends and potential risks. As Arvinder Bharath, Digital Expert Lead at the International Monetary Fund (IMF), notes, “Simulating cascading effects on the financial system utilizing quantum computing would be invaluable in predicting systemic risks and preventing financial crises.” This capability supports informed decision-making, proactive risk management and improved financial stability.[13]

> As the technology matures, financial services firms must be proactive in integrating quantum solutions to ensure robust and strategic operational practices.

FIGURE 3



Quantum computing

With its unmatched computational power, quantum computing is poised to transform industries and enable groundbreaking applications. Strategic adoption can benefit financial services organizations in multiple ways.

Why it's important

Benefit gained
Quantum computing delivers superior performance for complex computations, enabling breakthroughs in optimization and data analysis.

Catalyst for transformation
Quantum computing acts as a transformative force, enabling financial services firms to reimagine traditional processes. By harnessing quantum algorithms, organizations can explore new frontiers in solving business challenges and anticipating risks.

How to approach integration

Strategic exploration
Identify key areas where quantum computing can add strategic value and create a comprehensive plan for responsible integration into business operations.

Active and multifaceted engagement
Initiate pilot projects, cultivate partnerships, invest in training, prioritize quantum use cases and stay informed on advancements to drive innovation and adoption.

Early case studies (non-exhaustive)

CASE STUDY 1

Financial crash estimation within a network of small and medium-sized enterprises

Understanding and predicting financial crashes is vital for maintaining global economic stability. A key problem in financial mathematics is identifying vulnerabilities in financial institution networks to prevent crises that could impact businesses and markets.[14] Turkish bank Yapı Kredi has taken a significant step towards addressing this issue by developing an innovative approach to estimating financial risks.

As part of an R&D initiative, Yapı Kredi created a model to identify potential failure points in its network of small- and medium-sized enterprises (SMEs). Identifying potential failure points is crucial to avoiding potential domino effects (wherein a single delayed payment may initiate a chain reaction of financial distress among interconnected enterprises, ultimately resulting in a cascading failure across the entire financial network). Analysing these intricate networks using classical computing, however, is difficult and time-consuming. To overcome this, the R&D team used quantum computing technology from D-Wave, which allowed them to efficiently explore thousands of possible scenarios and pinpoint businesses at risk of financial distress. This provided valuable insights for credit loan departments, helping the bank identify hidden risks not yet reflected in customers' financials and make better decisions.[15]

"Risk management is one of the most critical components of banking. We applied our model to a real-life scenario covering 4,297 out of a network of over 600,000 corporate clients. An analysis that would traditionally take years to compute was completed in just seven seconds thanks to the technology we developed. Our goal is to carry our clients into the future with a more robust financial infrastructure and to establish a model that will shape the industry." – Gökhan Özdinç, Executive Vice President, Technology, Data and Process Management, Yapı Kredi.

Importantly, all data was anonymized to comply with regulations. Looking ahead, Yapı Kredi plans to scale this approach to its entire SME network and expand its use to other areas of the organization. This experiment demonstrates how cutting-edge technology can help financial institutions protect businesses, mitigate risks and ensure long-term stability.

CASE STUDY 2

Advantages of financial fraud detection using quantum machine learning

Fraud detection poses a significant challenge for financial institutions, compelling banks to undertake a variety of activities, including real-time transaction monitoring, advanced algorithms and biometric verification. Traditional machine learning algorithms, however, often struggle to accurately identify fraud patterns, limiting their effectiveness. To address this, Italian bank Intesa Sanpaolo explored the use of quantum computing to improve fraud detection.

The bank conducted a study using quantum machine learning, specifically variational quantum circuit (VQC)-based classifiers. By analysing a dataset of 500,000 transactions, the R&D team reduced the data complexity to match current quantum hardware capabilities. Using IBM's quantum tools, the quantum model outperformed traditional methods in identifying fraud and achieving better accuracy and efficiency with fewer data features. This approach also introduced transfer learning, enabling models trained on one dataset to be applied to others, cultivating collaboration and innovation across the financial sector. Due to quantum hardware limitations, the study run by Intesa Sanpaolo used a phased approach starting with quantum-inspired (classical hardware) solutions, followed by the integration of quantum tools with existing systems and concluding with full adoption of quantum-based workflows when available. Compliance was ensured through anonymized datasets and privacy-by-design principles, aligning with regulatory standards and organizational security practices.

This initiative highlights the potential of quantum computing to revolutionize fraud detection. By improving accuracy and enabling collaboration through open-source platforms, banks can strengthen anti-fraud measures and enhance global financial security. As quantum technology advances, its scalability will unlock even greater benefits for the industry.[16]

Early case studies (non-exhaustive) (continued)

CASE STUDY 3

Exploring bond-hedging strategies with quantum-inspired solutions

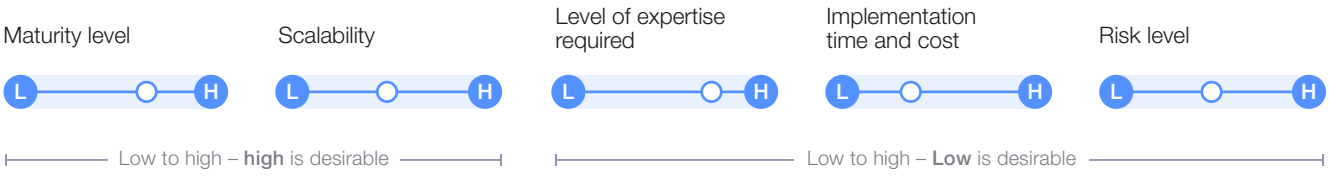
Santander explored the application of quantum-inspired (classical hardware) algorithms to optimize bond-hedging strategies. Managing large books requires substantial computational resources, which are expected to increase in volume in the medium term. Conventional methods, however, struggle to incorporate additional risk factors for real-time hedging, limiting their effectiveness in rapidly changing market environments. This often results in high execution costs and variance, necessitating more efficient solutions. To address this challenge, Santander Bank explored the application of quantum-inspired algorithms to optimize bond-hedging strategies.

The hedge problem was executed on a quantum-inspired optimization platform, harnessing its ability to handle millions of decision variables efficiently. The results of the experiment indicated the solution's faster execution time and ability to scale to a greater number of variables, reducing runtime significantly and enabling the optimization of larger bond portfolios.

Santander Bank's proof of concept (PoC) highlighted the competitive performance of quantum-inspired solutions. Further research, however, is needed to assess the cost-effectiveness of scaling these technologies for production environments. Testing other quantum-inspired solutions could provide additional insights into scalability and efficiency.

This initiative demonstrates the feasibility of using quantum-inspired algorithms for bond hedging, achieving faster execution, improved scalability and enhanced risk management – showcasing its potential for integration into broader financial applications.

Indicators



See the Appendices (A2) for other notable case studies.

Multi-phase integration action plan

Phase 1
Foundation and exploration

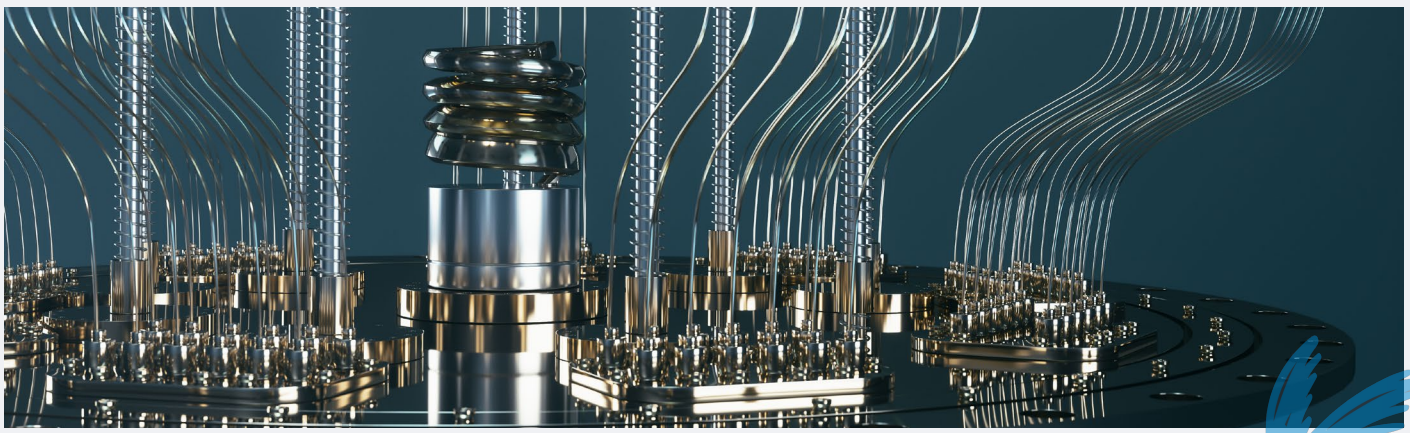
- Assess available technologies.
- Identify and prioritize use cases.
- Engage with experts.
- Conduct initial training.
- Initiate PoC.
- Establish pilot project criteria.
- Evaluate risks and challenges.

Phase 2
Pilot and scaling

- Initiate pilot projects that expand on PoC.
- Develop integration strategies.
- Implement training programmes.
- Forge strategic partnership(s).
- Monitor performance metrics.
- Allocate resources effectively.

Phase 3
Optimization and leadership

- Continuously refine solutions.
- Cultivate strategic innovation.
- Engage stakeholders regularly.



3 Quantum sensing

The role of quantum sensing in the financial sector remains niche compared to other quantum technologies.

“ An emerging opportunity lies in sustainability-focused investments, wherein quantum sensors can provide highly accurate environmental data.

Quantum sensing applications in financial services are limited compared to quantum computing, quantum security and quantum communications. While the technology excels in precision measurements, its role in the financial sector is primarily centred on quantum clocks that can enhance algorithmic trading by improving the accuracy and synchronization of HFT algorithms. This leads to better market predictions and improved execution timing.[17]

Additionally, quantum sensors will offer opportunities for enhanced infrastructure monitoring, e.g. through the detection of structural vulnerabilities in data centres and transaction systems. The niche applicability of quantum sensing, however, along with its lower scalability compared to quantum computing and security solutions, makes it a longer-term investment rather than an immediate priority for financial services firms.

Another emerging opportunity lies in sustainability-focused investments, wherein quantum sensors can provide highly accurate environmental data to enhance environmental, social and governance (ESG) reporting and climate risk assessments. Investment firms can harness quantum sensing to improve sustainability transparency, attract environmentally conscious investors and influence stock valuations through ESG-aligned financial strategies. Furthermore, financial institutions can play a role in advancing quantum sensing technology by funding ventures in this area. Nevertheless, high setup and operation costs, combined with unclear performance advantages of quantum sensors over existing sensors, are currently hindering the technology from reaching its full potential.[18]

Unlike quantum computing, which offers well-defined applications in risk modelling and financial optimization, or quantum communication, which enhances cybersecurity, quantum sensing lacks a clear and immediate use case in financial service operations. Furthermore, integrating quantum sensors into existing information technology (IT) infrastructure requires significant technical modifications, as most financial systems are not equipped to handle quantum-enhanced data streams, leading to potential operational inefficiencies.[19]

While quantum sensing holds potential for financial market precision, infrastructure security and sustainability-focused investing in the long term, its current scalability limitations, high implementation costs and lack of immediate return on investment (ROI) make it a future consideration rather than a current strategic consideration. Financial services firms should continue monitoring quantum sensing developments while prioritizing more mature and impactful quantum technologies.

FIGURE 4

Quantum sensing

Quantum sensing harnesses advanced quantum technologies to achieve unparalleled precision in measurement and detection, offering advantages in various fields. Applications for the financial sector are currently limited.

Why it's important

Precision and sensitivity
Quantum sensing provides unmatched precision and sensitivity in measurements, enabling advancements in areas such as HFT, environmental monitoring and infrastructure monitoring.

Ongoing advancements
By staying informed about quantum sensing advancements, financial services firms can ensure they are strategically prepared to integrate these technologies when they become more scalable and cost-effective.

How to approach integration

Strategic exploration
Identify areas where quantum sensing may deliver value and draft a preliminary plan for responsible integration (to be refined as the measurable benefits become clearer).

Ensuring preparedness
Stay informed on advancements to drive innovation and adoption, and prepare to scale successful pilot projects once initiated.

Early case studies (non-exhaustive)

CASE STUDY 4

Ultra-precise timestamps for financial transactions

Accurate timing is essential for financial transactions, especially in HFT, where thousands of trades occur in fractions of a second. Quantum optical atomic clocks, a groundbreaking innovation in quantum sensing, offer precision that's a hundred times greater than conventional atomic clocks. This level of accuracy can help financial institutions better track and understand the sequence of trades, improving transparency and compliance with regulations. While existing atomic clocks already meet the EU's Markets in Financial Instruments Directive II (MiFID II) requirement of timestamps accurate to 100 microseconds, quantum optical atomic clocks could go beyond these standards, addressing future needs driven by higher trade volumes and tighter precision demands. Their unmatched accuracy might help pinpoint the exact sequence of transactions and their impact on market events.

By providing ultra-precise timestamps, quantum optical atomic clocks can help financial institutions better understand the cascading effects of trades in real time. This enhanced precision is critical for analysing the impact of HFT on interconnected, artificial intelligence (AI)-driven financial markets and supporting compliance with future regulatory standards that may require even tighter timing accuracy as trading speeds and volumes continue to rise.

As these advanced clocks transition from research labs to commercial use, they are likely to influence certain aspects of the financial industry. Beyond finance, these clocks are becoming vital in telecommunications. With the rapid growth of data driven by technologies like 5G, 6G and AI, precise timing is critical for synchronizing networks and minimizing errors. Quantum optical atomic clocks offer unmatched stability, ensuring seamless data transmission and reducing congestion across financial services and other industries.[20]

A major milestone in this field is the delivery of Tiqker, a commercial quantum optical atomic clock, to the University of Strathclyde in the UK. Tiqker is part of an effort to develop a distributed quantum timing infrastructure, enhancing resilience in critical systems and advancing timekeeping technologies.[21] This innovation underscores the critical role of precise timing in driving technological advancements, cultivating economic growth and supporting a sustainable, interconnected global economy.

Indicators

Maturity level	Scalability	Level of expertise required	Implementation time and cost	Risk level
L – H	L – H	L – H	L – H	L – H
Low to high – **high** is desirable		Low to high – **Low** is desirable		

See the Appendices (A2) for other notable case studies.

Multi-phase integration action plan

Phase 1
Foundation and exploration

- Identify and prioritize business areas.
- Assess available technologies for each business area.
- Establish collaborations with vendors and research institutions.
- Develop detailed plans for initial pilots.

Phase 2
Expansion

- Launch pilot projects to test feasibility.
- Analyse the pilot and refine the quantum sensing strategy.
- Begin developing useful applications.
- Develop a comprehensive plan for integration.
- Deploy solutions into existing infrastructure.
- Test and monitor performance.
- Refine and optimize sensing systems.
- Share insights and innovations within the industry.

Phase 3
Optimization and leadership

- Roll out solutions.
- Engage stakeholders and gather feedback.
- Share insights and innovations within the industry.
- Plan for future advancements and expansions.
- Conduct a strategic review to assess overall impact (across all phases).

4 Quantum security and quantum communications

Adopting an agile security strategy that integrates both quantum-resistant and quantum-native technologies is essential to mitigating the quantum threat.

4.1 Quantum-safe cryptography

As cryptographically relevant quantum computers (CRQCs) become feasible, today's widely used encryption methods – such as RSA (Rivest-Shamir-Adleman) and ECC (elliptic curve cryptography) – will be increasingly vulnerable.

Quantum-safe cryptography refers to cryptographic systems and strategies designed to protect digital systems from quantum-enabled threats. Unlike quantum-native technologies, these solutions do not rely on quantum mechanics themselves but are engineered to withstand attacks from quantum adversaries.[22]

Key terms and concepts:

- **PQC** refers to a subset of quantum-resistant cryptography that's based on hard mathematical problems and believed to be secure against both classical and quantum attacks. PQC is currently the most scalable and implementation-ready approach to quantum-resistant security. It includes algorithms based on lattice problems, hash functions and multivariate equations (many of which are being standardized by NIST).
- **Crypto agility** refers to the ability of systems to rapidly switch between cryptographic algorithms as threats evolve or standards change. This is essential for future-proofing systems. It allows organizations to adopt PQC today while remaining flexible enough to integrate new standards or respond to unforeseen vulnerabilities.[23]

> **Efforts to identify the full potential of quantum technologies are critical to developing an effective post-quantum cryptography strategy. Organizations must begin the journey towards crypto agility – their ability to quickly adapt to changing cryptographic solutions – which will help ensure the security of the global financial sector and maintain the trust of all its stakeholders.**
>
> Mike Silverman, Chief Strategy and Innovation Officer, Financial Services Information Sharing and Analysis Center (FS-ISAC)

4.2 Quantum communications

> Organizations that embrace both quantum-resistant and quantum-native approaches will be best positioned to lead in a post-quantum world.

"Quantum communications" refers to the use of quantum mechanical properties – such as superposition and entanglement – to transmit information securely with novel capabilities. They enable ultra-secure networks and are expected to be as vital to quantum computing as traditional networking is to modern computer systems. QKD, a key early application, enables two parties to share encryption keys with provable security against eavesdropping. As the name suggests, QKD is specifically designed for secure key exchange and represents the first practical implementation of quantum communications.[24] QRNGs, which use quantum processes to generate truly unpredictable random numbers, often serve as a foundational component of QKD systems.

QKD, however, is just the beginning. Future quantum communications will extend far beyond key exchange. Technologies based on entangled photon transmission and quantum repeaters could enable broader functionalities, such as distributed quantum computing, secure multi-party computation and quantum-enhanced networking.[25] While the term "quantum internet" is often used to describe this vision, it's worth noting that some in the academic community prefer more precise terminology due to this term's broad and sometimes ambiguous connotations.

Technologies like QKD and QRNG are referred to as quantum-native security technologies because they rely directly on quantum mechanical principles to achieve security guarantees that are fundamentally different from those of classical cryptography.

4.3 Defence-in-depth and strategic roadmap

A defence-in-depth strategy integrates PQC and quantum-native technologies like QKD and QRNG, enabling financial institutions to build layered, adaptable security frameworks that evolve with the quantum threat landscape. Each of these technologies addresses specific use cases and challenges, and there is no single "silver bullet" solution to achieving quantum security. Instead, a combination of these technologies can provide a more robust and comprehensive approach. This multi-layered approach aligns with a broader quantum transformation journey, moving past foundational awareness towards pilot deployment and (ultimately) strategic leadership.

4.4 Resilience and leadership

Organizations that embrace both quantum-resistant and quantum-native approaches will be best positioned to lead in a post-quantum world. This dual strategy not only mitigates risk but also signals technological leadership and regulatory foresight.[26]

As organizations prepare for a future shaped by quantum computing, it's critical to recognize that current PQC solutions may not be sufficient in the long term. If quantum computers evolve beyond today's expectations, the foundational assumptions behind PQC could be undermined. This concern is echoed by quantum computing expert Scott Aaronson, who notes, "If we want evidence that quantum computing could survive a collapse of P (problems solvable in polynomial time) and NP (nondeterministic polynomial time), we must also seek evidence that bounded-error quantum polynomial time (BQP) is a subset of PH (polynomial time hierarchy)."[27] In other words, our understanding of quantum computational boundaries remains incomplete. To mitigate this uncertainty, forward-looking security strategies should consider quantum-native technologies such as QKD and QRNG, whose security is rooted in the laws of physics rather than assumptions about computational difficulty.

FIGURE 5

Quantum security and quantum communications

Quantum security and quantum communications are foundational to ensuring the long-term protection of sensitive financial data, systems and infrastructure in the quantum era. Financial services leaders will need to integrate both quantum-resistant and quantum-native technologies to mitigate the quantum threat.

Why it's important

Strategic imperative and essential resilience

The eventual arrival of CRQCs will render classical encryption vulnerable – potentially including PQC if quantum computing proves powerful enough to compromise hard problems.[28] This means that quantum-native technologies, like QKD and QRNG, may ultimately be the only provably secure alternatives. Financial institutions must act now to build layered, adaptable security frameworks that can evolve with the quantum threat. This is essential for firm viability as well as financial system resilience.

Practical roadmap

PQC is ready for immediate adoption and offers the broadest path to near-term security upgrades. At the same time, QRNG is already pilotable and enhances entropy quality in both classical and quantum-resistant systems. QKD, though still maturing, is foundational for future infrastructure like the quantum internet and select high-value links. Piloting and co-developing QKD/QRNG with telecommunication providers now will position firms to lead as these capabilities reach production scale.[29]

Early case studies (non-exhaustive)

CASE STUDY 5

Securing tokenized gold transactions using quantum technology

HSBC is addressing the future risks posed by quantum computing, which could compromise traditional encryption methods, by deploying quantum-secure technologies. As quantum computers advance, they threaten the security of sensitive financial data, especially in areas like distributed ledger technology (DLT) and asset tokenization. To tackle this, HSBC integrated advanced quantum technologies into its Orion digital assets platform, which supports its gold tokenization initiative.

The bank's solution combines PQC and QRNG from Quantinuum, which are mature products that are ready for deployment. QRNGs provide highly secure randomness for cryptographic keys, making them more unpredictable and resistant to attacks. Additionally, PQC virtual private network (VPN) tunnels protect communication between nodes in the distributed ledger. This ensures that transaction data remains secure against potential quantum threats. Tested on Azure networks, the solution maintains efficiency with minimal impact on performance while upgrading security.

This initiative has made HSBC's gold tokenization platform quantum-secure, safeguarding transaction data and ensuring interoperability between blockchains. The approach is cost-effective, enhancing security without requiring major changes to existing systems. HSBC's proactive adoption of quantum-secure technologies ensures compliance with cybersecurity standards and regulatory requirements while protecting sensitive financial data through privacy-by-design principles. By integrating quantum technologies, HSBC is not only mitigating risks but also improving efficiency and liquidity in tokenized asset markets.[30]

How to approach integration

Strategic and timely preparation

Develop a quantum security roadmap, beginning with a comprehensive assessment of current cryptographic systems and their exposure to quantum threats. Prioritize PQC adoption, as it is immediately actionable and scalable across most forms of infrastructure. Begin to test quantum-native technologies to prepare for potential future risks.

Agility and leadership

Adopt a crypto-agile defence-in-depth approach to be best equipped to adapt to regulatory shifts, mitigate operational risk and ensure stability in a post-quantum world. Stay informed on advancements to remain at the forefront of secure innovation and industry-wide resilience.

CASE STUDY 6

Quantum-safe infrastructure initiative

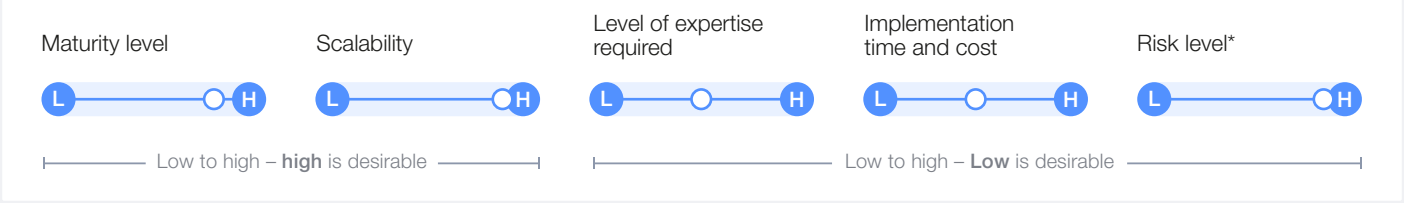
Banco Sabadell, in collaboration with Accenture and QuSecure, recently completed a four-month project exploring the adoption of PQC technologies. This initiative represents a significant step towards quantum resilience in the financial sector, addressing emerging risks associated with advances in quantum computing.

The project harnessed QuSecure's software and open-source libraries to modernize encryption protocols, focusing on cryptographic agility. Through this process, Banco Sabadell identified the key steps required to transition to quantum-safe technologies, with an emphasis on protecting sensitive information and critical banking operations (including payments and communications with market infrastructure).

According to Joan Puig, Group Chief Information Security Officer of Banco Sabadell, "This collaboration has allowed us to explore the impact of PQC adoption on the bank's infrastructure." Accenture's quantum security expertise and test labs provided a roadmap for implementing NIST PQC standards, while QuSecure demonstrated how encryption agility in the network layer can protect enterprises without disrupting existing systems.

This initiative underscores the urgency of proactively addressing quantum computing risks. As highlighted by the Financial Services Information Sharing and Analysis Center (FS-ISAC), developing crypto agility is a long-term strategy essential for safeguarding digital communications in the quantum era. Banco Sabadell's experience offers practical insights for financial institutions and stakeholders worldwide, demonstrating the feasibility and importance of adopting quantum-safe technologies in anticipation of future cryptographic vulnerabilities.[31]

Indicators



*Level is "high" primarily due to risk of inaction.

See the Appendices (A2) for other notable case studies.

Multi-phase integration action plan

Phase 1
Awareness and assessment

- Formulate a quantum security strategy aligned with enterprise risk posture.
- Inventory current cryptographic assets, assess quantum exposure and apply the latest PQC algorithms.
- Benchmark against industry frameworks – e.g. NIST, the World Economic Forum and the European Telecommunications Standards Institutes (ETSI).
- Draft strategic roadmap prioritizing PQC and entropy strengthening.

Phase 2
Implementation and integration

- Deploy PQC in production systems where feasible, e.g. VPNs, transport layer security (TLS) and application programming interfaces (APIs).
- Pilot QRNG for key generation in hardware security modules (HSMs) or secure enclaves.
- Collaborate with telecommunication providers to explore QKD use cases (e.g. secure inter-bank links).
- Conduct system-wide testing and crypto agility validation.
- Train teams on post-quantum and hybrid cryptography operations.

Phase 3
Optimization and quantum readiness leadership

- Expand PQC deployment across broader systems.
- Monitor the cryptographic ecosystem for new BQP-class breakthroughs and adjust strategy.
- Integrate QKD into high-sensitivity communication pathways where feasible.
- Engage in standards development and quantum internet pilot programmes.
- Continuously revise policy and technical controls to maintain readiness.

5

Strategic pillars for stakeholders

Advancing quantum in financial services requires multistakeholder engagement, strategic vision and targeted investments across the value chain.

To realize the full potential of quantum technologies in financial services, policy-makers, industry leaders and academics must prioritize six core pillars, as outlined in Figure 6. Each pillar is explored in depth in the following sections, drawing on best practices and successful initiatives from leading financial and technology institutions globally.

FIGURE 6 **Focus areas for multistakeholder engagement**

5.1 R&D

> Regulatory sandboxes offer a practical approach to the integration of quantum in financial services.

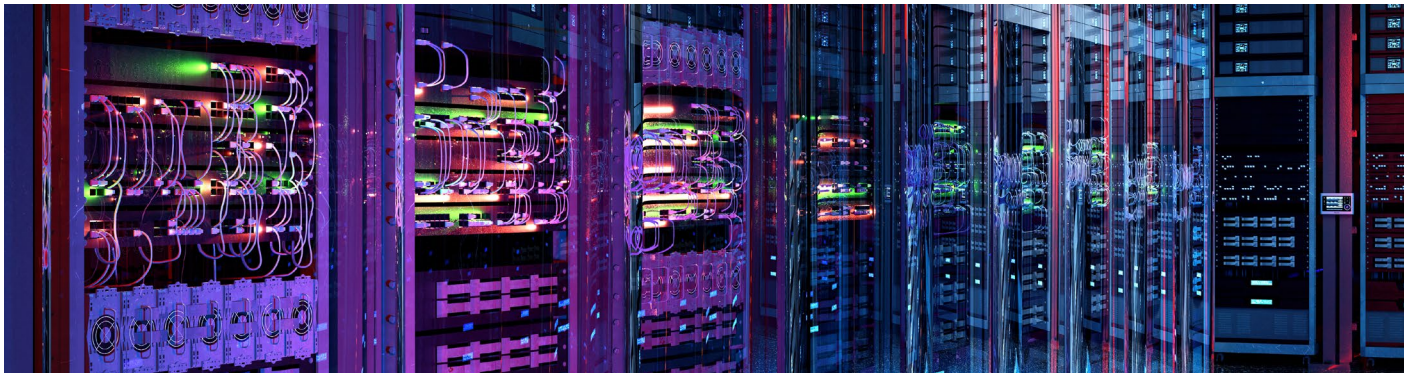
A robust R&D foundation is essential to accelerating the integration of quantum technologies in financial services. Policy-makers should support sustained investment in research while cultivating multidisciplinary collaboration to address the sector's technological and operational challenges.

Despite attracting growing interest, the integration of quantum technologies into financial services remains a complex undertaking, with many industry leaders awaiting clear regulatory guidance on associated risks, standards and governance frameworks. Regulators must stay updated on quantum advancements and create adaptive frameworks that balance innovation, security and customer protection.

Collaborative initiatives such as the World Economic Forum's Quantum Economy Network and the Financial Conduct Authority's (FCA) Emerging Technology Research Hub are helping to shape cross-industry standards and best practices for quantum governance and security. The white paper *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches* recommends a four-phase roadmap – prepare, clarify, guide, and transition and monitor – to transition to a quantum-secure financial sector. This roadmap promotes a collaborative, harmonized and globally informed approach to addressing the security challenges posed by the quantum transition. Regulators are also encouraging financial institutions and supervisory authorities to assess quantum-related risks and begin developing mitigation strategies.

Regulatory sandboxes offer a practical approach to the integration of quantum in financial services. By providing a controlled environment for experimentation, they enable firms to test quantum technologies with regulatory support, reducing compliance friction. These sandboxes also help regulators refine their frameworks in response to new developments while giving start-ups the opportunity to innovate and compete with established players.

Showcasing growing commitment, in April 2025, the UK government announced a £121 million investment in quantum technology to tackle crime, fraud and money laundering by supporting research hubs and funding pilot projects. Spotting the first signs of fraud and halting money laundering could save billions for the UK economy.[32]



5.2 Infrastructure enablement

Establishing resilient infrastructure is critical to supporting the growth of quantum technologies in financial services. Governments should cultivate an enabling environment that attracts investment in quantum data centres, secure communication networks and advanced national laboratories. To bolster quantum security infrastructure, both public- and private-sector leaders should support quantum research initiatives.

As quantum and other emerging technologies are integrated into essential services in the financial sector, they must meet the rigorous standards already applied to existing systems. Furthermore, embedding robust security measures into the design phase of quantum systems is crucial to addressing vulnerabilities (especially threats to current encryption methods). Over time, as risks become more well-understood, new standards may need to be introduced.

Harmonizing cybersecurity practices is vital to streamlining compliance, improving interoperability across sectors and ensuring the effective implementation of these technologies. Additionally, regulators must work towards building regulatory clarity and creating interoperable frameworks for quantum security, facilitating a cohesive transition to a quantum-safe system.

5.3 Public-private collaborations

Sustained collaboration between policy-makers, regulators, academia and industry (including start-ups) is essential for advancing quantum technologies. These collaborations provide access to expertise and innovation while facilitating risk-sharing and accelerating infrastructure development.

In a nascent ecosystem like quantum for financial services, regulators play a pivotal role in facilitating international cooperation. By working to harmonize cybersecurity standards and regulatory approaches across jurisdictions, they help ensure the secure and ethical integration of quantum technologies into the global financial system. Initiatives like the UK's Responsible Quantum Industry Forum (RQIF) exemplify how governments are working with industry leaders to promote ethical innovation, aligning technical progress with public interest protections.[33]

Several financial regulatory authorities have taken proactive measures to specifically address quantum security challenges. For instance, in February 2024, the Monetary Authority of Singapore (MAS) issued an advisory urging financial institutions to maintain an inventory of cryptographic assets and prioritize critical assets for migration to quantum-resistant encryption and key distribution.[34] In April 2024, the EU released a memorandum to its member states advocating for a coordinated transition to quantum-safe digital infrastructure.[35] In November 2024, the Group of Seven (G7) Cyber Expert Group (which advises G7 finance ministers and central bank governors on cybersecurity policy matters important to the security and resilience of the financial system) endorsed a unified approach to combatting financial sector risks from quantum computing.[36] Similarly, in January 2025, the Bank of Israel mandated financial entities to develop a preparedness plan for cyber risks associated with quantum computing capabilities.[37]

Many financial institutions are actively participating in various collaborative initiatives to tackle security challenges. The FS-ISAC PQC working group, for example, has published multiple reports and guidelines, and Europol's Quantum Safe Financial Forum released a position paper in February 2025.[38] Additionally, several organizations are encouraging public-public and private-private collaborations. In February 2025, for instance, the Bank for International Settlements (BIS) organized the "quantum-readiness for central banks and supervisors conference", which saw participation from over 40 central banks worldwide.[39]

"De-risking early-stage ventures via grants, public-private co-investment mechanisms or government-backed funding instruments can help catalyse innovation.

5.4 Entrepreneurship support

Cultivating entrepreneurial activity and attracting private capital are critical to developing the quantum economy. Policy-makers and regulators can support this by promoting start-up formation through targeted incentives, dedicated incubators and simplified regulatory pathways. Additionally, de-risking early-stage ventures via grants, public-private co-investment mechanisms or government-backed funding instruments can help catalyse innovation and unlock long-term value.

Initiatives at the local and federal levels demonstrate how targeted support can help build a robust ecosystem. As an example, in Singapore, MAS committed SGD 100 million (Singaporean dollars) under the Financial Sector Technology and Innovation Grant Scheme to support financial institutions in building capabilities in quantum. This funding was also directed towards the advancement of quantum- and AI-related innovation and adoption in financial services.[40]

In the United Arab Emirates, efforts are under way to raise awareness of the potential of quantum computing in financial services. The Abu Dhabi Investment Authority (ADIA) has publicly recognized the significance of quantum computing and is working to position the United Arab Emirates as a hub for quantum computing applications in finance, thereby creating fertile ground for start-ups and venture capital.[41]

The UK, a leading global financial centre, is emerging as a hotspot for quantum innovation in finance. Start-ups in this area are exploring funding opportunities from government initiatives and collaborations with research centres, especially through Innovate UK grants and the National Quantum Technologies Programme. More established organizations are also taking note. For instance, a collaboration between Toshiba Europe, HSBC and British Telecom (BT) aims to expand the capabilities of QKD networks.[42]

5.5 Education and workforce development

Developing and implementing quantum technologies in financial services will require a highly skilled workforce with expertise at the intersection of finance, quantum mechanics, engineering and software development. To prepare for this shift, the financial services industry must actively collaborate with academic institutions to build a pipeline of talent equipped to navigate this new frontier. As quantum technologies increasingly intersect with fields such as AI and cybersecurity, cross-disciplinary skills will become even more critical.

Several early initiatives are already working to close the quantum skills gap. For example, QuantFi and QURECA (Quantum Resources and Careers), in collaboration with Strangeworks, have launched a training programme in the field of quantum computing applications for the financial sector – covering areas such as quantitative asset management and trading, financial engineering, risk management and applied research.[43] Similarly, the Centre for Finance, Technology and Entrepreneurship (CFTE) has introduced specialized courses to help financial professionals understand the implications and opportunities of quantum technologies.[44]

Upskilling existing workers who have some of the needed skills is the fastest way to grow the pool of workers with relevant skills. HSBC, in collaboration with IBM, has invested in internal training programmes to equip its employees with the necessary knowledge and skills to understand and harness quantum computing.[45]

In Italy, national quantum strategies include expanding quantum-focused graduate programmes, launching industrial PhD programmes and retraining traditional IT professionals to transition into roles such as quantum software engineering and quantum algorithm design.[46]

> **Education in quantum technologies across diverse graduate curricula will significantly advance the future development of this sector, particularly within the financial industry, where it is expected to have the largest number of quantum computing use cases.**
>
> Davide Corbelletto, Distinguished Quantum Specialist, Intesa Sanpaolo

There is also an urgent need for curricula that address quantum security threats. As an example of progress in this area, executives at the HDFC Bank in India have benefited from the Certified Quantum Technology & Security Professional (DCQTSP) programme, supported by India's National Centre of Excellence for Cybersecurity Technology Development (NCoE). This programme is designed to equip industry leaders with the necessary skills and knowledge to navigate emerging quantum security challenges and prepare for the evolving cybersecurity landscape.[47]

In essence, to effectively harness the transformative potential of quantum technologies within the financial services industry, it is imperative to establish targeted training programmes on "quantum for finance". Tailored programmes – developed by industry forums and designed specifically for regulators, middle managers and senior leaders in both financial services and technology companies – can ensure that key decision-makers understand the risks and opportunities of quantum. These efforts will be instrumental in driving innovation, strengthening resilience and preparing the financial services industry for the quantum era.

5.6 Responsible quantum deployment

As quantum technologies advance, it is crucial to adopt a responsible and forward-looking approach to ensure their ethical and sustainable integration into the financial services industry. The Forum's quantum computing governance principles recommend that the safe, ethical and responsible use of quantum computing be included in regulatory frameworks, sector-based codes of practice and organization-level policies.[48]

Quantum ethics involves developing guidelines that prioritize privacy, security and human rights while ensuring transparency and accountability in quantum research and applications. Initiatives such as the Canadian Innovation Network's focus on responsible quantum computing, IBM Research's emphasis on ethical dimensions and Stanford Law School's Center for Responsible Quantum Technology demonstrate a commitment to cultivating ethical practices in quantum technology development.[49]

These initiatives underscore the importance of ethical innovation, sustainability, security, privacy, inclusive growth and collaborative governance as quantum capabilities mature. For financial services leaders, aligning with these values can help build trust, minimize unintended consequences and promote long-term viability. A secure and ethical foundation will be critical to ensuring that quantum technologies benefit a broad range of stakeholders and contribute positively to the global financial system.[50]

Conclusion

Quantum technologies have the potential to redefine the financial services industry and unlock significant opportunities for innovation, efficiency and growth. To harness this transformative potential, financial leaders must act decisively, aligning strategic roadmaps with actionable insights to capture the benefits of quantum advancements. By adopting an iterative approach, organizations can take initial steps, refine strategies based on outcomes and build a robust roadmap for long-term success.

FIGURE 7 **Strategic initiatives and benefits of quantum technologies**

	Strategic initiatives	Benefits
Quantum computing	Initiate PoCs. Launch pilots that expand on PoCs. Collaborate with academia and technology experts to advance quantum research.	Process datasets more efficiently improving decision-making. Enhance analytics for better trend and risk predictions. Optimize systems, reducing inefficiencies and boosting performance.
Quantum sensing	Identify business areas where quantum sensing improves accuracy. Foster partnerships with research institutions and technology vendors, and monitor developments.	Deliver precise data, reducing uncertainty in decisions. Improve measurement accuracy, enhancing stability. Support strategies with clear goals and expert insights.
Quantum communications and security	Inventory current cryptographic assets, assess quantum exposure and apply the latest PQC algorithms. Pilot QRNG for key generation in HSMs or secure enclaves. Collaborate with telecom providers to explore QKD use cases (e.g. secure inter-bank links).	Prevent the potential threat of a quantum computer-based attack. Ensure compliance with evolving regulations and reduce risks. Lead in adopting secure technologies, building trust and resilience.

Collaboration is the cornerstone of the quantum revolution. Building a thriving quantum ecosystem requires strong partnerships across academia, industry and government. Public-private collaborations, targeted R&D investments and adaptive regulatory frameworks will be essential in driving quantum adoption while addressing critical concerns such as cybersecurity, data privacy and ethical implications. Furthermore, global alignment on standards and regulations will ensure the secure and ethical deployment of quantum technologies, enabling financial institutions to navigate the complexities of the quantum era with confidence.

Appendices

A1 Explanation of indicators

These indicators also influence one another, with risk being particularly affected by the combined impact of all other factors.

TABLE 1 **Indicator explanations**

Indicator	Explanation of indicator levels	Quantum computing	Quantum sensing	Quantum communications and security
Maturity level How developed and ready the technology is for practical use **High** is desirable	**Low** – Experimental stage, mainly theoretical, no real-world use cases **Medium** – Some proven applications, but large-scale deployment is limited **High** – Well-developed, widely adopted and integrated into various industries	**Medium** Emerging applications in financial modelling and risk analysis; ongoing development	**Low** Limited direct financial services applications, primarily in research phases	Between **medium** and **high** Quantum-resistant algorithms and quantum-native cryptographic technologies being tested and deployed for cryptographic assurance and secure communications
Scalability The ability of the technology to expand and handle increasing workloads **High** is desirable	**Low** – Limited scalability due to hardware, cost or environmental requirements **Medium** – Some expansion possible, but significant improvements needed **High** – Easily scalable, deployable across industries with minimal barriers	**Medium** Current hardware limitations restricting scalability; potential growth with advancements	Between **low** and **medium** Niche applications limiting scalability within the financial services industry	Between **medium** and **high** High PQC and QRNG scalability potential across global financial networks, QKD scalability challenges to be overcome
Level of expertise required The effort and expertise required to adopt and use the technology **Low** is desirable	**Low** – Easy to learn and integrate, with user-friendly tools and widespread training available **Medium** – Specialized knowledge required (but practical applications are more intuitive) **High** – Very complex, requiring deep expertise in quantum physics and engineering	Between **medium** and **high** Requires specialized knowledge in quantum algorithms and computing	**Medium** Involves integration of quantum sensors; moderate complexity	**Medium** Necessitates understanding of quantum cryptography principles
Implementation time and cost The resources required to deploy the technology **Low** is desirable	**Low** – Cost-effective and quick to implement at scale **Medium** – Moderate cost and time commitment, with potential long-term ROI **High** – Expensive, long-term investment with slow deployment	Between **low** and **medium** Expensive and long-term investment required, with gradual improvements	Between **medium** and **high** Costs associated with integrating quantum sensors into existing systems	Between **medium** and **high** Significant investment in deploying quantum-secure communication networks
Risk level Potential challenges or negative outcomes from adoption or non-adoption **Low** is desirable	**Low** – Minimal risk, well-established technology with clear benefits **Medium** – Some uncertainties, but risks can be managed with strategic planning **High** – Significant risks, including high costs, security vulnerabilities or potential disruptions.	**Medium** (for both adoption and inaction) Technical uncertainties and regulatory challenges persist, although are expected to dissipate as advancements continue; over time, inaction could reduce competitiveness and revenue opportunities	Between **low** and **medium** (for both adoption and inaction) Lower risk due to limited financial services application; adoption risks centre on poor implementation	**High** (for inaction) Urgent need to address potential threats to data security from quantum advancements Risk level will be **low** for adoption; risks include poor implementation and lack of coordination with ecosystem partners

A2 Other notable case studies

Below are additional notable case studies that represent PoCs:

BOX 1 Quantum computing

- Enhancing quantum optimization methods with high-performance computing (HPC) and operational research techniques; synthetic data generation for back-testing financial models (e.g. asset allocation, electronic trading and pricing) by the Fidelity Center for Applied Technology (FCAT)[51]
- Novel mathematical modelling to diversify investments and maximize Sharpe ratio (risk-adjusted return), and an enhanced Quantum Credit Risk Analysis (CRA) framework by Intesa Sanpaolo[52]
- Fallen-angels forecasting in the financial risk management field by Crédit Agricole Corporate and Investment Bank, and Pasqal[53]

BOX 2 Quantum security and communications

- Quantum-safe services by Singtel and ID Quantique[54] for secure banking in the future
- Quantum security collaboration involving the Monetary Authority of Singapore (MAS), several banks – DBS, HSBC, Oversea-Chinese Banking Corporation (OCBC), United Overseas Bank (UOB) – and technology providers SPTel and SpeQtral, with a study on QKD for financial services applications[55]
- Cryptographic protection of blockchain infrastructure using QRNG and PQC algorithms by AME Chain and QNu Labs[56]

More case studies can be found in the financial services section of the *Embracing the Quantum Economy: A Pathway for Business Leaders* report.

Contributors

Lead authors

Syamasundar Gopasana
Technology Innovation Engineering Senior Manager, Accenture; Quantum Fellow, World Economic Forum

Shreyas Ramesh
Managing Director, Accenture; Quantum Fellow, World Economic Forum

Arunima Sarkar
Head, Frontier Technologies, World Economic Forum

Project team

Laura Converso
Thought Leadership Principal Director, Accenture; Quantum Fellow, World Economic Forum

Camille Georges
Specialist, Quantum Technology, World Economic Forum

Maximus Howard
Innovation Senior Manager, Accenture; Quantum Fellow, World Economic Forum

Drew Propson
Head, Technology and Innovation in Financial Services, World Economic Forum

Kelly Richdale
Senior Adviser, SandboxAQ; Executive Fellow, Quantum, World Economic Forum

Bo Sun
Consultant, Cyber Next, Accenture; Quantum Fellow, World Economic Forum

Acknowledgements

Olivia Adams
Lead, Research and Content, Center for Technology Integrity (CTT), Centre for the Fourth Industrial Revolution

Ahmad Alabdulkareem
Chief Technology Officer, Intelmatix

Basmah AlBuhairan
Managing Director, Centre for the Fourth Industrial Revolution, Saudi Arabia

Filipe Beato
Manager, Cyber Resilience, Centre for Cybersecurity, World Economic Forum

Andre Belelieu
Head, Financial Services Industries, World Economic Forum

Krisztian Benyo
Technical Pre-Sales Consultant, Europe, PASQAL

Arvinder Bharath
Digital Expert Lead, International Monetary Fund (IMF)

Ege Bilaloglu
Project Fellow, Technology for Climate Adaptation, World Economic Forum

Giuseppe Bruno
Director, Economics, Statistics and Research, Bank of Italy

Scott Buchholz
Quantum Computing Lead, Deloitte

Richu Channakeshava
Senior Product Manager, Enterprise & NetSec R&D, Palo Alto Networks

Davide Corbelletto
Distinguished Quantum Specialist and Team Leader, Intesa Sanpaolo

Berkay Coşkuner
Expert R&D Engineer, Yapı Kredi Teknoloji

Michael Dascal
Vice-President Quantum Technology, Fidelity Center for Applied Technology (FCAT)

Marcin Detyniecki
Head, Research; Group Chief Data Scientist, AXA

Stefan Deutscher
Partner and Director, Cybersecurity and IT Infrastructure, Boston Consulting Group

Ege Dinçer
Senior Research and Development Engineer, Yapı Kredi Teknoloji

Donna Dodson
Senior Strategist, evolutionQ

Gabrijela Dreo Rodosek
Professor; Founding Director, Research Institute CODE, Universität der Bundeswehr München

Carl Dukatz
Innovation Strategy Managing Director, Accenture

Roland Fejfar
Head, Technology Business Development International, Morgan Stanley

Sabrina Feng
Chief Risk Officer, Technology, Cyber and Resilience, London Stock Exchange Group

Petra Florizoone
Director, IBM Quantum, Global Partnerships & Business Development, IBM

Jacques Francoeur
Team Lead, Security & Assurance Working Group, Digital Currency Global Initiative, International Telecommunication Union (ITU)

Jaime Gómez García
Global Head, Quantum Threat Program, Santander

Ross Grassie
Technical Program Manager, University of Edinburgh

Roger A. Grimes
Data-Driven Defense Evangelist, KnowBe4

Petra S. Häfliger
Senior Risk Manager, Swiss Financial Market Authority (FINMA)

Marc Hulzebos
Innovation Officer, eurofiber

Bruno Huttner
Director, Strategic Quantum Initiatives, ID Quantique

Salih İmece
Applied Data Science Manager, Yapı Kredi Teknoloji

Philip Intallura
Global Head, Quantum Technologies, HSBC

Nauman Ishaq
Head of Data Innovation, Saudi Awwal Bank

David Keyes
Senior Associate to the President for Strategic Partnerships, King Abdullah University of Science and Technology (KAUST)

Bilge Köroğlu
Director, Applied Artificial Intelligence and R&D, Yapı Kredi Teknoloji, Koç Holding

Rebecca Krauthamer
Co-Founder and Chief Executive Officer, QuSecure

Charlie Markham
Senior Associate, Emerging Tech & Research, Data Technology & Innovation, Financial Conduct Authority

Patrick McMullen
Director, Deutsche Bank

Paul Mee
Partner, Information Technology and Operations Practice, Oliver Wyman

Kristin Milchanowski
Chief AI & Data Officer, Bank of Montreal

Michele Mosca
Chief Executive Officer, evolutionQ

Mehmet C. Onbasli
Associate Professor, Koc University

Tom Patterson
Managing Director, Cyber Next, Accenture

Antoine Pietri
Thought Leadership Expert, AXA

Marco Pistoia
Managing Director and Head of Research and Engineering, JPMorganChase

Ana Predojevic
Associate Professor, Stockholm University

Manuel Proissl
Global IBM Quantum Applications Lead for Financial Services and Senior Executive, IBM

Manoj Puri
Chief Security Officer, Absa Group

Heike Riel
Head, Science and Technology; Lead, IBM Research Quantum Europe and Africa, IBM

James Robertson
Vice-President, Strategy & Chief Technologist, Office of the CTO, Hewlett Packard Enterprise

Vikram Sharma
Founder and Chief Executive Officer, QuintessenceLabs

Jacob Sherson
Professor, University of Aarhus

Roshan Shetty
Head, Banking, Financial Services and Insurance (BFSI) and Public Sector, Tech Mahindra

Elvira Shishenina
Senior Director, Strategic Initiatives, Quantinuum

Bal Shukla
Chief Technology Officer and Head, AI, Financial Services, Infosys

Mike Silverman
Chief Strategy and Innovation Officer, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Catherine Simondi
Vice-President, Marketing and Communications, ID Quantique

Rafael Sotelo
Dean of Engineering, Universidad de Montevideo

Salvador E. Venegas-Andraca
Professor, Tecnológico de Monterrey

Jingbo Wang
Professor; Director, Quantum Information, Simulation and Algorithms Research Hub (QUISA), University of Western Australia

Mike Wilkes
Senior Security Advisor, New York University

George Woodman
Quantum Computing Lead, AXA

Haimera Workie
Vice-President and Head, Financial Innovation, Financial Industry Regulatory Authority (FINRA)

Elena Yndurain
Adj. Professor Deep Technology, IE University

Reena Dayal Yadav
Founder and Chief Executive Officer, Quantum Ecosystems and Technology Council of India

Verena Zimmermann
Chief of Staff, PlanQC

Production

Louis Chaplin
Editor, Studio Miko

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Endnotes

1. World Economic Forum Quantum Economy Network. (2025). *Impact & insights*. https://initiatives.weforum.org/quantum/impact-insights.
2. World Economic Forum Quantum Economy Network. (2025). *Quantum security*. https://initiatives.weforum.org/quantum/security.
3. World Economic Forum Technology, Innovation and Systemic Risk. (2025). *Our insights*. https://initiatives.weforum.org/technology-innovation-and-systemic-risk/static-insights.
4. How, M. & Cheah, S. (2023). Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. *Businesses*, vol. 3, no. 4, pp. 585-605. https://www.mdpi.com/2673-7116/3/4/36.
5. The Quantum Economic Development Consortium (QED-C). (2024). *Quantum Technology for Securing Financial Messaging*. https://quantumconsortium.org/publication/financial24/.
6. Citi Group. (2024). *Quantum Sensing: Tech's New Eyes and Ears*. https://www.citigroup.com/global/insights/quantum-sensing-tech-s-new-eyes-and-ears.
7. US Congress. (2022). *H.R.7535 - Quantum Computing Cybersecurity Preparedness Act*. https://www.congress.gov/bill/117th-congress/house-bill/7535; The White House. (2022). *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/; National Institute of Standards and Technology (NIST). (2024). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards; European Union Agency for Cybersecurity. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.
8. Mastercard. (2024). *Quantum cyber threats are likely years away. Why and how we're working today to stop them*. https://newsroom.mastercard.com/news/perspectives/2024/quantum-cyber-threats-are-likely-years-away-why-and-how-we-re-working-today-to-stop-them/; HSBC. (2023). *HSBC becomes first bank to join UK's pioneering commercial quantum secure metro network*. https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network; JPMorgan Chase. (2023). *JPMorgan Chase and QC Ware Evolve Hedging for a Quantum Future*. https://www.jpmorgan.com/technology/news/jpmorganchase-qcware-evolve-hedging-for-a-quantum-future
9. Euro HPC Summit. (2025). *European Quantum Readiness Center's presentation*. https://www.eurohpcsummit.eu/livestream.
10. McKinsey Digital. (2023). *Quantum technology use cases as fuel for value in finance*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/quantum-technology-use-cases-as-fuel-for-value-in-finance.
11. Naik, A. et al. (2025). From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance. *Springer Open Financial Innovation*, vol. 11, no. 88. https://jfin-swufe.springeropen.com/articles/10.1186/s40854-025-00751-6.
12. TRENDS Research and Advisory. (2025). *Quantum Revolution: Redefining Industry and the Global Chip Race*. https://trendsresearch.org/insight/quantum-revolution-redefining-industry-and-the-global-chip-race/; World Economic Forum. (2024). *Quantum-inspired High-Frequency Trading system*. https://initiatives.weforum.org/quantum/case-study-details/quantum-inspired-high-frequency-trading-system/aJYTG0000000H7J4AU.
13. Bharath, A. (2025). *Virtual interview*.
14. World Economic Forum. (2025). *Financial Crash Estimation in Enterprises*. https://initiatives.weforum.org/quantum/case-study-details/financial-crash-estimation-in-enterprises/aJYTG0000000S7Z4AU.
15. D-Wave. (2024). *D-Wave Customer Story: Yapı Kredi Teknoloji*. YouTube. https://www.youtube.com/watch?v=bcNAe-TKmu0.
16. A, Tudisco. et al. (2024). Evaluating the Computational Advantages of the Variational Quantum Circuit Model in Financial Fraud Detection. *IEEE Access*, vol. 12, pp. 102918-102940. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10606260.
17. Citi Group. (2024). *Quantum Sensing: Tech's New Eyes and Ears*. https://www.citigroup.com/global/insights/quantum-sensing-tech-s-new-eyes-and-ears.
18. Boston Consulting Group (BCG). (2023). *Making Sense of Quantum Sensing*. https://www.bcg.com/publications/2023/making-sense-of-quantum-sensing.
19. Ibid.
20. Citi Group. (2024). *Quantum Sensing: Tech's New Eyes and Ears*. https://www.citigroup.com/global/insights/quantum-sensing-tech-s-new-eyes-and-ears.
21. Business Wire. (2024). *Infleqtion Marks Milestone with First UK Sale of Quantum Clock, Tiqker*. https://www.businesswire.com/news/home/20240626231360/en/Infleqtion-Marks-Milestone-with-First-UK-Sale-of-Quantum-Clock-Tiqker.
22. National Institute of Standard and Technology (NIST) Computer Security Resource Center. (2020). *NIST IR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. https://csrc.nist.gov/pubs/ir/8309/final.

23. National Institute of Standard Technology (NIST). (2025). *Considerations for Achieving Crypto Agility – Strategies and Practices*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf; Boston Consulting Group (BCG). (2025). *Ensuring Online Security in a Quantum Future*. https://www.bcg.com/publications/2021/quantum-computing-encryption-security.
24. Stephanie, W., Elkouss, D. & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, vol. 362. https://www.science.org/doi/10.1126/science.aam9288.
25. Fazel, M. et al. (2024). Fluorescence microscopy: A statistics-optics perspective. *Rev. Mod. Phys.*, vol. 96, no. 2. https://pure.tudelft.nl/ws/portalfiles/portal/210946439/RevModPhys.96.025003.pdf.
26. IDQ. (2024). *Why the financial sector is embracing a dual quantum-safe strategy*. https://www.idquantique.com/why-the-financial-sector-is-embracing-a-dual-quantum-safe-strategy/.
27. Scott, A. (2010). BQP and the Polynomial Hierarchy. *Electron. BQP and the polynomial hierarchy*, pp. 141-150. https://dl.acm.org/doi/10.1145/1806689.1806711.
28. Ibid.
29. World Economic Forum. (2024). *Navigating Cyber Resilience in the Age of Emerging Technologies: Collaborative Solutions for Complex Challenges*. https://www.weforum.org/publications/navigating-cyber-resilience-in-the-age-of-emerging-technologies-collaborative-solutions-for-complex-challenges/; Stephanie, W., Elkouss, D. & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, vol. 362. https://www.science.org/doi/10.1126/science.aam9288.
30. HSBC. (2024). *Asset tokenisation in the Quantum Age*. https://www.gbm.hsbc.com/en-gb/insights/innovation/asset-tokenisation-in-the-quantum-age.
31. Accenture Newsroom. (2024). *Banco Sabadell Collaborates with Accenture and QuSecure to Advance Quantum Safe Infrastructure*. https://newsroom.accenture.com/news/2024/banco-sabadell-collaborates-with-accenture-and-qusecure-to-advance-quantum-safe-infrastructure.
32. UK Government. (2025). *£121 million boost for quantum technology set to tackle fraud, prevent money laundering and drive growth*. https://www.gov.uk/government/news/121-million-boost-for-quantum-technology-set-to-tackle-fraud-prevent-money-laundering-and-drive-growth.
33. UK Quantum. (2025). *UK Regulators Report: Nation Navigates Quantum Technology Growth with Responsible Innovation, Strategic Collaboration*. https://ukquantum.org/uk-regulators-report-nation-navigates-quantum-technology-growth-with-responsible-innovation-strategic-collaboration/.
34. Monetary Authority of Singapore. (2024). *Advisory on Addressing the Cybersecurity Risks Associated with Quantum*. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf.
35. European Commission. (2024). *Commission publishes Recommendation on Post-Quantum Cryptography*. https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography.
36. G7 Cyber Expert Group. (2024). *Statement on Planning For the Opportunities and Risks of Quantum Computing*. https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf.
37. Bank of Israel. (2025). *Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities*. https://boi.org.il/media/sm4f1ssu/202501en.pdf.
38. Financial Services Information Sharing and Analysis Center (FS-ISAC). (2025). *Post Quantum Cryptography (PQC)*. https://www.fsisac.com/knowledge/pqc; Europol. (2025). *Call for action: urgent plan needed to transition to post-quantum cryptography together*. https://www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together.
39. Bank for International Settlements. (2025). *Quantum-readiness for central banks and supervisors*. https://www.bis.org/events/250212_quantum_conference.htm.
40. Monetary Authority of Singapore (MAS). (2024). *MAS Commits up to S$100 Million to Support Quantum and Artificial Intelligence Capabilities in the Financial Sector*. https://www.mas.gov.sg/news/media-releases/2024/mas-commits-up-to-s$100-million-to-support-quantum-and-artificial-intelligence-capabilities.
41. Computer Weekly. (2025). *UAE eyes quantum computing for financial services*. https://www.computerweekly.com/feature/UAE-eyes-quantum-computing-for-financial-services.
42. UK Research and Innovation. (2025). *Quantum Missions pilot competition winners announced*. https://www.ukri.org/news/quantum-missions-pilot-competition-winners-announced/.
43. QURECA. (2021). *Quantum Computing for Finance: A New Educational Series*. https://www.qureca.com/quantum-computing-for-finance-a-new-educational-series/.
44. Centre for Finance, Technology and Entrepreneurship. (2025). *Be a part of the future of quantum computing for finance*. https://courses.cfte.education/be-a-part-of-the-future-of-quantum-for-finance-with-cfte/.
45. IBM Newsroom. (2022). *HSBC Working with IBM to Accelerate Quantum Computing Readiness*. https://newsroom.ibm.com/2022-03-29-HSBC-Working-with-IBM-to-Accelerate-Quantum-Computing-Readiness.
46. The Pinnacle Gazette. (2025). *Italy Launches Ambitious National Quantum Technology Strategy*. https://evrimagaci.org/tpg/italy-launches-ambitious-national-quantum-technology-strategy-245858?srsltid=AfmBOooMQic4UBDP9F3XfOrRw4Kt4M9sJRhGpmKaIQPQ-dsz3EIOA_xz.

47. Data and Security Council of India (DSCI). (2025). *DSCI Certified Quantum Technology & Security Professional (DCQTSP)*. https://www.dsci.in/content/dsci-certified-quantum-technology-security-professional-dcqts.

48. World Economic Forum. (2022). *Quantum Computing Governance Principles*. https://www.weforum.org/publications/quantum-computing-governance-principles/.

49. Stanford Law School. (2023). *SLS Launches a First-of-its-Kind Center for Responsible Quantum Technology*. https://law.stanford.edu/press/sls-launches-a-first-of-its-kind-center-for-responsible-quantum-technology/; Inside Quantum Technology News. (2024). *May Siksik, Chief Executive Officer on "Responsible Quantum Computing" at IQT Vancouver 2024 on June 6*. https://www.insidequantumtechnology.com/news-archive/may-siksik-chief-executive-officer-canadian-innovation-network-will-speak-on-responsible-quantum-computing-at-iqt-vancouver-pacific-rim-2024-on-june-6/; Inside Quantum Technolgy News. (2024). *Mira Wolf-Bauwens, Responsible Quantum Computing Lead at IBM Research is an IQT the Hague 2024 Speaker*. https://www.insidequantumtechnology.com/news-archive/mira-wolf-bauwens-responsible-quantum-computing-lead-at-ibm-research-is-an-iqt-the-hague-2024-speaker/.

50. Inside Quantum Technology News. (2023). *Quantum Ethics and Quantum Policy: Ethicqual provides solutions via trainings, impact assessments, scenario planning, and policy research towards responsible quantum technology*. https://www.insidequantumtechnology.com/news-archive/quantum-ethics-and-quantum-policy-ethicqual-provides-solutions-via-trainings-impact-assessments-scenario-planning-and-policy-research-towards-responsible-quantum-technology/.

51. Fidelity Center for Applied Technology (FCAT). (2024). *Solving QUBOs with a Quantum-Amenable Branch and Bound Method*. https://fcatalyst.com/blog/july2024/solving-QUBOs-with-a-qunatum-amanable-branch-and-bound-method; Fidelity Center for Applied Technology (FCAT). (2021). *FCAT and IonQ Explore Machine Learning With Quantum Computing*. https://fcatalyst.com/blog/sept2021/FCAT_and_IonQ_explore_machine_learning_with_quantum_computing.

52. Mattesi, M., & et al. (2024). Diversifying Investments and Maximizing Sharpe Ratio: A Novel Quadratic Unconstrained Binary Optimization Formulation. *MDPI Open Access Journals - Quantum Reports*, vol. 6, no. 2, pp. 244-262. https://www.mdpi.com/2624-960X/6/2/18.

53. Leclerc, L. et al. (2023). Financial risk management on a neutral atom quantum processor. *Phys. Rev. Research*, vol. 5, no. 4, pp. https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.5.043117.

54. Singtel. (2025). *Singtel Quantum-Safe Network (QSN)*. https://www.singtel.com/business/products-services/quantumsafenetwork.

55. Monetary Authority of Singapore (MAS). (2024). *MAS Collaborates with Banks and Technology Partners on Quantum Security*. https://www.mas.gov.sg/news/media-releases/2024/mas-collaborates-with-banks-and-technology-partners-on-quantum-security.

56. AME Chain. (2022). *AME Chain Whitepaper*. https://whitepaper.amechain.io/; QNU. (2025). *Complete Network-Level Security*. https://www.qnulabs.com/quantum-security-platform/secure-vpn-service.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org