UK FINANCE

IDENTIFYING AND MINIMISING THE RISKS POSED BY QUANTUM TECHNOLOGY

November 2023

Contents

***FIGURE 1**: - AI Generated depiction of future quantum technology hardware*

"Never mind AI (artificial intelligence) — quantum computing is the next big thing".

Martha Lane Fox, President of the British Chambers of Commerce - June 2023

Preface

As the financial services sector delves further into the realm of emerging technologies, it becomes increasingly evident that the advancement of Quantum Computing is rapidly gaining momentum. The time has come for the industry to comprehensively grasp both the potential risks and opportunities that Quantum Computing presents to the UK's financial services industry. In a collaborative effort, UK Finance and IBM have joined forces to offer an insightful perspective on the evolution of Quantum Technology, its ramifications for the industry, and practical steps that can be taken by the sector moving forward.

Executive Summary

In an era of rapid scientific advancement, quantum computing is poised to reshape the landscape of the UK's financial services sector. With the potential to efficiently solve challenges that currently remain beyond the reach of even the world's most powerful high-performance computers, quantum technology promises to be a game-changer when applied to processes such as portfolio risk optimisation, fraud detection and product personalisation.

The UK Government recognises this potential and in March 2023 published the *National Quantum Strategy*, a 10-year plan backed by a funding commitment of £2.5 billion.[1] The UK is not alone in identifying the possible advantages of quantum computing; global advancements in quantum technology are progressing rapidly, benefiting from significant national investment, fast-paced industrial R&D innovation, and expanded venture capital funding. Major economies such as China, India, South Korea and the USA have all published quantum strategies and other jurisdictions are also racing to establish themselves as global leaders in the future quantum era. The UK must continue to invest heavily in this technology if it is to take its place at the head of the pack.

Opportunity but not without risks

Realising the potential of quantum computing will not come without risks. The IT systems and networks used in financial services rely on cryptography to ensure their security, an approach based on problems that are hard to solve on a classical computer but simple on a quantum computer. Should a Cryptographically Relevant Quantum Computer be built, it could break the encryption underpinning the security on all payments, electronic commerce, and other on-line systems.

Such cryptographic vulnerabilities are not isolated to the financial services, but their effects are particularly acute as they exist in conjunction with potential risks. UK Finance has grouped these risks into five categories:

- Cryptographic vulnerabilities
- Market instability caused by unequal access to the technology.
- Insufficient quantum talent in the UK
- Technological debt from legacy systems
- Ethical and environmental considerations associated with quantum technology.

It is vital that all parts of the financial services sector act to address these risks and become "Quantum Safe". Only then can the benefits of quantum computing be safely and fully grasped.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142942/national_quantum_strategy.pdf

Transitioning to Quantum Safe requires cross-sector collaboration

The need to be Quantum Safe has been understood since the mid-1990s, but the risk posed by quantum technology was contingent on the development of large-scale quantum computers. That time is now arguably upon us and UK financial sector firms, the third parties that supply them, and regulators that oversee them need to develop comprehensive strategies to achieve “Quantum Safe”. This transition cannot happen in isolation; all market participants must be actively supported in their efforts by complimentary cross-sectoral strategies (including exercising). UK Finance recommends that a new financial sector Quantum Safe task force – potentially under the auspices of the Cross-Market Operational Resilience Group – be established with this objective.

Firms must act now

At the firm level, UK Finance has identified specific steps that market participants of all types should make to transition to Quantum Safe. These include:

- Identifying systems, process and standards that depend on potentially vulnerable cryptography
- Performing an in-depth risk assessment of systems and processes
- Building and enhancing the skills and capabilities to support the transition to Quantum Safe
- Identifying stakeholders from firms, government, regulators and vendors
- Developing cross-sector governance for the UK’s transition to Quantum Safe

With the UK regulatory authorities in possession of so much important and sensitive market, firm and customer data, it is vital that they too begin the journey to Quantum Safe.

Quantum Safe needs a quantum literate workforce

Firms and regulators looking to exploit the benefits of quantum computing will need a skilled, quantum-literate workforce. This workforce will need not only knowledge of quantum algorithms, but also tangible experience in applying this technology to real-world business applications. With such skills currently in great demand, it is likely that organisations will need develop home-grown skills in the near-term to complement their external recruitment efforts. To help bridge this gap, UK Finance recommends that HM Government develop a specific quantum-literate workforce strategy incorporating quantum education into future amendments to the UK’s educational curriculum and targeted reforms to the migration system.

Being Quantum Safe is the key to unlocking quantum technology’s potential

Quantum computing’s potential is considerable, but it cannot be viewed in isolation; the risks inherent to this technology must be proactively addressed if these opportunities are to be realised. Transitioning to Quantum Safe will give clients, customers and key market participants the confidence to embrace this technology, but it will require active management from all parts in the financial services sector. We recommend that this is achieved through the central development of, and adherence to, sector-specific Quantum Safe roadmaps.

Section 1: An introduction to Quantum Computing

Quantum Computing is fundamentally different to classical computing. Simply stated, quantum computers will likely solve problems faster, cheaper and more efficiently.

Quantum computing is an emerging technology that harnesses the principles of quantum mechanics to revolutionise current computation methods. While classical computers process information using bits represented as 0s and 1s, quantum computers utilise quantum bits (qubits) that can encode information in a fundamentally different manner. This unique approach enables quantum computers to tackle complex problems in entirely new ways.

What is Public Key Cryptography?

The technology that underpins the security of the web, electronic commerce, mobile communications and government services. A way of sharing confidential information that does not require the prior exchange of secret keys. It is ideal for securing communications when the parties have not met before. e.g., online commerce. RSA is one widely used public key system.

The strength of quantum computing lies in three fundamental principles of quantum mechanics: superposition, interference, and entanglement. These three principles, among others, empower quantum computers to potentially perform complex computations that would be intractable for classical computers or require exponentially more classical resources to compute.

For instance, public key cryptography is widely used to secure communications, websites, and blockchains, using algorithms such as RSA. Breaking these keys involves finding prime factors of a large number. In a classical approach, breaking a single key would take the world's most powerful supercomputer millions of years.

What is Shor's Algorithm?

In 1994, Bell Labs researcher Peter Shor came up with a way (an "algorithm") to use a quantum computer to factor a large number very quickly. The implication is that Shor's Algorithm can break public-key cryptography such as RSA in a few hours, not the few million years that it would take using a classical computer. Shor's Algorithm has been implemented and proven to work on simulators and on actual quantum computers. The scale of quantum computers currently available limits how large a number we can factor.

The quantum approach relies on two innovations to break RSA keys in a few hours, disrupting fields that rely on cryptography and computational security. One innovation is **Shor's Algorithm** which is already proven to speed-up breaking RSA. The other innovation is a quantum computer of sufficient scale and quality – which we call a CRQC.

Quantum computing has many potential application areas in a variety of industries which include simulating nature, mathematics, processing data with complex

structure (machine learning) and optimisation and simulation. Within these use case areas, the ability to solve a problem more efficiently, more accurately or faster with a quantum computer than using purely classical computation alone is defined as the point of "Quantum Advantage". This includes both solving problems we note as intractable today i.e., breaking RSA encryption, but also solving problems we can solve today but more efficiently i.e., derivative pricing.[2]

What is a Cryptographically Relevant Quantum Computer (CRQC)?

The quantum computers available in 2023 do not have the number of qubits or the quality required to run Shor's Algorithm for the large numbers used in public key cryptography. Our current quantum computers are "noisy intermediate scale quantum computers" or NISQ. The technology of quantum computers is improving. The number of qubits increased from 5 qubits (in 2016) to 433 qubits (in 2023). The quality has also improved. A CRQC is one that has the potential to break current public key systems. This definition of a CRQC is from the US National Security Agency (NSA).

The journey so far

Since its inception, quantum computing has embarked on a remarkable journey of advancement, ushering in a new era of computation that challenges the boundaries of classical computing paradigms. Over the past few decades, this field has witnessed significant progress, marked by a series of ground-breaking milestones. From initial theoretical concepts to experimental realisations of quantum bits (qubits) and their manipulation, the journey has been both inspiring and transformative. As we stand at the intersection of theoretical promise and tangible progress, it is imperative to delve into the key milestones achieved thus far, understanding their significance, and to project the potential trajectories that quantum computing might take in the foreseeable future.

Gaining insight into the trajectory of quantum computing progress and the significant milestones attained is of paramount importance, serving as a crucial guidepost for businesses operating within the financial services sector. While the exact implications of quantum computers remain uncertain, it is evident that the pace of technological advancement in this arena is advancing. Consequently, enterprises must grasp the intricacies of this evolving landscape and proactively monitor indicators of progress and potential disruptions to effectively navigate this transformative journey.

After decades of R&D and billions of dollars of investment, quantum computers are no longer purely theoretical, with large technology firms such as IBM, Google, Amazon and Microsoft all developing quantum hardware. We are now beginning to see the impact of this progress with a rapidly developing quantum computing market. By some estimates, the global Quantum Computing as a Service (QCaaS) market could reach £21 billion by 2030.[3]

[2] https://arxiv.org/pdf/1905.02666.pdf

[3] https://thequantuminsider.com/2021/08/12/report-quantum-computing-as-a-service-market-to-hit-26-billion-by-end-of-decade/

While much ambiguity exists across the quantum computing area there is an emerging consensus that the next few years will be the tipping point for the technology. In a recent UK cross sector survey nearly half the executives who completed the survey (48%) believe quantum computing will play a significant role in their industries by 2025.[4]

In 2016 the US National Institute of Standards and Technology started the post-quantum cryptography standardisation process. The objective was to identify and standardise replacements for vulnerable public key cryptography algorithms such as RSA and DS. By mid-2023, the process had published draft standards with more expected in the immediate future.

Company	Qubit Tech	2023	2024	2025	2026	2027	2028	2029	2030
ColdQuanta	Cold Atom		1,000+						
Google	Superconducting							1mn+	
IBM	Superconducting	1,121		1,386+		4,158+		10K-100K	
Pasqal	Cold Atom		1,000+						
Rigetti	Superconducting	84		336		1,000+		4,000+	

***TABLE 1**: The projected future improvements (in terms of power) that some of the world's leading quantum computers will achieve between 2023-2030. Source: CITI Quantum report 2023 – page 23 - Citi GPS: Global Perspectives & Solutions - QUANTUM COMPUTING Moving Quickly from Theory to Reality*

Various technology companies are developing quantum computers and releasing roadmaps to chart their paths forward.

The qubit count (i.e., the scale of quantum computers) is generally used as main driver to represent the development of the quantum machine, as many qubits are needed to implement production scale use cases and error correction techniques. Table 1 details the number of qubits that projected quantum machines will have in the next 7 years for many of the leading players in the industry.

[4] https://assets.ey.com/content/dam/ey-sites/ey-com/en_uk/topics/emerging-technology/quantum/ey-quantum-readiness-survey-2022.pdf

What is Q-Day?

Shorthand for when a cryptographically relevant quantum computer is available that can break a production public key system, e.g., RSA-2048.

Scale isn't the only driver of progress, however, the speed in which quantum computers operate and quality of the computation are also just as significant factors in their development. Various innovations have allowed and will continue to allow improvement in all these areas, facilitated by both the physical engineering of the quantum computers and logical components such as intelligent orchestration of computational jobs or error mitigation techniques.

The NSA defines a quantum computer as one that is capable of attacking real world cryptographic systems that would be infeasible to attack with a normal computer (i.e, "break encryption") as a CRQC.[5] As the scale, quality and speed of these machines improves, we become incrementally closer to the point where the security of existing encryption is in jeopardy. In June 2023 the journal *Nature* published a paper investigating and comparing classical methods of a specific calculation against quantum methods using a currently available 127-qubit quantum machine. The article showed the achievement of a result well out-of-reach for classical simulations alone and argues that such a result evidences promise for utility of a quantum computer at current levels of fault tolerance. This benchmark experiment suggests quantum computers could have useful real-world applications within two years, with experts such as John Martinis, a physicist at the University of California, Santa Barbara commenting that "it makes you optimistic that this will work in other systems and more complicated algorithms.[6]

The development of quantum computing is occurring at a time of global competition. Nation states with the technical capability and the strategic intent are demonstrating signs of being engaged in a race to achieve a dominant position.

While supported by their respective governments, western endeavours in quantum technology have been largely driven by commercial and private business entities. To be at the head of the pack, the UK's Quantum Strategy must address both the development of quantum hardware and lead the way in becoming safe. Additionally, the UK needs to remain aware of developments on the international stage if we are to become a global leader in this technology.

[5] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[6] https://www.nature.com/articles/d41586-023-01965-3

The global view

Efforts undertaken by other nation states and geopolitical collectives (like the EU) can broadly be split into one of two categories:

1. Actions and investments aimed at the protection of their national assets from the threats posed by quantum technology.
2. Actions and investments designed to advance develop and utilise quantum technology, such as the design and build of quantum hardware.

While some actions, such as the advancement of quantum focused academic programs, could be seen as supporting of both, it is evident that many nation states are, like the UK, are pursuing goals in each.

India

The National Mission for Quantum Technology and Applications (NM-QTA) was announced in 2020 with funding of Rs 8000 crore (£790million).[7] In April 2023 the Union Cabinet approved the "[Indian] National Quantum Mission" with a budget of Rs 6000 crore (£590 million)[8] from FY 2023 to FY 2030. Its aim is to develop 1000 qubit quantum hardware and quantum communications networks. If delivered, this will be a powerful addition to fulfilling their quantum ambitions.

India's quantum program goes further, also encompassing work on other quantum technologies such as satellite based secure quantum communications and a multi-node network with quantum memories. Combined with India's huge technical talent pool, this will benefit a range of sectors (including financial services) and help all parts of its economy harness the potential of quantum technology.

Finally, the Indian Army established the Quantum Lab at the Military College of Telecommunication Engineering, with one of its core objectives being to transform the current system of cryptography in the Indian Armed Forces to post-quantum cryptography.[9]

[7] Budget 2020 announces Rs 8000 cr National Mission on Quantum Technologies and Applications, Department of Science and Technology, https://dst.gov.in/budget-2020-announces-rs-8000-cr-national-mission-quantum-technologies-applications

[8] Budget 2020 announces Rs 8000 cr National Mission on Quantum Technologies and Applications, Department of Science and Technology, https://dst.gov.in/budget-2020-announces-rs-8000-cr-national-mission-quantum-technologies-applications

[9] Almost into 2022 – a glance at India's work towards "quantum technologies", 30 Dec 2021, Ministry of Electronics and Information Technology (MeitY), https://indiaai.gov.in/article/almost-into-2022-a-glance-at-india-s-work-towards-quantum-technologies

China

In 2016 China launched Micius, the world's first quantum communications satellite. In May 2023 Chinese researchers claimed that they have developed an algorithm capable of running on a small quantum computer which could potentially decipher advanced encryption systems commonly used by governments and financial institutions. Nevertheless, scientists outside of China have greeted these claims with considerable scepticism.

China has made substantial investments in the development of quantum technologies. While precise figures are unclear, existing studies suggest that China holds a commanding lead in government expenditure in this field. According to McKinsey's June 2022 estimates, the Chinese government has publicly announced a sum of £12.6 billion in funding, nearly double that of the European Union (£7 billion) and more than triple that of the United States (£3 million) billion USD). Nevertheless, it's worth noting that these figures aren't universally accepted; studies conducted by Q*uantum Insider* have placed the range of Chinese government investments in the quantum sector somewhere between £.3.3 billion and £14 billion.

Chinese researchers are also working on post-quantum cryptography. A national process run by the Chinese Association for Cryptologic Research led to the selection of Post Quantum Cryptography (PQC) algorithms for China in 2020.[10] In terms of timing, this puts China ahead of the western, NIST's *Post-Quantum Cryptography Standardization Project* which is expected to select PQCs in early 2024.

Russia

The Russian government announced in 2021 that it would invest $790 million in quantum computing research over the next five years. In July 2023, Russian president Vladimir Putin was presented with a 16-qubit quantum computer at the Forum for Future Technologies.

Additionally, Russia is known to be engaged in multiple research projects in quantum communications.[11] Whilst is it less well known as to how Russia intends to utilise the results of this research, it can be assessed that its prime use will be for the protection of information from eavesdropping.

[10] Announcement on the Algorithm Selection Results of the National Cryptography Algorithm Design Competition, Chinese Association for Cryptologic Research, 2 January 2020 (in Mandarin), https://www.cacrnet.org.cn/site/content/854.html

[11] World Tour: Quantum Communication Activities in Russia, A. Federov, Russian Quantum Center. ETSI Quantum Workshop, 2018, https://docbox.etsi.org/Workshop/2018/201811_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/01worldtour/RUSSIA_FEDOROV.pdf

Russia's cryptography standardisation committee TK.26 created a working group on post cryptographic mechanisms in 2019. At this point there are proposals for key encapsulation and digital signature, but no published standards.[12]

South Korea

The President of South Korea announced the '*National Strategic Technology Nurture Plan'* in October 2022 with next generation nuclear energy and quantum the two primary national strategic technology projects.[13] In June 2023, the South Korean government announced the details of the quantum program with combined investment of 3 T won (£1.8 billion) from government and industry.[14]

In terms of workforce, South Korea objective is to build a skilled workforce of up to 2500 quantum researchers and 10,000 professionals, while similarly to India, the South Korean government also plans to build an inter-city quantum communications network.

Finally, and in the search for international partners , South Korea and the US have agreed a co-operation plan for quantum information science and technology.[15] In relation to PQC South Korea's Ministry of Science and ICT has stated that in preparation for the collapse of existing encryption systems due to the development of quantum computers, they will establish plans for the transition to next-generation encryption and develop Korean algorithms. To this end, KT (a South Korean telecommunications provider) implemented a commercial VPN service secured using PQC in 2023.

United States

The US *National Quantum Initiative Act 2018* aims to "accelerate research and development [of quantum technology] for the economic and national security of the United States."

The bipartisan Quantum Computing Cybersecurity Preparedness Act was signed December 2022. This legislation mandates both the identification of vulnerable federal government information technology, and the subsequent migration towards "quantum safe" equivalents. Various commentators have noted that the private sector will eventually have to follow suit and input similar measures to protect itself from the threats that will arise when the current encryption standards are no longer sufficient to protect sensitive data.

---

[12] A Brief Survey of World Post-Quantum Cryptography Standardization Efforts, 01 Nov 2022, https://www.linkedin.com/pulse/brief-survey-world-post-quantum-cryptography-efforts-igor-barshteyn/

[13] Korea to announce national strategy to become a technology hegemon, Ministry of Science and ICt, 28 Oct 2022, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=746&searchOpt=ALL&searchTxt=

[14] In 2035, Korea Becoming the Global Hub for Quantum Economy, Ministry of Science and ICT, 27 Jun 2023, https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=6930&insttCode=A110439&type=O

[15] Joint Statement of the United States of America and Republic of Korea on Cooperation in Quantum Information Science and Technologies – April 23

Unlike Russia and China, both of whom are independently developing their own PQC algorithms, many nations allied to the US are awaiting the results of the NIST project to develop a standard. It is highly likely that the UK will adopt this standard when it is released. While led by NIST, this has been an international effort which should be looked upon as an example of how geopolitically aligned nations can tackle these problems collectively for the betterment of the collective.

Recommendation 1: Understand the global picture

The UK's national strategy must encompass two fundamental components supporting technological advancement and driving quantum safety. Achieving this necessitates both direct investment and advocating for and facilitating the adoption of secure quantum practices and cutting-edge technology by private enterprises. Only through this two-fold strategy can the UK maintain its leadership position.

Other national initiatives on quantum cryptography

Government guidance on managing the transition to post-quantum cryptography is available across a wide range of countries. For firms operating across multiple jurisdictions and who are considering how they can start the transition to Quantum Safe, a high-level summary is provided below.

Country / Region	Summary	Reference
Canada	The Quantum-Readiness Working Group, launched in 2020 by the Canadian Forum for Digital Infrastructure Resilience brings together key organisation in Canada's financial sector and publishes best practice and guidelines for Canadian firms by studying what it will take to make Canada "quantum ready" for the years ahead.	*Canadian National Quantum-Readiness: Best Practices and Guidelines*, Version 03 – June 12, 2023
China	The Chinese Association for Cryptologic Research ran a design process competition to standardise post-quantum cryptographic algorithms for China. The primary goal is to support the construction of new network security systems.	*Announcement on the Algorithm Selection Results of the National Cryptography Algorithm Design Competition*, Chinese Association for Cryptologic Research, 2 January 2020
EU	The European Union Agency for Cybersecurity (ENISA) publishes guidance on post-quantum cryptography and migration to PQC. ENISA seeks to give insight on post-standardisation challenges, and the necessity to design new cryptographic protocols and integrate post-quantum systems into existing protocols. As a follow-up to ENISA's 2021 *Post-Quantum Cryptography: Current State and Quantum mitigation* study, the new report elaborates on the topic to address technical areas of interest.	*Post-quantum cryptography - Integration study*, 18 Oct 2022, ENISA - European Union Agency for Cybersecurity https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
France	ANSSI *(Agence nationale de la sécurité des systèmes d'information - the National Agency for the Security of Information Systems*) provides guidance on the transition to post-quantum cryptography for French firms and outlines views on the so-called post-quantum cryptography transition. The paper seeks to provide directions to industrials developing security products	*ANSSI views on the post-quantum cryptography transition* March 25, 2022, ANSSI. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

	and outlining the transition agenda in terms of French security visas.	
Germany	The BSI (Bundesamt fur Sicherheit in der Informationstechnik, or Federal Office for Information Security) publishes guidelines on post-quantum cryptography. The BSI's guide is intended to provide an overview of the most important developments in the field of quantum technologies from the point of view of IT security, as well as recommendations for action for migrating to quantum-safe cryptography.	Quantum-safe cryptography – fundamentals, current developments and recommendations, 18.05.2022, Bundesamt fur Sicherheit in der Informationstechnik (Federal Office for Information Security)
South Korea	South Korea is running a national competition to identify standardisation of post quantum cryptography, organised by the Quantum Resistant Cryptography Research Center.	Korean Centre for Quantum Resistant Cryptography's Quantum Resistant Cryptography National Competition (2022-on).
USA	NIST has been running an open process to standardise post-quantum cryptographic algorithms since 2016. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and can protect sensitive government information well into the foreseeable future, including after the advent of quantum computers. The NSA has also been running a process to standardise post-quantum cryptographic algorithms for US Government use. The NSA released the "*Commercial National Security Algorithm Suite 2.0*" (CNSA 2.0) Cybersecurity Advisory (CSA) in September 2022 to notify National Security Systems (NSS) owners, operators and vendors of the future quantum-resistant (QR) algorithms requirements for NSS — networks that contain classified information or are otherwise critical to military and intelligence activities.	NIST Post-Quantum Cryptography https://csrc.nist.gov/projects/post-quantum-cryptography NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems (07 Sep 2022) https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

TABLE 2: *Existing government guidance on managing the transition to post-quantum cryptography by state.*

Finance sector initiatives on quantum cryptography

There are finance sector-specific initiatives to manage the transition post-quantum cryptography in Canada, Japan and from several international bodies.

Organisation	Description of initiatives
Bank for International Settlements	*Project Leap: Quantum-proofing the financial system,* Bank for International Settlements Innovation Hub, June 2023 Project Leap was launched by the BIS Innovation Hub's Eurosystem Centre together with the Bank of France and Deutsche Bundesbank, the project partners within the Eurosystem, to prepare central banks and the global financial system for a transition towards quantum-resistant encryption.
Bank of Canada	*Privacy-Preserving Post- Quantum Credentials for Digital Payments*, Staff Working Paper/Document de travail du personnel — 2023-2033, June 2023 The paper proposes a pseudonymous credential scheme for use in payment systems to tackle the problem of protection for users from fraud and abuse while retaining privacy in individual transaction. The scheme is privacy-preserving, efficient for practical applications, and hardened against quantum computing attacks.
Bank of Japan	*Recent Trends on Research and Development of Quantum Computers and Standardisation of Post-Quantum Cryptography.* Kazutoshi Kan and Masashi Une*, Discussion Paper No. 2021-E-5*, Bank of Japan. This paper discusses recent trends in the R&D of quantum computers and the security risks of public-key cryptographic algorithms. It reviews NIST's ongoing progress in standardising post-quantum cryptography and the responses of other organisations in support of the migration and the future challenges for its real-world implementation.
Industry Canada	*Canadian National Quantum-Readiness: Best Practices and Guidelines,* Version 02 – June 17. 2022. Published by the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) The Quantum-Readiness Working Group, launched in 2020 by the CFDIR brings together key organisation in Canada's financial sector and publishes best practice and guidelines for

Organisation	Description of initiatives
	Canadian firms by studying what it will take to make Canada "quantum ready" for the years ahead.
World Economic Forum	Quantum security project, including *Transitioning to a Quantum-Secure Economy* (published 13 September 2022) In September 2022, in collaboration with Deloitte, the World Economic Forum (WEF) published a white paper outlining a roadmap for organisations achieving a quantum secure economy and seeking to maximise the opportunities, and minimise the risks, represented by the arrival of quantum computers. This white paper arises from in-depth discussions between senior leaders and quantum experts from the quantum security working group, part of the quantum computing network of the World Economic Forum.

***TABLE 3**: Financial sector specific initiatives aimed at helping manage the transition to post-quantum cryptography.*

The UK's approach

As highlighted in the August 2023 UK National Risk Register, preventing disruption to the financial services sector is a key concern to the UK's national interests. With the financial sector heavily reliant on technology that could be vulnerable to quantum computing-enabled attacks, and with the UK's international competitors investing heavy in quantum technology, HM Government must work closely with the financial services sector to build capability and transition to Quantum Safe, UK's National Quantum Strategy.

In March 2023 the UK Government's Department for Science, Innovation and Technology (DSIT) released Its *National Quantum Strategy*.

The vision aims to establish the UK as a preeminent quantum-driven economy by the year 2033. This strategic ambition envisions a robust quantum sector that seamlessly integrates quantum technologies into the very core of the nation's forthcoming digital infrastructure and advanced manufacturing capabilities. This approach is poised to contribute to economic growth, enhance societal resilience, and usher in a prosperous era.

In line with this vision, a substantial investment of £2.5 billion has been proposed for the advancement of quantum technologies within the UK over the next ten years, commencing from 2024. This allocation represents a considerable augmentation of current public investments and is geared towards triggering an additional £1 billion in private investment. The overarching objectives of this comprehensive program encompass the following:

Cultivating quantum science and engineering excellence: The intent is to position the UK at the forefront of quantum science and engineering globally, thereby enriching the nation's expertise and skill base in this transformative field.

Enabling quantum enterprise: A strategic push to make the UK the preferred destination for quantum-focused businesses is evident. This will involve fostering a vibrant quantum ecosystem, integrating the nation into the international supply chain, and drawing in both global investors and top-tier talent.

Propelling quantum adoption: The strategy seeks to drive the widespread implementation of quantum technologies across the UK landscape. The ultimate goal is to yield substantial economic and societal benefits, all while augmenting the country's national security apparatus.

Instituting robust regulatory frameworks: The strategy acknowledges the necessity of well-defined national and international regulations that guide the ethical deployment of quantum technologies. This framework also serves to safeguard the UK's capabilities and national security interests.

The strategy outlines a comprehensive ten-year roadmap, with a plan of prioritised actions. The early stages of quantum technology advancement underscore the importance of bolstering scientific progress, nurturing a dynamic ecosystem, exploring diverse technology platforms, and leveraging the UK's unique strengths across different segments of the supply chain. Alongside these, a targeted emphasis on software development and exploration of viable use cases is duly acknowledged. Furthermore, a recognition of the significance of targeted efforts, wherein partnerships with industry players expedite progress in high-value applications as they surface, is salient. This tactical approach is instrumental in shaping a world-class quantum sector that significantly contributes to both the economy and society.

> *"That is why, today, we are putting the full might of the British government and our private sector partners behind our push to become a scientific and technological superpower, because only through being world-leaders in future industries like AI and quantum will we be able to improve the lives of every Briton."*
>
> **Science, Innovation and Technology Secretary Michelle Donelan**

The dynamic nature of quantum technology progression necessitates continual refinement of prioritised actions, adapting them to evolving trends and changing landscapes. HM Government has proposed that this adaptation process is undertaken through extensive consultation with the UK's quantum community. Ongoing updates will be provided to the National Science and Technology Council, chaired by the Prime Minister, thus ensuring robust oversight and accountability. Additionally, an annual progress report will be disseminated, underscoring the commitment to transparency and the achievement of quantum technology goals.

Accompanying the UK's ambitions for quantum technology is a growing understanding of the challenges inherent with its adoption. While the development of this understanding has been catalysed by the release of UK's *National Quantum Strategy*, UK Finance is concerned that the meteoric rise of awareness in Artificial Intelligence (AI) usage (specifically consumer use of generative AI platforms) may have drawn some attention away from the potentially more profound issues regarding quantum technology.

While quantum technology's "ChatGPT Moment" is yet to happen, the financial sector must do more to ensure that generative AI does not eclipse quantum computing on the technology agenda. There is a significant but fleeting opportunity for stakeholders to develop approaches, address the foreseeable issues and put in place viable mitigation measures to the risk and thus enable this technology.

Section 2: Addressing the Risks

Harnessing the potential of quantum technology will only be realised if the risks accompanying its adoption are addressed at both a firm and sectoral level. Financial services firms, the financial services sector, and the wider UK economy must become Quantum Safe.

If the UK's is to become Quantum Safe building an accurate picture of the risks that arise from this technology is key. UK Finance has identified the most important of these risks and grouped them into five categories:

1. Cryptographic risk
2. The technological debt from legacy systems
3. Shortages of talent and skills deficiencies
4. Ethical and environmental considerations
5. The risk posed by quantum computing to market stability

Issues arising from cryptography vulnerabilities due to the endemic nature of strong cryptographic algorithms currently used to secure the financial services sector make up the lion's share of the risk. This direct and tangential risk is only part of the picture; however, integral to the UK's planned adoption of quantum technology is the need for firms to consider the entire scope of risks in protect their interests. Only then the UK will be considered truly Quantum Safe.

What is Quantum Safe?

The concept of a system, entity, organisation or collective achieving a state where they are prepared to counter the threats posed by quantum technology.

Risk 1: Cryptographic risk

The emergence of quantum computers presents a formidable challenge to our trusted security measures. Cryptography – the shield that safeguards financial data and communications – faces potential vulnerabilities due to the extraordinary capabilities of CRQCs.

In the realm of cryptography, contemporary encryption techniques are built upon intricate mathematical puzzles that classical computers struggle to solve efficiently. he advent of CRQCs however poses a very significant threat; quantum computers can potentially crack these puzzles with remarkable speed, weakening the protection historic techniques provide.

Of particular concern are widely used cryptographic methods such as RSA and ECC. These underpin various layers of the technology estates supporting most products and services across the UK's financial services sector. This pervasiveness amplifies the urgency of addressing potential quantum vulnerabilities, with these commonly utilised cryptographic methods deeply embedded in the hardware

and software technology solutions that have been developed over decades. In some instances, these are deployed by in-house teams, while others have been deployed by vendors and partners. Such an approach has resulted in a complex landscape where these cryptographic methods are deeply embedded yet not always deployed in a transparent way across the technology supply chain.

Compromise of RSA and ECC by CRQCs could undermine critical aspects of financial operations such as data security and communication privacy. Recognising and understanding these vulnerabilities is paramount for UK financial institutions and underscores the necessity of adopting novel encryption methods capable of standing up to quantum threats. Proactively embracing such methods will enable the financial sector to fortify itself for a future where data remains secure, even in the face of formidable quantum computers.

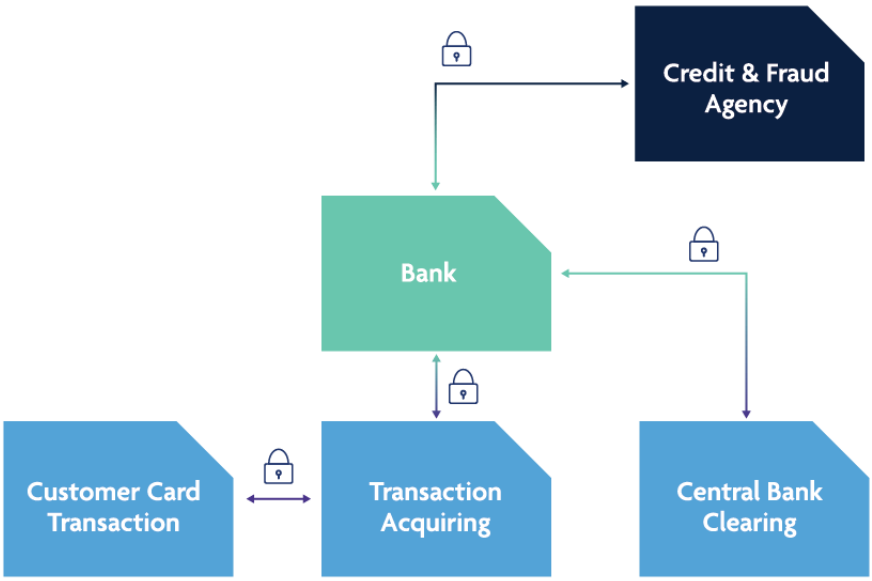

FIGURE 2*: Illustration of transaction processing and the dependency on encryption. Low cost and readily accessible encryption have allowed the UK FS sector to build out services across an interconnected ecosystem reducing costs and accelerating innovation for the sector)*

What cryptographic risks means for the financial services sector

Quantum technology and the advent of CRQCs brings both unprecedented opportunities and profound challenges to all parts of the of financial services sector. This includes not only private market participants such as banks and financial market infrastructures, but also the regulatory and supervisory bodies that oversee them. If all are to be prepared for the change that is coming, all must understand the how the risks apply to them.

At its most basic level, the continued evolution of CRQCs with bring with it a capability to unravel conventional cryptographic safeguards. This will pose a multifaceted risk to the security posture of financial institutions and regulatory bodies.

This section underscores the critical need for vigilance of the potential threats that CRQCs introduce, highlighting the intricate ways in which malicious actors could exploit these quantum machines to undermine the integrity and confidentiality of financial services businesses.

Cryptographic Risk 1: The security of stored personally Identifiable Information (PII)

In the age of rapid data accumulation, the security of personally identifiable information (PII) within financial services businesses remains a paramount concern. Malicious actors, utilising Advanced Persistent Threat (APT) strategies, can currently exploit vulnerabilities in traditional cryptographic systems to gain unauthorised access to sensitive customer information including account details and financial holdings. Compromised data may then be covertly stored, awaiting the eventual decryption power of CRQCs. This looming threat is particularly significant for Politically Exposed Persons (PEPs), whose PII data could retain its value and exploitability for the entirety of their lifetimes.

What is the "store now decrypt later" threat?

One risk arising from quantum technology is known as the "store now decrypt later" scenario. The essence of this threat lies in the potential capability of CRQC – potentially operated by state or state-backed groups – to retroactively decrypt data that has been stored with current encryption methods. This has profound implications for financial firms tasked with safeguarding their clients' confidential information, transaction records, and proprietary data.

“Store now decrypt later” poses significant challenges for any organisation that has obligations to securely retain sensitive data, not just those in the financial services sector.

Evidence of this risk is demonstrated by the increasing frequency of data breaches and cyberattacks targeting financial institutions. Globally, the financial sector experienced the second highest number of data breaches in 2022, behind only government, while the number of consumer records leaked in breaches globally exceeded 254 million.[16]

These breaches exposed millions of individuals' PII, emphasising the urgency for heightened cybersecurity measures that account for the evolving threat landscape posed by CRQCs. As CRQCs mature, the possibility of retroactively decrypting stored data becomes a substantial concern, necessitating proactive measures to safeguard sensitive information.

[16] https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/

Cryptographic Risk 2: Authentication vulnerabilities in wholesale payment systems

The security of wholesale payment systems – a cornerstone of financial infrastructure – faces a significant threat from the potential exploitation of CRQCs. State or state-sponsored actors, known for their APT capabilities, are already known to target central bank payment systems, such as the 2016 attack on the Bangladesh Bank and the Federal Reserve Bank of New York which exploited vulnerabilities in the SWIFT network, orchestrating fraudulent transactions that amounted to a staggering £788 million (with only £67 million recovered).

Wholesale payment systems heavily rely on public key cryptography for authentication, a mechanism susceptible to CRQCs immense computational power. A determined attacker equipped with a CRQC could undermine the authenticity of transactions by exploiting weak points in the cryptographic framework, allowing for the creation of fraudulent payment instructions that mimic legitimate transactions. The potential fallout from such an attack could be catastrophic, disrupting the financial stability and trust that underpin these systems.

The 2016 SWIFT attack serves as a sobering illustration of the vulnerabilities that already exist within our financial systems. As CRQCs inch closer to reality, the urgency to bolster security measures and implement post-quantum cryptographic protocols becomes ever more critical to safeguard wholesale payment systems from evolving threats.

Cryptographic Risk 3: Compromise of inter-bank system interfaces, e.g., Open Banking APIs

The proliferation of Open Banking initiatives and interconnected financial systems has brought remarkable convenience to customers, but it also introduces a potential avenue for exploitation by malevolent actors leveraging CRQCs. Open Banking APIs and inter-bank system interfaces form a critical juncture where data flows and transactions take place seamlessly between institutions.

The risk lies in the possibility of an attacker leveraging the immense computational power of CRQCs to exploit vulnerabilities within these interfaces. The compromised interfaces could enable unauthorised access to sensitive financial data, customer information, and transaction records, undermining the very foundation of trust that these systems are built upon.

Evidence of this risk can be seen in the rising number of cyber incidents targeting financial institutions and their interconnected systems. IBM's X-Force Threat Intelligence Index report shows that the UK accounted for 43% of attacks observed in Europe over the past 12 months. The energy and finance sectors suffered the most breaches each suffering 16% of the UK's cyberattacks in 2022.[17]

As we move forward, the preservation of the integrity and security of inter-bank system interfaces becomes an imperative. Strengthening these interfaces against the looming threat of CRQCs requires

[17] https://www.ibm.com/reports/threat-intelligence

both the adoption of robust encryption techniques and the exploration of innovative security measures to ensure the continued resilience of Open Banking and interconnected financial systems.

Cryptographic Risk 4: Compromise of Distributed Ledger Technology based financial instruments

Distributed Ledger Technology (DLT), including blockchain, has emerged as a potentially transformative force in the financial services landscape however this very innovation is not immune to the looming threat posed by CRQCs.

The inherent security of DLT is predicated on cryptographic principles, with the initial block (genesis block) serving as a foundational element. This genesis block, while designed to be secure in current cryptographic standards, could become a prime target for the computational prowess of a CRQC. The ability to retroactively alter the contents of the genesis block could unravel the entire integrity of subsequent blocks, potentially compromising the immutability and transparency that DLT promises.

The vulnerability of DLT-based financial instruments, particularly in their nascent stages, underscores the urgency to anticipate and address the implications of CRQCs. As the financial sector increasingly embraces DLT to enhance efficiency and security, it is imperative to invest in robust post-quantum cryptographic methods that fortify the foundations of this technology against future threats.

Cryptographic Risk 5: Authentication vulnerabilities for privileged access to infrastructure and systems

In the realm of financial services, maintaining the security and integrity of administrative access to critical infrastructure and systems is paramount. However, this very cornerstone of control is vulnerable to the disruptive capabilities of CRQC.

Administrative authentication – often reliant on public key cryptography – forms the bedrock of privileged access to financial systems, yet as CRQCs advance, the cryptographic foundations underpinning this authentication mechanism could be compromised. An attacker armed with a CRQC could potentially exploit the vulnerabilities within the authentication process, gaining unauthorised access to systems.

Once inside, the consequences could be dire. By manipulating software, security controls, or system configurations, the attacker could subtly alter the system's behaviour, facilitating the generation of fraudulent transactions that evade traditional detection methods.

The urgency to address this risk is underscored by the ripple effects such a compromise could trigger. As administrators hold the keys to critical financial systems, safeguarding their authentication mechanisms against quantum threats becomes imperative. Establishing quantum-resistant authentication protocols is an essential step towards preserving the sanctity of financial infrastructure and protecting against unauthorised manipulation.

Cryptographic Risk 6: Authentication vulnerabilities in consumer payment systems

As consumers increasingly embrace digital payment methods, ensuring the security of their transactions is of paramount importance. While the risk of compromise in consumer payment systems due to CRQCs may initially appear low, it is vital to maintain consumer confidence in the security of these systems.

Consumer payment systems heavily rely on authentication protocols to guarantee the integrity of transactions and safeguard sensitive user data. Even though the immediate quantum threat might be targeted towards high-value transactions, the long-term implications of compromised confidence in the system's security cannot be understated. It's essential to recognise that ensuring consumer trust in online financial services is integral to their widespread adoption and continued use.

Proactive steps to bolster authentication mechanisms with quantum-resistant encryption are not only about mitigating immediate risks but also about fostering a resilient foundation that instils confidence among consumers. As the financial services sector continues to evolve alongside quantum advancements, safeguarding consumer trust remains paramount to preventing potential abandonment of online services due to apprehensions about security vulnerabilities.

Cryptographic Risk 7: Vulnerabilities in software and system integrity

Maintaining the integrity of software and firmware updates is an essential pillar of security in modern financial systems. The emergence of CRQCs threatens this integrity.

Currently, digital signatures underpin the verification of software and firmware authenticity. These signatures often rely on public key-based algorithms, which, in the face of advancing CRQCs, can be compromised. An attacker with the capability to bypass these integrity checks could effectively manipulate the software and firmware running within financial systems. This manipulation not only opens the door to executing unauthorised transactions but also grants the attacker the ability to run arbitrary software, potentially wreaking havoc on critical systems.

To illustrate the urgency of this risk, consider the ramifications of a large-scale security breach stemming from compromised software or firmware. Such an event could not only result in substantial financial losses but also erode consumer trust in the financial institutions responsible for securing their transactions.

The SolarWinds incident serves as a stark reminder of the importance of robust cybersecurity measures and the potential risks associated with sophisticated cyberattacks. In this high-profile breach, threat actors compromised SolarWinds' Orion software, a widely used IT management and monitoring tool, enabling them to infiltrate the networks of numerous organisations, including government agencies and private companies.

This incident highlights the need for the financial services sector to remain vigilant and continuously adapt their cybersecurity strategies in the face of emerging threats. As quantum computing progresses, it has the potential to enable new types of cyberattacks that target financial institutions

and their data. Protecting against this risk requires a shift toward quantum-resistant cryptographic methods for digital signatures, ensuring that software and firmware updates remain invulnerable to the disruptive power of CRQCs. By fortifying the integrity of these updates, financial institutions can safeguard their systems' reliability and bolster consumer confidence in the face of quantum threats.

Cryptographic Risk 8: Altered financial transaction records – the private ledger

Financial transaction records held in multiple firms' internal IT systems serve as the information base for balance sheets; these, in turn, serve as the cornerstone of trust and accountability in the financial ecosystem. Safeguarding this data relies on robust encryption, both public key and symmetric. The advent of CRQCs introduces a unique and formidable threat including the potential alteration of historical data, undermining trust in financial record-keeping.

"The expert opinions we collected suggest that the quantum threat to cybersecurity will become non-negligible relatively quickly and it could well become concrete sooner than many expect."

Quantum Threat Timeline Report 2022, Global Risk Institute, December 2022

While encryption safeguards may be in place to protect these records, the prospect of an attacker with access to a CRQC presents a troubling scenario. Such an attacker could exploit the computational power of CRQCs to manipulate encrypted data, and in tampering with these records, potentially rewrite ownership of assets, create fraudulent transactions, change transaction history, and compromise the accuracy and transparency that these ledgers are designed to ensure.

Safeguarding against this risk relies on the exploration of novel cryptographic techniques that remain resilient in the face of quantum threats. Financial systems must be updated to migrate to post-quantum cryptography and become Quantum Safe.

Cryptographic Risk 9: Altered financial transaction records – the public ledger

Public asset records, preserved in ledgers like the Land Registry, serve as the basis for property ownership, mortgages and related securities.

As with private ledgers, encryption safeguards may be in place to protect these records. Similarly, to that outlined above, an attacker with access to a CRQC could manipulate encrypted data, tamper with records, rewrite ownership of assets, and create fraudulent transactions. This would compromise the accuracy and transparency of these ledgers.

The significance of these ledgers extends beyond individual financial transactions. In contexts like Land Registries where property ownership is documented, the potential fallout from compromised records could be monumental, jeopardising ownership claims and legal rights. In a similar way, public

company records, regulatory filings and other data sources could be tampered with reducing the ability for organisations to utilise these data repositories to make risk and lending decisions.

As quantum technology matures, maintaining the integrity of historical records becomes a pressing priority to sustain trust, accountability, and the overall stability of financial systems.

Why are second-order effects of cryptographic vulnerabilities important

In becoming Quantum Safe, the UK's financial services sector must also consider the consequential risks arising from cryptographic vulnerabilities being exploited.

These risks have far-reaching implications that extend beyond the immediate challenges associated with quantum computing itself. This section focuses on three key areas, or "spotlights," where these consequential risks may manifest: data breaches and privacy concerns, financial market instability and regulatory and compliance challenges.

Spotlight 1: Cryptographic data breaches and privacy concerns

As quantum computing makes progress, the integrity of current encryption methods raises questions about potential data breaches and privacy implications. The reliability of techniques that have traditionally safeguarded data security face scrutiny due to the increasing power of CRQCs.

To prevent these kind of breeches, financial institutions must reinforce their data and communication systems against the impending risk of quantum attacks in four ways:

Anticipate quantum threats: A call to action

As the quantum technology becomes more prevalent, financial institutions must prepare for an altered threat landscape. Ensuring the security and integrity of sensitive information is no longer solely about implementing traditional security measures. Rather it hinges upon adopting quantum-resistant cryptographic solutions capable of withstanding the computational supremacy of CRQCs. Firms must adopt a forward-looking approach involves reimagining data protection strategies to encompass the nuances of the quantum realm.

Safeguard sensitive information: Make it a priority

In a digital age where data breaches can have far-reaching consequences, firms cannot afford to be complacent. The ramifications of quantum attacks targeting current encryption methods could extend beyond financial losses, delving into breaches of privacy and eroded consumer trust. By embracing quantum-resistant cryptographic solutions, financial institutions can ensure the preservation of data integrity and communication privacy, underpinning the foundations of their operations, but only if they act now. Firms must prioritise their Quantum Safe programmes.

Collaboration towards quantum-resistant solutions

The battle against potential quantum vulnerabilities is not to be fought in isolation. Collaborative efforts across the financial services sector are paramount. Sharing insights, expertise, and resources can accelerate the development and implementation of quantum-resistant solutions. By rallying together, the financial institutions of the UK and its global allies can collectively forge a path towards a more secure future, mitigating data breach risks and privacy concerns posed by the evolving quantum landscape.

Managing the risk of a data breach is good business

Going beyond today's cyber controls and ensuring that an organisations' data remains safe from a data breach will require organisations to ensure that they are Quantum Safe. It is foreseeable that in future, organisations that are not Quantum Safe will not only expose themselves to unacceptable risks but will also find it increasingly difficult to meet the data security expectations of their partners and suppliers. Firms that are demonstrably Quantum Safe will have a competitive advantage over firms that do not.

Spotlight 2: Cryptographic risk and financial market instability.

The advent of quantum computing brings with it the potential for significant advancements in speed and efficiency across various industries, including the financial sector. However, these benefits may also lead to increased volatility and market instability. As we explore the implications of quantum computing on financial markets, it becomes crucial to understand the potential risks and challenges that may arise from this technological leap.

High-frequency trading (HFT) algorithms, which use powerful computers to execute trades at rapid speeds, are already a significant component of modern financial markets. With the introduction of quantum computing, these algorithms could potentially become even more powerful, accelerating the speed and complexity of trading strategies. This increased efficiency may disrupt traditional market dynamics, as quantum powered HFT algorithms outpace conventional trading systems and create new competitive pressures.

One potential consequence of such advancements in HFT is the increased risk of flash crashes or cascading effects due to the rapid execution of trades. Flash crashes are sudden, short-lived drops in market prices, often caused by high-frequency trading algorithms executing large volumes of trades in a short period. With quantum computing enabling even faster trade execution, the likelihood of these flash crashes occurring may increase, potentially resulting in greater market instability and disruptions.

Additionally, as trading strategies become more complex and interconnected due to quantum computing advancements, the potential for cascading effects (where the actions of one market participant trigger a chain reaction of events that impact other participants) could also increase. These cascading effects may lead to unforeseen consequences and heightened systemic risks within the

financial markets. By proactively addressing these challenges, the financial sector can harness the benefits of quantum computing while minimising potential disruptions and ensuring market stability.

Spotlight 3: Cryptographic regulatory and compliance challenges

The emergence of quantum computing presents various regulatory and compliance challenges for the financial services sector. As governments and regulators develop quantum strategies and impose restrictions on the export of quantum technologies, organisations must adapt to this evolving landscape and ensure their processes remain aligned with these changes. Other considerations include:

Navigating regulatory roadmaps and government restrictions

Multiple governments and regulators are creating quantum strategies to address the potential risks and opportunities posed by this emerging technology. Concurrently, some governments are restricting the export of quantum technologies to control their dissemination. Organisations must stay informed of these regulatory roadmaps and government restrictions, updating their regulatory and compliance processes accordingly.

Adapting to the evolving regulatory environment

To ensure a smooth transition to the quantum era, organisations must be able to adapt at an acceptable pace to the emerging regulatory environment relating to quantum computing. This may involve participating in sector working groups, engaging with regulators, and continuously monitoring policy changes and developments.

Revising compliance standards and regulatory frameworks

The introduction of quantum computing in the financial sector necessitates the adaptation of regulatory frameworks and compliance standards. These changes are crucial to address the new risks and potential disruptions posed by quantum computing, ensuring that financial systems remain secure, transparent, and fair.

Agility in responding to regulatory change

One of the key challenges for organisations will be the ability to react swiftly to changes in the regulatory landscape. Financial institutions must be prepared to update their policies, processes, and systems as required, and allocate adequate resources to manage the transition to quantum-safe practices.

Collaborating with stakeholders

Collaboration between financial institutions, technology providers, and regulators is essential in addressing the regulatory and compliance challenges associated with quantum computing. By working

together, stakeholders can develop consistent standards, share best practices, and promote a secure and resilient financial ecosystem in the quantum era.

Risk 2: Market stability

Quantum computing technology, once progressed through its present nascent stages, may initially see its adoption limited to those major players with substantial resources. This potential inequality in access to quantum computing resources could lead to market imbalances if large institutions or entities use their quantum-derived-derived technological advantage to maximum effect. In the medium-to-long term, this could impact competition, distort market competition and affect the proper functioning of markets if not properly managed.

Several UK headquartered Globally Systemically Important Banks have already emerged as early adopters and researchers of quantum computing, collaborating as they have with technology providers to develop quantum products and services in some cases as far back as 2017. In building dedicated research teams to formalise use cases and creating patents and real-world applications to enhance processes, these firms already have a clear first-mover advantage. it is a realistic possibility that this initial head start could result in market imbalances emerging over time as other firms race to catch up.

Fostering collaboration and shared learning could help counteract potential disparities with market distorting-effects emerging. Collaborative efforts such as sector working groups, shared research initiatives, and partnerships between financial institutions, technology providers, and regulators, could promote a more inclusive approach to quantum computing adoption. By engaging in joint projects and sharing knowledge, resources, and best practices, organisations of all sizes could benefit from advancements in quantum computing, all the while mitigating potential distortions. This may deliver a more balanced transition across the sector as a whole.

Equally, providing suppliers with access to quantum computing technology will be important. An ecosystem of technology vendors, open-source communities and research hubs has already been established within the quantum computing industry, largely ingesting and being provided quantum computing resources via the cloud. This is important; applications based on quantum computing will need both classical and quantum compute resources working together to develop and implement new applications. IBM, AWS and Azure among others offer such quantum computing machines, with consumption models similar to classical compute resources. Access to quantum machines via APIs through the cloud will allow for fair and level access to quantum computing services for potential suppliers.

At a more granular level, there are several learning and knowledge sources such as the open-source community Qiskit, a community surrounding a software development kit that allows user to build and run quantum computing algorithm. This has developed resources for IT professionals to build their skills and knowledge around quantum computing. The quantum computing community has a myriad of learning resources that spans the width of quantum computing, starting with technical education and

passing through worked examples to allow a student to build and run quantum algorithms. Part of these resources also detail specific worked examples applicable to financial services examples, including credit risk analysis, portfolio optimisation and others. The emerging community also provides hackathons, summer schools and a support network of community advocates to drive open engagement and learning. The volume and detail of learning material available for free within this and other communities ensures that the whole financial services sector has access to relevant and detailed training for them to build competencies and skills within their organisation.

Risk 3: A deficit of quantum literate skills

As the UK's financial services sector navigates the complex challenges and opportunities presented by quantum computing, one critical aspect that must be addressed is the availability of talent and expertise. Quantum technology specialists are currently in extremely short supply, and organisations must recognise the importance of attracting, developing, and retaining the skilled professionals necessary to successfully transition to quantum-safe systems.

To meet the needs of the UK financial services sector there is a need for both new skill sets and an uplift in the skill sets for existing technology professionals. Much of the needed deep quantum-related skills will likely be concentrated within a relatively limited pool, however a wider group of professionals will also be required to ensure organisations can leverage quantum computing effectively. As has been seen with other emerging technology shifts (such as cloud computing and data science), it is expected that talent joining the workforce will bring these new skills into organisations. Uplifting the skills of the existing workforce will also be critical in ensuring that financial services organisations can apply the knowledge these new professionals have.

The talent risk in the UK

Due to the nascent nature of quantum technology many concepts and techniques in flux. This dynamic environment can deter individuals from investing the time and effort required to acquire expertise. In this regard, there are some specific challenges that are faced in this area:

- **STEM education in UK:** Across the UK there is a systemic lack of STEM educated talent joining the workforce and this is a limiting factor on the scale of the talent pool which could acquire the necessary quantum computing skill sets.
- **Limited educational and training resources:** While educational resources for quantum computing are growing, there remains a shortage of comprehensive and accessible learning materials, particularly for those without an advanced background in physics.
- **Interdisciplinary nature:** Quantum computing requires expertise that spans multiple disciplines, making it challenging to find individuals with the necessary skill set. Professionals often need to bridge the gap between quantum mechanics, computer science, and mathematics.

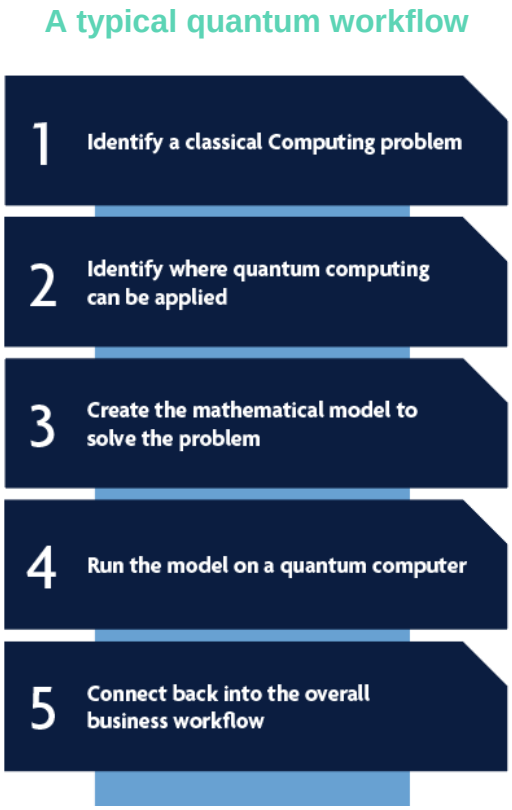

FIGURE 3*: Representative depiction of a typical workflow utilising quantum computing in-lieu of classical computing.*

As an illustration on the impact of skillsets the above illustrative workflow demonstrates how there is expected to be new requirements for skills in the workforce to utilise quantum computing:

- **Stage 1**: A task is identified which could be made more efficient if computerised.
- **Stage 2**: A fundamental understating of the types of problems that quantum can solve is required.
- **Stage 3**: A strong mathematical skillset would be required
- **Stage 4**: A quantum computer coding skillset would be required
- **Stage 5**: A good understanding of business process and architecture would be needed.

Quantum Safe skills and the expertise necessary to protect the UK's financial sector from quantum threats

In addition, the transition to Quantum Safe requires additional, and uncommon, skills.

- **Enterprise architecture:** Understanding all the systems within an enterprise that are dependent on cryptography requires familiarity with the end-to-end architecture.

- **Security engineering**: The design, implementation, testing and verification of secure systems.

- **Supply chain management**: The management of the ecosystem of software and hardware suppliers. The implementation of the CI/CD process for securely integrating software updates from internal development and from independent software vendors (ISVs).

- **Change management:** The ability to safely manage the transformation process where new disruptive technology in being introduced across the enterprise.
- **Cryptology**: Knowledge of both cryptography and cryptanalysis is necessary to evaluate the choice of cryptographic algorithms and protocols. Governance and management of the cryptographic algorithms and related supply chain.

Quantum computing skills and the expertise necessary for the UK to remain a leader in quantum technology adoption

UK Finance has also identified specific skills that are needed if the UK is to remain a leader in the adoption of quantum technology.

- **Quantum mechanics and mathematics:** An understanding of basic quantum mechanics concepts is fundamental for anyone working in quantum computing. Professionals must grasp concepts such as superposition, entanglement, quantum gates, and quantum algorithms. Additionally, strong mathematical skills are necessary to apply and analyse quantum algorithms and protocols.
- **Quantum programming:** Quantum computers require a different approach to programming compared to classical computers. Proficiency in quantum programming languages such as Qiskit, QuTiP, and Cirq is vital to translate high-level algorithms into quantum circuit representations.
- **Quantum algorithms:** Applying algorithms that leverage the unique capabilities of quantum computers requires creative thinking. Professionals in this area must possess the ability to conceptualise quantum algorithms for problems in optimisation, simulation, and machine learning.

Recommendation 2: Grow the quantum workforce

The UK Government should develop a specific strategy to develop a quantum literate workforce. This strategy should be developed in partnership with quantum technology experts and focus on all parts of the education and migration system. The UK Government should support this strategy via targeted investment in long-term workforce growth.

The UK Government's *National Quantum Strategy* identifies the need to grow a quantum-literate workforce. It does, for example, commit to engaging with UK professional bodies such as the Institution of Engineering & Technology and the Institute of Physics to develop awareness, skills and recognition of continuing professional development and careers in support of the quantum agenda. It also commits to broadening its activities to meet the growing need for non-university sourced quantum skills, aligning with wider government objectives to strengthen technical training in the UK. Finally, it also does outline specific plans to facilitate the short-term growth of the quantum workforce through measures such as growing targeted doctoral education programmes and bespoke migration routes.

These measures though welcome and necessary, do not go far enough. Growing a quantum literate workforce is a long-term objective which requires all parts of the education system – school, vocational and university – working together at all stages. More must be done to promote quantum skills at an earlier age, with specific quantum educational elements potentially incorporated into future changes in the national curriculum. More emphasis must be placed on attracting quantum-talent to the UK, and more routes available to retaining those students that have quantum-relevant education courses at UK universities. Supported these activities should specific funding designed to deliver an expanded quantum workforce over the long-term.

Risk 4: Technological debt within organisations

"Technological debt" is a concept used in business and software development to describe the long-term consequences of choosing a quick and easy solution over a more robust but time-consuming one. It's a metaphorical way of explaining how decisions made during the development or maintenance of technology systems can accumulate over time.

Preventing technology debt can be achieved through an orderly transition to Quantum Safe systems, but it requires a comprehensive understanding of an organisation's existing cryptographic landscape. Key questions to consider include:

- Which applications and business processes rely on cryptography?
- What types of cryptography are employed, such as algorithms, key lengths, protocols, and libraries?
- What key management infrastructure is in place, including certificate authorities, Public Key Infrastructure (commonly known as PKI), and hardware security modules? and
- How many instances of each component are deployed?

The recent Log4j security vulnerability highlighted the importance of maintaining a Software Bill of Materials (SBOM), an inventory of software components used within an organisation. A similar approach should be taken for cryptographic inventory, as it is equally crucial in managing the transition to Quantum Safety. The first step in this process is to conduct a discovery exercise to populate the cryptographic inventory.

In transitioning to Quantum Safe, organisations must carefully manage the deployment of new systems that have not yet been updated to incorporate post-quantum cryptography. This situation creates both risk and technical debt and must be addressed at the organisational level. By maintaining an accurate cryptographic inventory and understanding the interdependencies between various systems, organisations can prioritise updates and investments based on risk and business requirements. Furthermore, organisations should develop strategies for managing technical debt and reducing risks during the transition to Quantum Safe. This may involve working closely with technology providers to ensure they are incorporating quantum-safe solutions, continuously monitoring emerging threats, and updating internal policies and procedures to reflect the changing cryptographic landscape.

Risk 5: Ethical and environmental considerations

The future of computing will combine bits, qubits, and neurons into a compute fabric that lets us leverage each of these resources' strengths in a scalable way. The result will be a computing system capable of solving problems beyond the reach of classical computing and will create both opportunities and considerations that we must anticipate bringing about this future responsibly.

Each of those elements of that future computing system will require domain-specific expertise capable of understanding the considerations that each technology brings to that overall computing fabric. Hence, just as quantum computing will form part of the supercomputing fabric, responsible quantum forms part of the responsible computing landscape.

As the financial services sector adopts quantum computing, it is essential to consider the ethical and environmental implications of this emerging technology. By addressing these concerns proactively, organisations can ensure responsible and sustainable development and deployment of quantum computing solutions.

Responsible quantum computing considerations include making responsible choices about partners, clients and uses cases. While the full potential of quantum computing is not yet fully defined, when

scoping use cases, it should be clear that they should be designed in ways that create positive societal impact and in ways that are not in conflict with ESG considerations. Furthermore, use cases should be explored with foresight and possible unintended uses should be mitigated before deployment. Insights from and potential expectations of working with quantum computing should be communicated with scientific accuracy.

Quantum computing has the potential to enhance AI and machine-learning capabilities, which could lead to more efficient and sophisticated decision-making processes within the financial services sector. However, organisations must ensure that their quantum-powered AI systems adhere to ethical guidelines and principles, such as fairness, transparency, and accountability. This may involve implementing robust AI governance frameworks, conducting regular audits of AI systems, and addressing potential biases in data and algorithms.

Financial institutions must consider the energy efficiency of quantum computing solutions and explore ways to minimise their environmental footprint. This may involve investing in energy-efficient hardware, adopting green data centre practices, supporting research into more sustainable quantum technologies, or actively offsetting their carbon emissions. As quantum computing architecture varies between types of quantum computer energy consumption vary. Fundamentally, quantum computing is adiabatic (meaning no heat is produced from computation) so the main considerations are due to control electronics and achieving particular temperatures. The below figure details the progress made from IBM in reducing the amount of energy needed per qubit. The target per qubit for IBM being 10 milli-watts.

The scale of quantum computers that are judged to be cryptographically relevant, or relevant to achieve Quantum Advantage vary widely. This scale depends on many factors of development, examples being the efficiency of error correction and mitigation codes classical capabilities, algorithmic advancements, architectural workload considerations, hardware quality and more.[18],

[18] https://research.ibm.com/blog/error-correction-codes

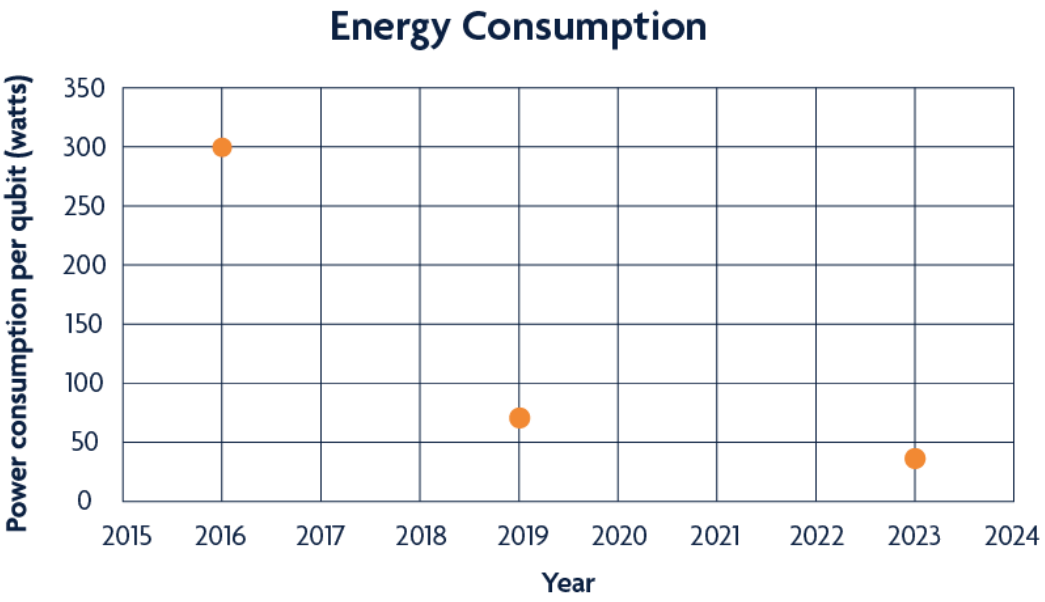

FIGURE 4*: Graph demonstrates the energy consumption required to generate a single qubit of quantum computing power between 2016-2023). Source - Quantum Computing Report* [19]

[19] https://quantumcomputingreport.com/podcast-with-oliver-dial-quantum-cto-at-ibm/

Section 3: Transitioning to Quantum Safe

Transitioning to Quantum Safe will require firms, the financial sector and regulatory bodies more widely to take practical, proactive steps to address the identified risks. As important as these steps are, however, they are only part of the picture.

Key to becoming Quantum Safe is collaboration; all parts of the sector collectively working towards clear and unambiguous objectives. Retail and wholesale banks, financial market infrastructures, asset managers, interdealer brokers, regulators and government must coordinate their efforts and develop and implement unified, coherent strategies to becoming Quantum Safe. The first step on this path is establishing a financial sector task force – potentially under the auspices of the Cross Market Operational Resilience Group (CMORG) – tasked with this purpose.

Recommendation 3: Establish a cross-sectoral Quantum Safe taskforce

The UK Government should create a financial sector task force mandated to develop and implement sector-wide Quantum Safe transformation strategies. This task force should represent all parts of the financial services ecosystem plus those critical national infrastructures on which the sector relies.

The supervisory authorities, in their role as custodians of extensive troves of sensitive and protected data, also share an inherent vulnerability to the threats covered in Section 2 of this paper. This mutual vulnerability underscores the need for regulatory bodies and oversight entities to also fortify their defences and adopt quantum safe practices. Firms and regulators stand at a juncture where they must collectively grapple with comparable challenges on the path to achieving quantum resilience.

Recommendation 4: The UK supervisory authorities must start their Quantum Safe journeys

UK financial authorities need to begin the journey of understanding of the implications of this technology for their own systems and controls. As important pillars of the financial ecosystem and holders of vast troves of sensitive market and firm data, the supervisory authorities must begin their own journeys towards becoming organisationally Quantum Safe.

Principles of a successful Quantum Safe transition plan

Transitioning to Quantum Safe will help firms secure their own integrity and contribute to a more resilient financial ecosystem. Firms will struggle achieve this outcome without a clear plan of action listing the clear, practical steps they must undertake on the journey to becoming Quantum Safe.

Necessary to designing and delivering this plan is a clear understanding of the underlying principles of any successful Quantum Safe programme. Incorporating these principles into firm Quantum Safe frameworks will be pivotal in ensuring data integrity, upholding regulatory obligations, and safeguarding client trust as quantum capabilities evolve.

Principle 1: Navigate timelines and establish priorities

The quantum risk landscape necessitates strategic timeline considerations. Financial institutions must evaluate the projected timelines for CRQC advancements and their potential impact on data security and protection against the “store now decrypt later” threat. Prioritising data types that are particularly vulnerable to quantum attacks becomes paramount. High-value financial transactions, personal identifiable information, and sensitive contractual details are examples of data that warrant immediate attention due to their potential exploitation by future quantum adversaries.

Principle 2: Take steps to prepare for the quantum future

In the face of the "store now decrypt later" threat, financial institutions must take proactive measures to fortify their data storage practices. An essential step involves the adoption of quantum-resistant encryption techniques to render stored data impervious to potential retroactive decryption by CRQCs. Regular assessments and audits of data storage systems are crucial to ensure they align with emerging quantum-safe standards.

Principle 3: Customise your Quantum Safe transition plan

While standard practices can guide the foundation of a quantum-ready strategy, customisation is key. Financial firms must consider their unique data landscape, regulatory requirements, and risk tolerance. A tailored approach allows institutions to pinpoint critical data sets, implement appropriate quantum-resistant protocols, and allocate resources efficiently.

Principle 4: Act against near-term measures

Given the inevitability of quantum advancements, firms must not delay in taking near-term action. This involves establishing cross-functional teams comprising experts in quantum technology, cryptography, and data security. Collaboratively, they can evaluate existing data storage frameworks, identify quantum vulnerabilities, and integrate robust quantum-resistant solutions that align with the institution's risk appetite.

As the financial services sector navigates the challenges and risks associated with the emergence of quantum computing, it is essential for organisations to take proactive measures to address these concerns. This section provides a series of practical steps that UK financial services organisations can follow to begin their journey towards mitigating the risks associated with quantum computing and transitioning to quantum-safe solutions. By implementing these actions, organisations can ensure a secure and resilient future in the evolving quantum landscape.

A Quantum Safe Transition plan for UK financial services firms

UK Finance recommends that financial services firms take to the following steps to transition to Quantum Safe.

Firm Action 1: Conduct a cryptographic inventory and assessment

Organisations should conduct a thorough inventory and assessment of their current cryptographic landscape. This process involves identifying the applications, business processes, and infrastructure that rely on cryptography and evaluating the specific cryptographic methods in use.

Understanding the existing cryptographic dependencies will help organisations identify potential vulnerabilities and prioritise updates based on risk and business requirements. This assessment will serve as the foundation for developing a tailored roadmap to transition to quantum-safe solutions.

Firm Action 2: Develop a quantum computing strategy and roadmap

Based on the cryptographic inventory and assessment, organisations should develop a comprehensive quantum computing strategy and roadmap. This should outline the key milestones, timelines, and resources required to transition to quantum-safe systems.

The roadmap should be tailored to the organisation's specific needs, priorities, and existing infrastructure and consider what is most important by assessing the impact risk and likelihood of compromise. By establishing a clear plan, organisations can effectively manage the transition and allocate resources efficiently, ensuring a secure and smooth migration.

Firm Action 3: Collaborate with sector partners and regulators

Firms should work collaboratively across financial institutions, technology providers, and regulators to address the challenges associated with quantum computing. By engaging in joint projects, sharing knowledge, and participating in sector working groups, organisations can stay informed of emerging developments and best practices.

Firm Action 4: Invest in Quantum-Safe technologies and solutions

Organisations should start researching and investing in quantum-safe technologies and solutions. This may involve working closely with technology providers to ensure they are incorporating quantum-resistant encryption techniques and staying informed of the latest advancements in the field.

By proactively investing in quantum-safe activities and technologies, organisations can mitigate the risks associated with quantum computing and remain competitive in the evolving landscape.

Firm Action 5: Enhance cybersecurity measures

As quantum computing progresses, new types of cyber threats targeting financial institutions and their data may emerge. Organisations need to stay vigilant and continuously adapt their cybersecurity strategies to address these emerging threats.

This may involve implementing multi-layered security measures, conducting regular security audits, and adopting a proactive approach to threat detection and response.

Firm Action 6 - Train and develop a quantum-literate workforce

The specialised nature of quantum computing may create a skill gap within the financial services sector. Organisations should invest in training and development programs to equip their workforce with the knowledge and skills necessary to effectively leverage and manage quantum computing technologies.

By fostering a culture of continuous learning and development, organisations can ensure they have the talent and expertise required to navigate the quantum era.

Firm Action 7 - Monitor regulatory changes and update compliance processes

Organisations must stay informed of regulatory changes and government restrictions related to quantum computing. By continuously monitoring policy developments and engaging with regulators, organisations can ensure their compliance processes remain aligned with the evolving landscape.

Updating internal policies and procedures to reflect the changing cryptographic landscape will help organisations maintain regulatory compliance and minimise potential disruptions during the transition to quantum-safe systems.

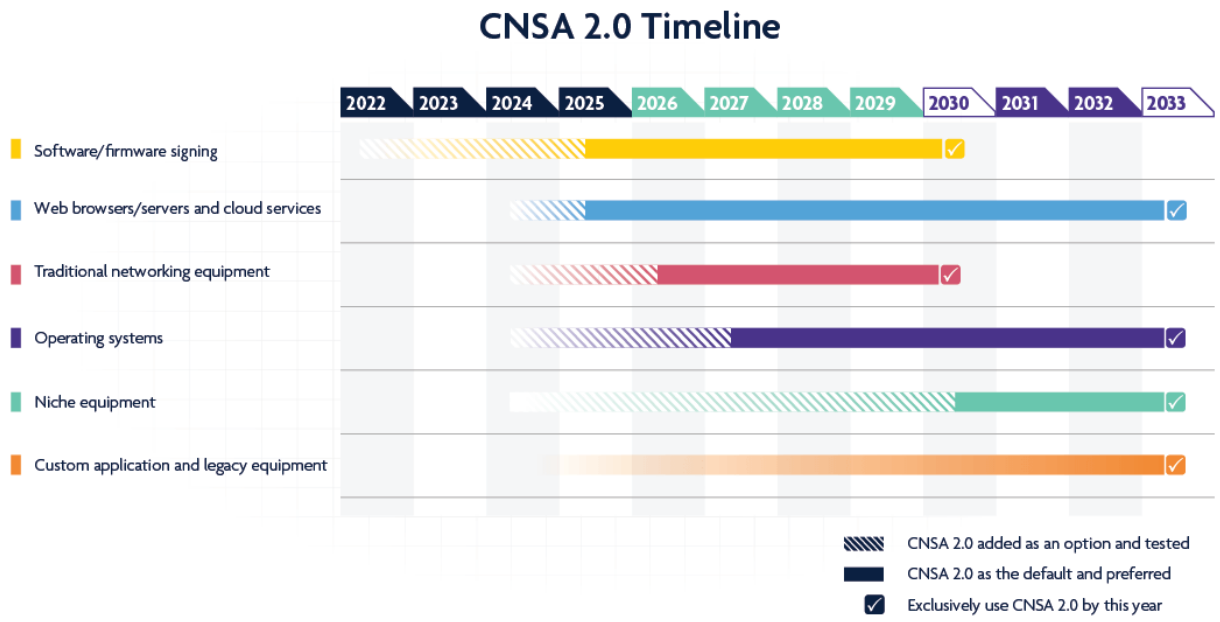

FIGURE 5: *This graphic represents the predicted timelines associated with different IT and OT systems that will require updating to become quantum safe. Source - NIST Migration Workshop*

Action Plan for the UK Financial Services Sector

In addition to the practical steps taken at the firm level, it is essential that the financial services sector collaborates and coordinates to address the challenges posed by quantum computing. The following steps outline actions that should be taken at a sectoral level following the establishment of a recognised cross-sectoral task taskforce.

Sector Action 1- Establish sector-wide roadmap, working groups and initiatives

Support the creation of sector-wide working groups and initiatives focused on quantum computing with the aim of knowledge sharing, collaborative research and the development of best practices across the financial services sector. Under the governance structure of UK Finance, these groups can bring together financial institutions, technology providers, researchers, and regulators to collectively address the challenges and opportunities presented by quantum computing. By working together, the sector should explore the feasibility of the development of a shared roadmap, consistent standards, guidelines, and quantum-safe solutions that benefit all participants.

Sector Action 2 - Engage with academic and research institutions

The financial services sector should actively engage with academic and research institutions to stay informed of the latest advancements in quantum computing and cryptography. By collaborating with researchers and experts in the field, the sector can gain valuable insights into emerging technologies, potential risks, and innovative solutions. This collaboration can also help to bridge the skill gap by fostering the development of quantum-trained professionals who can contribute to the sector's transition to quantum-safe systems. Additionally, the sector should aid the growth of the skill sets required by supporting collaboration with other initiatives such as UK Quantum, Tech UK the BCS (The Chartered Institute for IT), and the Institute of Physics, Quantum-Business Innovation and Growth.

Sector Action 3 - Advocate for supportive policies and regulatory frameworks

The financial services sector should actively participate in policy discussions and advocate for supportive regulatory frameworks for quantum technology. By engaging with policymakers and regulators, the sector can help ensure that new regulations and standards effectively address the risks and challenges associated with quantum computing while fostering innovation and growth. This collaborative approach will also help to create a more unified and well-prepared sector in the face of emerging quantum threats.

By taking these sector-level actions in conjunction with the practical steps outlined for individual organisations, the financial services sector can effectively address the challenges and risks associated with quantum computing and ensure a secure, resilient, and well-coordinated transition to Quantum Safe systems.

The need for private and public sector collaboration

The continued technological progress of quantum computing and the building momentum outside the financial services sector, in sectors such as telecommunications and the public sector, means that firms need to take on board the recommended actions from this paper to ensure they are well positioned to manage the emerging risks associated with quantum computing.

For the UK to successfully transition to PQC, it is essential that the UK Government, specifically the NCSC, work with the private sector to develop sector specific roadmaps. While there will be consistent themes and common threads throughout, sector specific nuances will make a national approach too broad to be truly effective.

Individual firms would then be responsible for producing an operationalising tailored roadmaps which adhered to the strategic guidance set out in the sector roadmap. A well-structured plan is crucial for a secure and smooth transition, addressing the key technology domains impacted and ensuring clarity for all stakeholders involved.

With a clear roadmap in place, organisations can effectively plan and manage the PQC migration. This includes allocating sufficient resources, engaging with partners, and collaborating with external stakeholders throughout the process. The roadmap should outline the key steps and milestones, as well as identify potential challenges and dependencies that may arise during the transition.

The 13 areas of critical national infrastructure:

- Chemicals
- Civil Nuclear
- Communications
- Defence
- Emergency Services
- Energy
- Government
- Health
- Space
- Finance
- Food
- Transport
- Water

For the UK's financial services sector, the roadmap should consider the unique characteristics and requirements of the sector, such as regulatory compliance, data security, and the interconnected nature of the ecosystem. It should also address the sector's reliance on legacy technologies and the potential need for significant investments in upgrading or replacing various technology solutions.

At the organisational level, each roadmap should be customised to address the specific needs, priorities, and existing infrastructure of the organisation. This may involve conducting a thorough assessment of the current cryptographic landscape, identifying critical applications and business processes that rely on cryptography, and evaluating the organisation's key management infrastructure.

Additionally, organisations should establish a strong governance structure to oversee the PQC migration process. This involves defining roles and responsibilities, setting up clear communication

channels, and ensuring that all stakeholders, both internal and external, are informed and aligned with the migration objectives and timelines. As an example, in the USA, the NSA is responsible for the security of all US Government systems.

In 2022 the NSA published a timeline for the transition to PQC for all federal systems with the goal of completing the migration by 2033. Funding for this initiative is provided by both Congress and White House executive orders. This is a good example of the type of governance required.

Given the potential consequences of falling behind other international stakeholders in the adoption of quantum computing, there is strategic risk in the UK not aligning its investments to its ambition. To retain its status as an internationally recognised financial hub, the UK must identify and address all aspects of quantum technology along with the associated opportunities and risks.

The financial services sector is a component part of the UK's critical national infrastructure. Consistent guidance, promoting standardisation across all these 13 sectors can only come from central government.

Recommendation 5: Develop targeted sectoral roadmaps

The UK Government, with strong support from the NCSC, should work with the private sector to develop sector-specific Quantum Safe roadmaps. This process should begin with the 13 areas of critical national infrastructure (including finance). Development of these roadmaps must include sector-wide groups, trade associations, regulated firms and regulators to develop a coordinated approach and define key milestones to on the journey to Quantum Safe.

Conclusion

The emergence of quantum computing presents a range of challenges and risks for the UK financial services sector. From encryption vulnerabilities and technological debt to market instability and power imbalances, organisations must proactively address these concerns to ensure a secure and resilient future in the evolving quantum landscape.

This paper has outlined the key risks associated with quantum computing, as well as practical steps that organisations and the sector can take to mitigate these risks and transition to quantum-safe solutions. By conducting comprehensive assessments of their cryptographic landscape, developing tailored strategies and roadmaps, collaborating with sector partners and regulators, investing in quantum-safe technologies, enhancing cybersecurity measures, and fostering a skilled workforce, organisations can navigate the challenges posed by quantum computing.

At the sector level, the establishment of working groups and initiatives, engagement with academic and research institutions will be key. Additionally, advocacy for supportive policies and regulatory frameworks, such as the development of a task force, will play a crucial role in ensuring a well-coordinated and secure transition to quantum-safe systems across the financial services sector.

The journey towards quantum-safe solutions will require ongoing vigilance, adaptation, and collaboration among all stakeholders within the financial services sector. By proactively addressing the risks and challenges associated with quantum computing, the UK financial services sector can harness the benefits of this revolutionary technology while safeguarding the security, stability, and integrity of the sector.

References

CNSA 2.0

Source: National Security Agency | U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

National Quantum Strategy, Department for Science, Innovation and Technology (UK Government), March 2023

Post-Quantum Cryptography, National Institute of Standards and Technology (US Government)

https://csrc.nist.gov/projects/post-quantum-cryptography

Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 February 2023, GSMA

https://www.gsma.com/newsroom/resources/post-quantum-telco-network-impact-assessment-whitepaper/

Factoring integers with sublinear resources on a superconducting quantum processor, arXiv 2212.1237

Quantum Threat Timeline Report 2022, Mosca & Piani, Global Risk Institute, Dec 2022

https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/