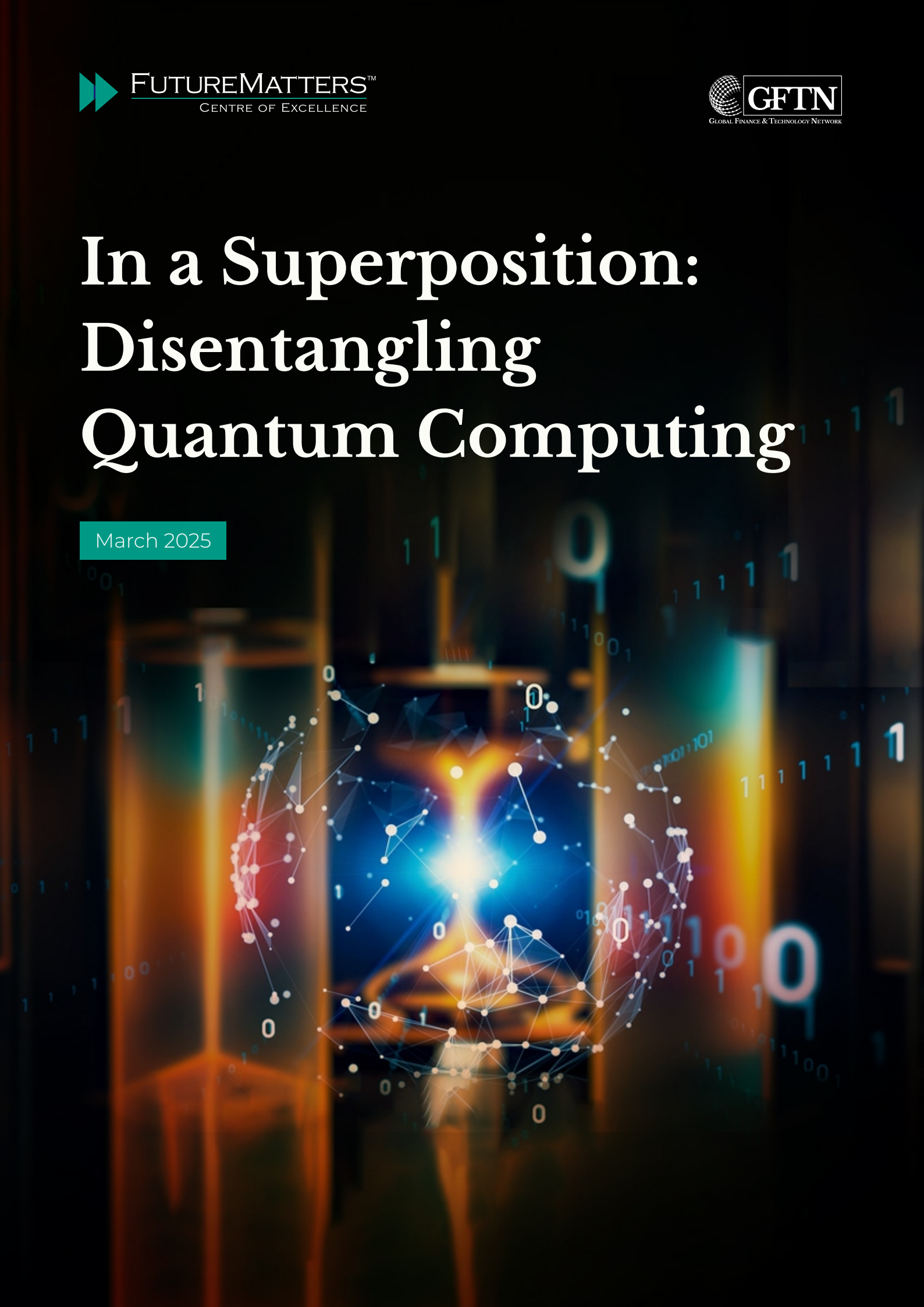
FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

In a Superposition: Disentangling Quantum Computing

March 2025



Contents

Introduction

This century has been marked by an increasing understanding of quantum mechanics, with our knowledge being continuously refined and complicated. As such, the quantum computer's potential for drug discovery, decryption and financial optimisation has gained increasing traction. With the United Nations declaring 2025 as the International Year of Quantum Science and Technology, the advent of the quantum technologies has drawn closer than many have prepared for. As the global community continues to approach the brink of quantum revolution, exciting opportunities and serious challenges have presented themselves to us. Quantum computers have evolved beyond the technological experiments locked in quantum science laboratories, they have become real, including the experimental creation of room-temperature quantum computing technologies at the Pawsey Supercomputing Research Centre in Western Australia, the radical streamlining of quantum algorithms which calculate the ground state energies of orbital electrons by Nicole Holzmann and her colleagues, and the optimism by firms in their capacity to provide useful commercial applications of quantum computers in less than a decade's time. As quantum computing continues to gain momentum in its rapid evolution, gaining progress in its abilities, the technology presents great possibilities which can further the endeavours of the global scientific and mathematical communities. However, the risks that quantum computers pose to cryptography, security and privacy, as well as financial assets cannot be ignored.

There has been great debate about the timeline that quantum technology will occupy, whether quantum computers will be a commodity within the next 5 years, or if it will take decades before a fully functioning machine is made. It is constantly too early, yet too late to react to quantum technology. Ultimately, while it is hard to predict when exactly a quantum revolution will take place, it is necessary to acknowledge the slow yet inevitable progress being made in this industry. As such, this whitepaper aims to investigate the fundamentals of quantum computing, giving an overview of the generalised risks and opportunities of quantum computing, based on insights gathered at the Insights Forum held at the Singapore Fintech Festival in November 2024. This is supplemented by specific opportunities and risks present in the finance and banking industry. Finally, this article discusses the specific preparations and preventative measures that companies can take to ensure that they are ready for a post-quantum future.

Comparison Between Classical and Quantum Computing

A key premise that should be established before further discussion on quantum computing is the difference between classical and quantum computing systems. The key difference lies in the basic information units which each model utilises. The classical computer utilises a binary digit (bit), which is the smallest unit of data that a computer can process and store. As its name suggests, a bit is always in a discrete physical state, represented by a binary value of 0 or 1. However, the quantum computer utilises quantum bits (qubits), which act similarly to a bit in terms of storage of information and are made using technologies such as superconductor rings or photons of light. This allows a system of n qubits to exist in a quantum superposition of 2^n possible states, but quantum algorithms are required to extract useful information from them efficiently. However, measuring the qubits collapses the state to a single classical result. Quantum algorithms exploit interference and entanglement to perform computations that would be infeasible for classical computers, such as factoring large numbers (Shor's algorithm) or searching databases (Grover's algorithm). Where a 2-bit register in a classical computer stores one of four configurations (00, 01, 10, 11), a qubit register in a quantum computer can store all four configurations simultaneously and continue to increase exponentially as more qubits are added.

The various other differences between the two systems of computing are extensions of this difference in their fundamental components – bits and qubits – namely, the manner in which calculations are carried out. The classical model operates under a deterministic method of calculations, where a given input will always result in the same output. Quantum computing leverages probabilistic behaviour and quantum interference to explore multiple computational pathways simultaneously. While measurement collapses the system to a single outcome, quantum algorithms are designed to amplify correct results while minimizing incorrect ones. This makes quantum computers particularly efficient in solving complex problems. A potential application of quantum computing is financial portfolio optimization, where quantum algorithms may help evaluate multiple asset combinations more efficiently than classical methods in specific cases. Moreover, quantum technology provides great opportunity for cybersecurity, keeping data encrypted for both data in transit and data at rest.

Risks to Data Security Posed by Quantum Computing

This ability for quantum computers to solve complex problems in a fraction of the time it would take for classical computing poses a particular threat to data security. A key premise that must be established is the widespread use of Rivest Shamir Adleman (RSA) cryptography in securing sensitive information across the private and public sectors. The RSA cryptography operates using an asymmetric encryption algorithm, which uses two keys, a public key, which is widely available and employed for encryption of the data, and a private key, which is employed for decryption. Both of these keys are mathematically linked and assist in ensuring that data remains confidential. This refers to data in transit, where data is securely connected between two endpoints over a network or the internet. An example of this is a credit card transaction through the SWIFT network, which must make a secure connection before data is transferred to ensure that a customer's information is kept confidential.

The threat posed by advancements in quantum technologies lies in its ability to solve classically intractable problems with greater efficiency, offering significantly greater accuracy or operational speed-ups with less energy consumption and less time. This is particularly concerning with the concept of "Harvest Now, Decrypt Later" that is prevalent amongst malicious actors who record users' data and can potentially decrypt sensitive information following potential advancements in quantum computing in the future. This has wider implications on many industries, such as in the military where communications between combat groups are conducted via the internet and must not be made vulnerable to interception and manipulation. The actionable approach that businesses can adopt is to conduct comprehensive threat models to identify vulnerabilities in their data, with particular focus on data with long-term sensitivity, such that they can proceed to decide how to quantum-proof highly sensitive data.

Applications in Finance and Banking

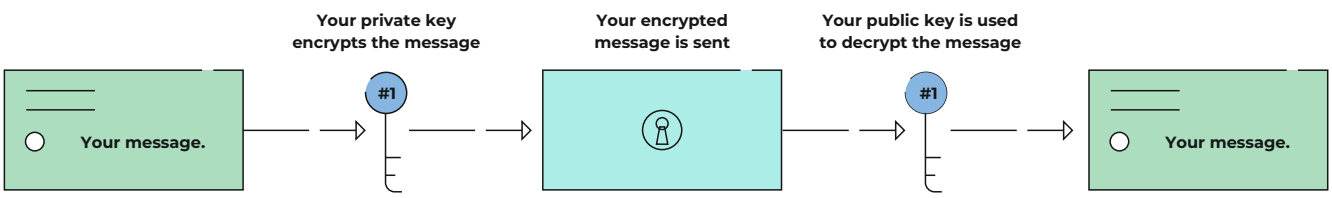
In spite of the risks associated with quantum computing, its potential to offer a computational paradigm shift cannot be ignored. The superpositions that qubits in quantum computers can inhabit enable them to outperform classical computers in performing certain computations, whether this be through providing more complex, sophisticated models or performing existing operations more efficiently. An example of such a quantum algorithm is Shor's algorithm, which can factor large prime numbers exponentially faster than classical algorithms, which has significant implications on the efficiency of various financial institutions and their operations in various fields such as portfolio optimisation, risk management or algorithmic trading. The opportunities quantum computing presents are powerful, and in the same vein, the threats it poses to the financial sector are complex and fundamental – fundamental, because standard encryption methods are embedded in every part of financial systems today, and complex because of the cryptographic elements which permeate all interconnected information technology (IT) systems used in the financial landscape.

Central Banks

In the context of central banks, quantum technologies and algorithms have major implications for monetary policy and financial stability. Quantum computing facilitates processes such as models running analyses, forecasting and the modelling of simulations which assist central banks in understanding how future growth and inflation may be affected in a fraction of the time, making models increasingly complex as well as providing a greater number of scenario analyses.

As previously mentioned, sensitive information transmitted and stored by central banks, such as financial transaction data, will be heavily compromised due to the ability of quantum technologies to decrypt classically intractable

Figure 1: Diagram of the Operation of an RSA Encryption



problems more efficiently, affecting the integrity of customers' financial data. Similar risks also extend to the prospective undertakings of Central Bank Digital Currencies (CBDC). As such, many central banks have begun to factor post-quantum tech (PQC) alongside the fulfilment of other CBDC requirements, such as scalability and vulnerability. PQC mechanisms such as Key Encapsulation Mechanism (KEM), KEMs facilitate secure key exchange, ensuring symmetric keys remain protected from quantum adversaries; and Digital Signature Algorithm (DSA), which uses asymmetric encryption to create and verify electronic signatures.

While adopting PQC in such endeavours is advisable, central banks should also acknowledge the limitations of PQC. Firstly, the integration of PQC in retail CBDC has large-scale implications on the efficiency of the CBDC. For example, many PQC mechanisms often involve larger key sizes, which may increase storage requirements and affect data transmission efficiency, depending on the algorithm used. This heavily impairs the performance of CBDC as it can lower transaction speed significantly, particularly for high-frequency, low-value transactions. Furthermore, the practical implementation of PQC poses challenges to central banks as it is a highly complex exercise, where central banks must plan and execute an order transition of its operations to PQC mechanisms. To be able to implement such mechanisms in the dense and interlinked applications that are linked to retail CBDC, such as payment platforms and financial systems, requires precise and meticulous calibration. Hence, safeguarding central banks' data from the threats of quantum technology requires more time and research, but central banks must embed PQC thinking into the design and implementation of future initiatives.

Investment

In the context of investment, the notion of investing into quantum computing is not a new notion, and there is already discussion on entering a third wave of investing into quantum computing. The impending onset of quantum technologies is validated by the increase in public money being invested in quantum computing, with 2023 being the first year that more public than private money was invested in this sector. Over 30 countries have committed to around USD$40 billion in public funds being invested into quantum technologies over the next few decades [1]. The increase in public money being invested into this sector is due to the nature of the threats that quantum computing poses, which hold significance to matters concerning technology of national security. Hence, it is crucial for investment companies to understand both the market and the technology behind quantum computing, how far it has developed and the potential advancements it may make, such that investors can make informed decisions on whether to invest or adjust their portfolios accordingly. For example, high investor enthusiasm could result in too high valuation of the quantum technology market, resulting in quantum technology companies struggling to find follow-on investments. Finally, a promising model which investment companies should take note of is quantum computing as a service, which could potentially attract a high concentration of investors in the future. This is dependent on the rapidness of the quantum technology sector's advancements, as well as the financial industry being willing and able to utilise such technology.

Cryptocurrency (Bitcoin)

This section focuses on the implications of quantum technology on cryptocurrency, with a particular reference to Bitcoin as a case study. Bitcoin utilises two cryptographic primitives: hashing and digital signatures. Bitcoin relies on two cryptographic primitives: hashing (SHA-256) for mining and proof-of-work and digital signatures (ECDSA) for transaction authentication. While Grover's algorithm could weaken SHA-256's security over time, it does not pose an immediate threat. However, Shor's algorithm poses a more serious risk to ECDSA, which could compromise transaction authenticity unless post-quantum cryptographic alternatives are adopted. Hashes can be defined as "a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus, regardless of the original amount of data or file size involved, its unique hash will always be the same".[8] Hashes are designed to be computationally irreversible and hence protect data by making it difficult for malicious actors to retrieve the original input from its hash. However, the security of hashing is threatened by algorithms which can be performed much more efficiently by quantum computers, such as Grover's algorithm, which operates by "[providing] a quadratic speedup for searching unsolved databases"[3]. In theory, a quantum computer can invert a hash much more efficiently than a classical computer. In practice, however, error correction processes in a quantum computer can impede its efficiency, which minimises quantum supremacy over classical computers.[2] In spite of this limitation, crypto-currency companies should still take preventative measures against such threats posed by quantum computers, such as doubling the size ofz symmetric keys or values being hashed.

The second cryptographic primitive used in Bitcoin is digital signatures. Digital signatures are an extension of hashing as well as asymmetric key encryption and are utilised for Bitcoin users to prove ownership over coins and allow for the transfer of these coins to other users. This is achieved by the hashed function being signed by the sender using their private key. The recipient then verifies the signature by

using the sender's public key, ensuring that the identity of the sender is validated while still protecting the private key of the sender. Bitcoin utilises the Elliptic Curve Digital Signature Algorithm (ECDSA), which similarly, can be easily overcome by algorithms which quantum computers can perform extremely efficiently such as Shor's algorithm which can solve discrete problems exponentially faster than classical algorithms".[6] It is advisable for cryptocurrency projects to transition their signature protocols to quantum-secure cryptographic protocols, to ensure that transactions remain secure, and asset ownership remains verifiable, even against future quantum attacks.

Potential Solutions to Risks

The quantum computer exists as a piece of hardware which requires assembly of qubits and storage of information in these qubits. One possible application of the quantum computer, as mentioned previously in "Risks to Data Security Posed by Quantum Computing" is to break the RSA algorithm due to its computational power which completely overrides that of a classical computer, leading to breaches in data as data in transit is no longer securely transmitted. However, companies can mitigate this potential threat even without the use of another quantum computer.

There are two main solutions that companies can adopt: firstly, software solutions, which refer to post quantum cryptography (PQC). According to the National Institute of Standards and Technology (NIST), "The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks."[10]. This migration to PQC has started to gain traction, with U.S. federal agencies expected to spend an estimated $7.1 billion by 2035 on this transition. However, the long-term efficacy of PQC still remains uncertain, with NIST detailing both primary & backup standardisations of PQC cryptographic algorithms to hedge against the uncertainty surrounding the power of quantum computers, and their ability to break PQC.

The other solution is a hybrid solution, involving the PQC and Quantum Key Distribution (QKD), which is a hardware solution. QKD requires transmitters and receivers that exchange quantum signals, generating an encryption key that is random and secure. However, the limitation of this is the hardware involved, which is largely unfeasible to implement on a wide-scale due to its design that necessitates the presence of an optic channel. As such, companies can consider implementing these solutions in tandem, utilising a blend of technologies, prioritising the hybrid solution for strategic areas which involve the transmission of particularly pertinent data.

Another consideration that companies must make is whether to adopt open source or proprietary software. This is a key step in ensuring the general security and safety of a company's data, which deals with the actions that companies can take in order to safeguard their data against quantum threat. Open-source software comes with its source code, enabling users to modify and improve it according to the terms of its license, while proprietary software belongs entirely to a company under a license. According to the National Bureau of Economic Research, more than 90% of Fortune 500 companies use open source software.[11] The popularity of open source software follows Linus' Law, the assertion that "given enough eyeballs, all bugs are shallow"[16]. The accessibility and visibility of open source software, paradoxically, makes it especially secure. This operates under the assumption and precedent that people online are much more likely to report bugs than exploit them, allowing creators to identify vulnerabilities in their software and buttress their software. An example of this is blockchain code, which operates using an open source foundation which ensures greater transparency as users can scrutinise the code which provides the system with its operational capabilities, verifying its security. It is highly recommended, therefore, for companies to adopt open source software. However, should they wish to use proprietary software, they can opt for a business source license where they retain the rights to their code while still allowing others to access the code and verify its security.

Preparations

The concept of "quantum supremacy", the point at which a quantum computer is able to outperform a classical computer, has gained traction, and it has become crucial for companies to prepare for the migration and transition into a quantum safe future. It is particularly important for companies to act now: the dangers posed by quantum computing do not lie in the distant future, they are real threats which have the potential to massively uproot various financial data security systems as we know them. To secure highly sensitive data from the malicious trend of "harvesting now, decrypting later", companies must not panic and ensure they have the suitable knowledge and people to assist in this process. Senior management should remain abreast of latest developments in quantum computing, following the advice of local regulators.

A case study to consider is Singapore, where the Monetary Authority of Singapore (MAS) published an advisory on addressing the cybersecurity risks associated with quantum in 2024, urging companies to develop strategies to address the risks posed by developments in quantum technologies[12]. This course of action ensures that companies can identify risks in a timely manner as the nascent quantum computing industry continues to mature, educating themselves on trends in this industry. The MAS has also funded sandboxes to provide financial institutions with secure environments to undergo trials with quantum security solutions, making them cognisant of quantum technology's potential to impact their existing operations. This process of experimentation and discovery of the potential impacts of implementing quantum safe technologies serves as a basis on which companies can make decisions regarding their modus operandi.

The final, and arguably most important, step for companies to take is to ensure that their staff are equipped with the relevant technical competencies and requisite skills to bolster this migration towards quantum-safe technologies. This requires partnerships with research institutions and investment from financial institutions into upskilling staff.

Conclusion

Ultimately, quantum computing has the potential to revolutionise many industries irreparably, transforming the world as we know it. It is only through staying relevant and updated with quantum technology, continuously upskilling our workforce, upgrading our existing operations, and supporting research institutions that we will be able to sufficiently prepare to not just survive in, but thrive in a post-quantum world.

Authors

Dr Andrzej Gwizdalski
Researcher, University of Western Australia & Founder, Western Australia Web3 Association

Kate Nattaya Sia
Student at St. Joseph's Institution

Contributors

Yogesh Hirdaramani
Content Manager, GFTN

Production

Sachin Kharchane
Graphic Designer

References

1. State of Quantum 2024 Report | Press releases IQM. https://www.meetiqm.com/newsroom/press-releases/state-of-quantum-report-2024
2. Vaezi A, Movaghar A, Ghodsi M, et al. Quantum Computational Complexity vs Classical Complexity: A Statistical Comprehensive Analysis of Unsolved Problems and Identification of Key Challenges. arXiv. Published online 2024.
3. Bradben. “Theory of Grover's Search Algorithm - Azure Quantum.” Learn.microsoft.com, 23 Oct. 2024, learn.microsoft.com/en-us/azure/quantum/concepts-grovers
4. Brooks, Michael. “Quantum Computers: What Are They Good For?” Nature, vol. 617, no. 7962, 24 May 2023, pp. S1–S3, www.nature.com/articles/d41586-023-01692-9, https://doi.org/10.1038/d41586-023-01692-9
5. Canorea, Elena. “Quantum Computing: Potential and Challenges Ahead.” Plain Concepts, 19 June 2024, www.plainconcepts.com/quantum-computing-potential-challenges/
6. Classiq. “Quantum Cryptography - Shor's Algorithm Explained.” Www.classiq.io, 19 July 2022, www.classiq.io/insights/shors-algorithm-explained.
7. Cobb, Michael. “RSA Algorithm (Rivest-Shamir-Adleman).” TechTarget, Nov. 2021, www.techtarget.com/searchsecurity/definition/RSA.
8. Frankenfield, Jake. “Hash Definition.” Investopedia, 2019, www.investopedia.com/terms/h/hash.asp.
9. Nili, Cameron, et al. “Safeguard CBDC Systems in the Post-Quantum Computing Age.” World Economic Forum, 21 May 2024, www.weforum.org/stories/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/
10. NIST. “Post-Quantum Cryptography | CSRC | CSRC.” CSRC | NIST, 3 Jan. 2017, csrc.nist.gov/projects/post-quantum-cryptography.
11. Open-Source Software Creators: It's not just about the money. NBER. https://www.nber.org/be/20241/open-source-software-creators-its-not-just-about-money
12. Quantum Computing Programme. “Quantum Computing Programme.” Mas.gov.sg, 2024, www.mas.gov.sg/schemes-and-initiatives/quantum-computing-programme.
13. Swayne, Matt. “White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration.” The Quantum Insider, 12 Aug. 2024, thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/. Accessed 10 Dec. 2024.
14. Tucker, Amanda. Diagram of the Operation of an RSA Encryption, 30 Sept. 2024, www.securew2.com/blog/what-is-rsa-asymmetric-encryption.
15. “What Is RSA Asymmetric Encryption? How Does It Work?” SecureW2, 30 Jan. 2024, www.securew2.com/blog/what-is-rsa-asymmetric-encryption.
16. The Cathedral and the Bazaar. O'Reilly Media; 1999.

Global Finance &
Technology Network (GFTN)

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