Deloitte.

Quantum Cyber Readiness

Deloitte's perspective on: transitioning to a quantum secure economy

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Cyber readiness in the quantum era

Organisations should start planning now to ensure their sensitive data stays secure in the quantum era.

How can the transmission of information be kept secure in the quantum age? Although quantum computers are not yet commercially available, when they do materialise and fully mature, attackers are likely to use them to break some current cryptographic systems which may cause devastating effects on how nations, businesses, and individuals keep sensitive data secure. Advancements in cybersecurity technologies designed to protect secure communications from such quantum threats, like the National Institute of Standards and Technology (NIST) activities to select and standardise fundamental quantum resistant cryptography (known as Post Quantum Cryptography) algorithms, are signals that society is becoming more aware of the pending risk.
However, it is still uncertain whether business and cyber leaders have the awareness and guidance required to assess the specific impact of the impending quantum threats on their organisations, which will allow them to move toward cryptographic agility, update to quantum resistant technologies, and keep their enterprises thriving in a post-quantum era.

This document distills some of the observations from the white paper recently published by the World Economic Forum (the Forum), in collaboration with Deloitte, that provides executive-level guidance regarding quantum risk. Through the establishment of the Forum's Quantum Security Network– a global forum consisting of businesses, academia, and international bodies– the Forum and Deloitte convened community discussions which focused on key issues and questions regarding the current state of the quantum threat and of organisations' cyber readiness. Out of these discussions, an overview of what organisations can do today to prepare for the quantum threat was developed. Some key outcomes include:

- Building awareness around the quantum threat via the education of senior business leaders
- Developing a strategy for a quantum-safe enterprise, along with a transition roadmap
- Understanding and engaging with the quantum security ecosystem
- Practicing good general cyber hygiene

Quantum readiness is a specific lens through which cyber assessments will be done – the fundamental steps of such assessments start with data classification and cryptographic discovery, and these are crucial cyber hygiene actions to undertake at any time!

The quantum threat to cybersecurity

Quantum computers are set to dramatically enhance computing capabilities, but will also create foundational risk to today's secure communications.

Physics and computer science have always been interrelated. Most notably, the invention of the semiconductor drove the first quantum revolution. We are now on the verge of the second quantum revolution. In this new era of Quantum Information Science (QIS), information will be stored and processed according to the laws of quantum mechanics. The premise of this new theory is to replace the current fundamental unit of information, the binary digit (bit), with its quantum counterpart, the quantum bit (qubit). While the classical bit can only be in one of two states (0 or 1), a qubit can be in practically any combination of 0 and 1. This property, together with other quantum mechanical properties unleashes tremendous computing power which enables solution for some specific mathematical problems that were previously intractable with classical computers. Unfortunately, such hard mathematical problems also form the foundation of some cryptography algorithms which are vital to digital security. Quantum computing could therefore severely undermine the security of our current digital society.

Cryptographic algorithms are used to preserve confidentiality, integrity, authenticity and non-repudiation of information stored in the form of data. This is crucial for securing data storage, creating secure communication channels, ensuring that data is not altered without authorization, and many other vital aspects of digital society. The security of cryptographic algorithms is based on hard mathematical problems which are assumed to be extremely difficult to solve using a classical computer, today or in the future.

The new paradigm of quantum computing proposes to solve some of the mathematical problems that form the basis of cryptographic algorithms. Using so-called "Shor's Algorithm"[1], which is designed to solve integer factorisation in discrete logarithm problems exponentially faster than using classical methods, would render some of the cryptographic algorithms used to protect data obsolete. Primarily, it is public-key, or asymmetric cryptography systems that would be vulnerable to quantum attacks by implementing Shor's Algorithm. The main challenge with public-key cryptography today is that there are currently no approved and/or standardised alternatives to replace vulnerable algorithms, although the National Institute of Standards and Technology (NIST) recently announced several candidates for standardisation[2]. Examples of how the quantum threat to public-key encryption could affect business and our daily lives include:

- Breach of sensitive health, financial, or personal data
- Interception of messages on the internet
- Lack of ability to verify the integrity of digital documents
- Challenges to the basis of cryptocurrencies

[1] Shor, P.W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th *Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press: 124–134.

[2] NIST. (2022). *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates.* https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 Global Risk

Quantum computers and the Bitcoin blockchain

A specific example of how quantum computers will impact cyber security is cryptocurrencies (and blockchain technology in general). A cryptocurrency is a decentralised system where trust is provided by cryptographic methods, instead of a central authority. As cryptography is so deeply rooted in cryptocurrencies, a quantum computer could break this trust and render the technology useless.

Quantum computers could break public-key cryptography by stealing credentials (a private key) from a blockchain address. What makes this case unique is that such an attack is only possible if the blockchain address has already been used in the past to send funds to other addresses. This nuance leads to specific attack vectors that are unique to cryptocurrencies.

At Deloitte we performed a detailed technical analysis of the Bitcoin and Ethereum blockchain to quantify the quantum risk. We found that, as of July 2022, 25% of Bitcoin and 66% of Ether are vulnerable. We also describe how the transaction process in cryptocurrencies could be broken with a quantum computer, but the resources such a quantum computer requires are much larger than what is generally needed to break cryptography algorithms.

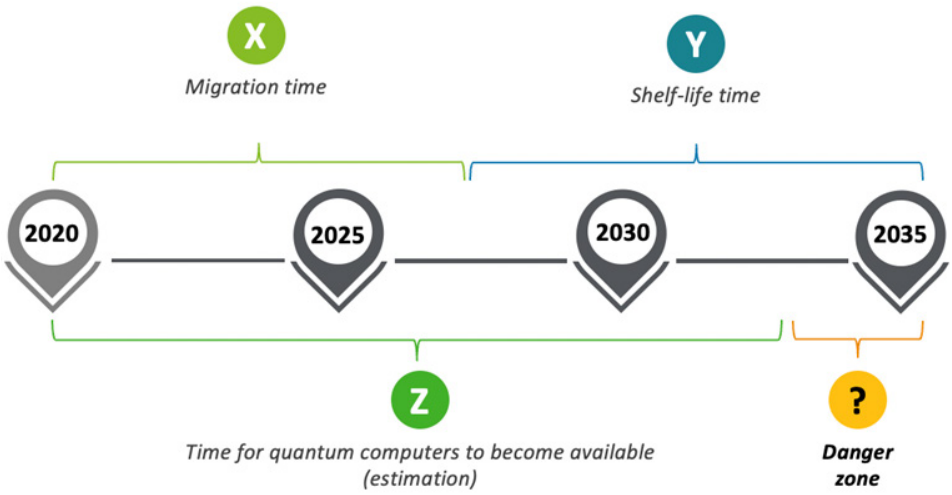
For more information about our analysis see the following links:

https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html

When will the quantum threat materialise?

Although it's hard to determine when the quantum treat will materialise due to continuous developments in the field of quantum mechanics, some leading experts polled in the *2021 Quantum Threat Timeline Report*[3] believe it could be as soon as the next 10 years. Independent from the quantum threat timeline, experts point out that businesses won't be able to transition to post-quantum cryptography (the cryptographic algorithms that will be able to withstand attacks from quantum computers) overnight. Organisations should also consider the amount of time (x) that it would take to make the quantum secure transition and the shelf-life (y) of sensitive data. These two factors often pull the threat timeline (z) forward, as illustrated by Mosca's Theorem[3] below:



In contrast to the Y2K issue, where the timeline was well understood but the impact was unknown, the impact of the quantum computing threat on public -key cryptography is well known and is immense, but the timeline is ambiguous. Further, there is a threat today based on "harvest-now, decrypt-later", whereby attackers are stealing data on the anticipation that they can decrypt it in the future. This - along with the fact that updates to cryptographic capabilities will take some considerable time – means that organisations should start carefully assessing their risk today.

[3] Institute. (2022). Quantum Threat Timeline Report. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

What technologies are available?

As the market for quantum encryption technologies continues to mature three (3) distinct categories of quantum -resistant risk solutions are emerging: 1) Post-Quantum Cryptography (PQC); 2) Quantum Random Number Generation (QRNG); and Quantum Key Distribution (QKD).

Although the quantum threat has not materialised yet, technologies are becoming available to help mitigate the risk. All of these technologies focus on mitigating the risk to public-key encryption, but in various ways. The three most mature technologies in the market today are PQC, QKD and QRNG. These three solutions tackle the challenges with public-key cryptography from different angles. At this point in time, PQC gives the most protection against Shor's Algorithm, but QKD and QRNG can be used alongside to provide safe key exchanges and produce better entropic sources (randomness).

Technology	Added benefits	Current limitations
Post-Quantum Cryptography New math-based public-key cryptography algorithms that can withstand attacks from quantum computers	• Widely considered to be the leading solution for quantum threats to encryption due to relative familiarity as an "extension" to current encryption systems • Considered to be secure against (currently-known) quantum attacks. • Software based solution can be implemented within existing infrastructure.	• All known PQC schemes (from the NIST standardisation process) have performance drawbacks, such as the required long keys and long processing time, compared to currently used algorithms which makes them unsuitable as a direct drop-in replacement. • Developments in classical and quantum attacks (cryptoanalysis) might impact the security of these schemes in the future
Quantum Key Distribution Generating secure communication channels based on quantum physics techniques, used to distribute symmetric cryptography keys	• Increased protection against harvest-now, decrypt-later attacks, as the key exchange protocol is not vulnerable to quantum attacks • Can be used in combination with other schemes to add a new layer of security • Information theoretic security, which means that no algorithms can be developed to access the exchanged keys	• Requires specialised hardware (dark fibers) and therefore require a significant investment. These dark fibers might not be required in the future • Has significant distance limitations until quantum repeaters and/or satellite QKD are developed and commercially available; secured/trusted repeaters are needed in the meantime • As opposed to classical methods where authentication is part of the protocol, a QKD link requires a separate authentication channel, which adds additional complexity to the solution
Quantum Random Number generation Using quantum properties to enhance randomness, leading to strengthened security protocols	• While classical RNGs (Random Number Generators) are derived from some source of entropy (such as thermal noise), QRNGs are inherently random • The possibility of proof of randomness (certifiable randomness) for some implementations	• Some applications require repeatability, which is not possible for QRNGs • Difficult to quantify the improvement in security

With the NIST announcement of PQC algorithm candidates for standardisation, the next stage of PQC maturity begins with NIST working through a Federal Information Processing Standard (FIPS) which will articulate algorithm configurations. Following this, it is expected that NIST will submit the FIPS documents to international standards bodies such as International Organisation for Standardisation (ISO) and Internet Engineering Task Force (IETF). Alongside this, national security organisations such as Cybersecurity and Infrastructure Security Agency (CISA - US), Federal Office for Information Security (BSI - Germany), and National Cybersecurity Agency (ANSSI - France) are issuing implementation guidance and the US National Cybersecurity Center of Excellence (NCCoE) has started an implementation project. These steps will help industry to bolster their defenses against the quantum cyber threat.

What can organisations do today?

Mitigating the quantum risk to cryptography is an enterprise-level initiative that will take time and resources. Organisations should start preparing today.

While there is some quantum threat to symmetric cryptographic algorithms, they are generally secure with the right length of cryptographic keys. The main quantum threat is to public-key cryptography based on Shor's Algorithm. Understanding the vulnerabilities of public-key cryptography is a critical step in getting ready to tackle the security threats quantum computing will impose on organizations. Cryptographic algorithms that are fundamental to digital communication and e-commerce will become vulnerable and will need to be replaced by quantum-resistant solutions.

What are the steps to consider?

In order to prepare for the implications of Shor's Algorithm, it is important to understand the current state of postquantum cryptography and know how to prepare for quantum-safe cryptographic systems, procedures, and governance. Leveraging NIST initiatives such as their development of standards and migration playbooks can be valuable. In parallel to NIST initiatives, there are steps that can be taken to help prepare organizations for a quantum transition.

- **Build awareness of the quantum threat:** Understanding the risk of quantum computers will help to educate senior leaders and gain support for investments in new infrastructure that might be needed.
- **Review cryptographic governance:** Some elements of cryptographic management may need a shift of perspective for instance, the benefits of adaptability of agile software delivery practices can also be used for a dynamic cryptographic infrastructure that is able to evolve with the enterprise and security challenges.
- **Become crypto-agile:** Following on the previous action, organisations can leverage crypto-agility to create tools to efficiently update cryptographic algorithms, parameters, and technologies when needed.
- **Engage with the quantum security ecosystem:** Building public-private and industry ecosystem relationships in order to stay up to date in technology innovation and advances in quantum computing, quantum-resistant cryptography, and crypto agility.
- **Practice good cyber hygiene:** Adopting cybersecurity leading practices and keeping sensitive data secure from threats including those posed by quantum computing

Currently, the urgency for many organisations to prioritize protective measures for threats that are seen as being so far off may be low. Corporate and cyber leaders will have to balance investments against the impact of quantum risk activities in conjunction with other priority cybersecurity initiatives.

Identifying relevant drivers

There are various organisational drivers that may be influencing a quantum transition. Once a high-level vision is set for your quantum transition, drivers should be evaluated in order to influence how your organisation might approach its transition. The following drivers are examples and do not reflect an exhaustive list, but things to consider include:

- **Quantum computer capabilities,** quantum computers will enable attacks on traditional cryptography. Meaning it is a reaction to an actual compromise, or the understanding that the threat is imminent
- **Regulatory pressures,** such as the adoption standards, or an anticipation that national or international regulators will require action
- **Market dynamics,** including drivers or activities by ecosystem parties or competitors that influence your own planning
- **Non-quantum security driven threats or pressures to manage cryptography in a more agile manner,** driven by current or emerging threats, and operational challenges

It is increasingly important that organisations prioritise their cyber remedial activities, especially in challenging economic times. Organisations need a framework that can be used to align with their various cyber activities – in line with their mission – and produce prioritisation outcomes. While quantum cyber readiness may seem like a long-term activity, it is important today to assess what steps are required, based on your organisations unique risk profile.

CONTACTS

Southern Africa

Greg Rammego
Risk Advisory Africa | Risk Advisory Africa
Mobile: +27 82 417 5889
Email: grammego@deloitte.co.za

Leishen Pillay
Risk Advisory Africa | Cyber Privacy Leader
Mobile: +27 76 827 0782
Email: lpillay@deloitte.co.za

Tiaan van Schalkwyk
Risk Advisory Africa | Senior Associate Director
Mobile: +27 83 475 3551
Email: tvanschalkwyk@deloitte.co.za

Kiran Bagratee
Senior Manager | Risk Advisory Africa
Mobile: +27 84 299 2291
Email: kibagratee@deloitte.co.za

East Africa

Urvi Patel
Risk Advisory East Africa Leader
Mobile: +254 71 405 6887
Email: ubpatel@deloitte.co.ke

West Africa

Temitope Aladenusi
Risk Advisory West Africa Leader
Mobile: +23 41 904 1730
Email: taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader
Mobile: +263 867 700 0261
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory Central Africa
Mobile: +263 867 700 0261
Email: rdean@deloitte.co.zm

Deloitte.