TOSHIBA

Building a Quantum-Secure Future

Financial Services Sector

SECURE • ADAPT • THRIVE

QUANTUM-READY NETWORKS FOR FINANCIAL EXCELLENCE

Why the Financial Services Sector needs to **Upgrade their Network Infrastructure.**

THREAT Quantum computers, able to decrypt sensitive data currently being transmitted across ordinary networks, have the potential to threaten the security underpinning today's digital economy.

RISK Sensitive data is being 'harvested' from networks vulnerable to eavesdropping so quantum computers can decrypt it at a later date. Industries whose data is both sensitive and long-lasting – such as financial services – are particularly at risk from these attacks.

ADAPT Only by transitioning to a quantum-secure network can organisations protect their data both now, and in the future.

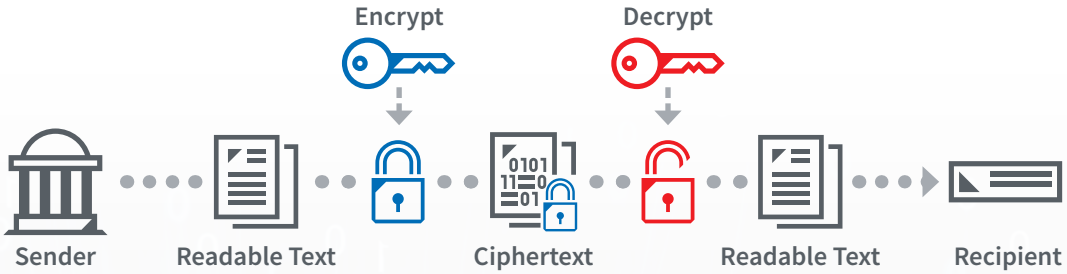
The arrival of powerful quantum computers promises to be a milestone moment, with the potential to disrupt computing as we know it. Many of the fundamental principles of cybersecurity we rely on will be undermined, threatening the security of information online.

It's a development that should be of particular concern to industries with highly sensitive and long-lasting data, who will be at a greater risk of exploitation by attackers. The only solution? Quantum secure networks, which can protect data from interception and decryption, even by quantum computers.

The adoption of these networks supports the **United Nations (UN's) Sustainable Development Goals (SDGs)** – the development of quality, reliable, sustainable, and resilient infrastructure. Quantum networks, more resilient against eavesdropping attacks, are the only method of data transmission provably secure against quantum computers.

Understanding the **Quantum Threat**

Today's digital economy is underpinned by the security of standards such as Public Key Cryptography (PKC), which has so far been successful at encrypting data against current threats. Decryption requires computations such as factoring very large numbers, which – although possible – would take a classical system a huge length of time to complete.



During the 1990s, an algorithm developed by mathematician Peter Shor was the first to demonstrate that the underlying physics of quantum computers meant they could exploit novel mathematics to perform this task many orders of magnitude faster than a classical system.

In short, he proved that quantum computers could bypass current security algorithms in mere seconds. At that point, the industry realised it would have to replace today's standards with a new generation of security designs – ones which would be resistant to quantum computers.

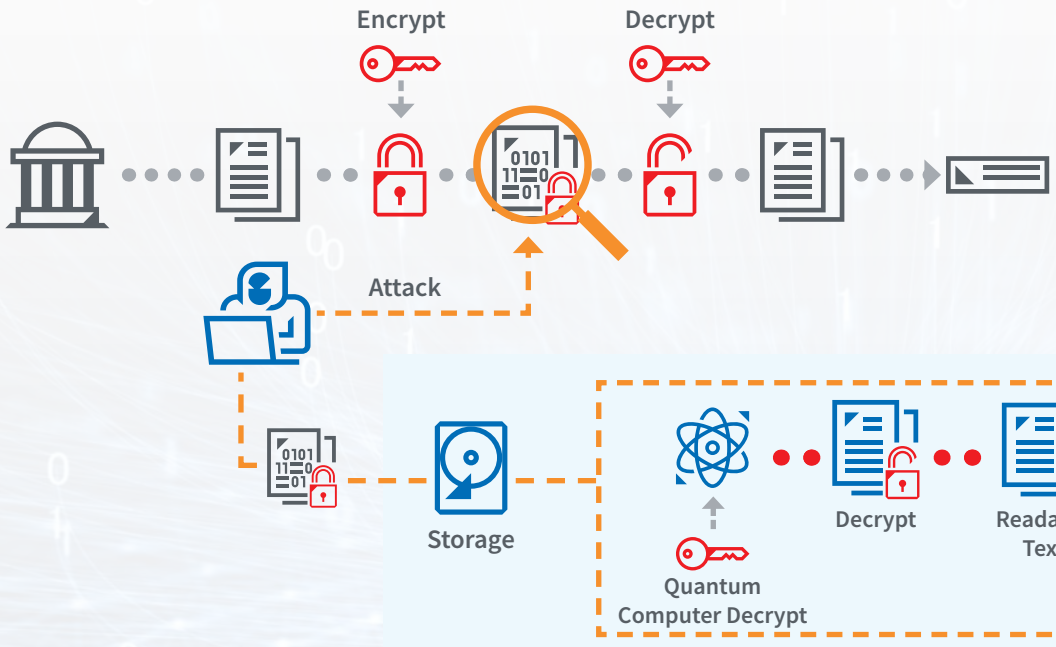
Destabilising the **Financial Sector**

> Industry experts recognize that **quantum technology** opens up new possibilities for businesses, yet it also **introduces potential risks**. This underscores the importance for organizations to approach quantum advancements with careful planning and strategic foresight.

Even though malicious actors don't have access to quantum computers today, there's widespread evidence that attackers have already begun to collect large amounts of encrypted data, storing it until a quantum computer becomes available to unlock it.

These attacks are known as harvest now, decrypt later. They're evidence that the mere potential existence of quantum computers puts today's data at risk.

Harvest now, decrypt later attacks exploit the fact that important data such as financial information or military secrets age slowly, and would therefore remain useful to an attacker for many years.



It means that the most vulnerable organisations – like banks, or government departments – are likely already being targeted, the attacks indistinguishable from other encrypted data interceptions.

The risk for organisations is not simply that the point at which quantum computers are able to break PKC is drawing near. There is also a significant threat that, when such a breakthrough is made, it might not be publicly announced. This would give the owner of the quantum computer an invisible advantage – one that the industry wouldn't know they had to protect themselves against.

COST OF DATA BREACH

ASEAN countries, *including Singapore*

US $3.05M*

Data breach in 2023

6% Increase Year-To-Year

**Average cost | Source: IBM Data Breach Report 2023*

SERVICES SECTOR SEE THE HIGHEST BREACH COSTS

Financial Services

US $4.81M

Average per breach

Energy Companies

US $3.60M

Average per breach

Source: https://futurecio.tech/cost-of-a-data-breach-hits-us3-05m-for-asean-businesses/

Even the unconfirmed possibility that this has happened could prove destabilising to the financial sector, as organisations, shareholders and regulators all scramble to find out if supposedly-secure sensitive data is really still safe.

The key defence against this uncertainty is to be proactive – and ensure that networks are protected by quantum-safe encryption well in advance of such a breakthrough being made.

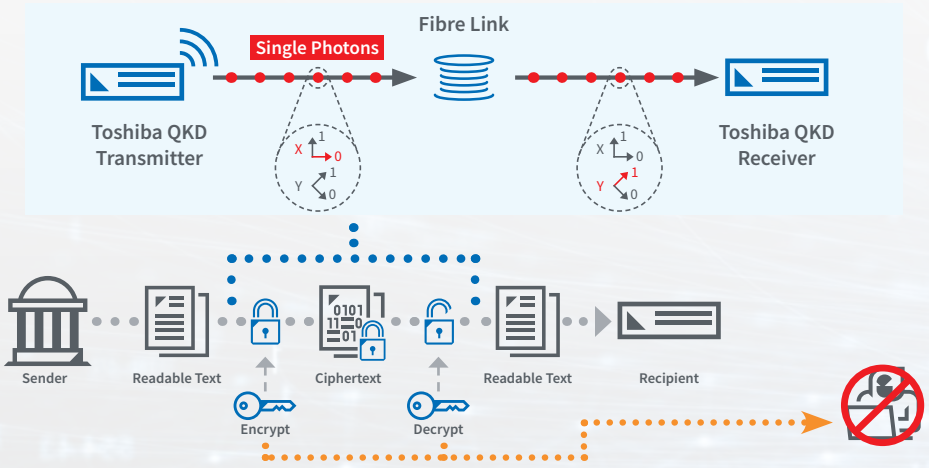
Becoming
Quantum Safe

Addressing the quantum risk requires the development of new encryption algorithms able to resist quantum computers. The resultant encryption keys must be resistant to being cracked by a quantum computer, making the data itself hard to decrypt. The keys themselves must then be distributed in a secure manner across a network, safe from eavesdropping attempts.

Quantum Key Distribution (QKD) is an example of such a quantum secure method of data transmission, and can be used today to distribute ultra-secure encryption keys – creating networks which can respond to the quantum threat digital businesses are facing.

Unlike RSA (the most common algorithm today), which utilises mathematical principles, QKD security is underpinned by fundamental physical laws. Each bit of key material is encoded using a sequence of photons in random states or qubits and, due to the nature of measuring quantum systems, any attempt to intercept these photons disturbs the encoding of their states.

This alteration reveals eavesdropping attempts, discards the current key, and restricts a new key from being successfully created until the eavesdropping stops. This makes QKD a highly-secure method of data exchange, provably secure even against quantum computers.



Quantum Key Distribution (QKD). The encoding of two photons is shown. The first shows a photon encoded in the X basis with a bit value of "0". The second shows a photon encoded in the Y basis with a bit value of "1".

Toshiba's QKD is a mature technology, the result of two decades of research. It is underpinned by proprietary technology that make it world-leading: running across longer distances than competitors, or deploying over existing fibre networks.

Toshiba QKD Products Range

The Toshiba **Multiplexed QKD System** uses an O-band quantum channel, which removes the need for dark fibre when operating on a 'lit' existing optical fibre; the **Long-Distance QKD System** uses a C-band quantum channel for the longest possible range.

The Toshiba **Quantum Key Management System (Q-KMS)** enables Quantum Secure Networks (QSN) to be easily deployed using Quantum Key Distribution (QKD) systems available today by managing key distribution in the QKD network. Q-KMS provides an abstraction from the underlying physical QKD hardware layer and helps QSN service providers implement a QKD overlay to their secure communication applications.

Key Features

- High Key Rates
- Long Range
- Data Co-existence
- Networking Technologies
- Active Stabilisation
- Ultimate Security

Why Toshiba QKD

Decades of research and unmatched expertise position Toshiba as leaders in quantum communication technology.

- Support More Users and Use Cases
- Achieve Competitive Advantage
- Reduce CAPEX
- Deploy on Existing Fibre
- Leading in R&D
- A Name You can Trust

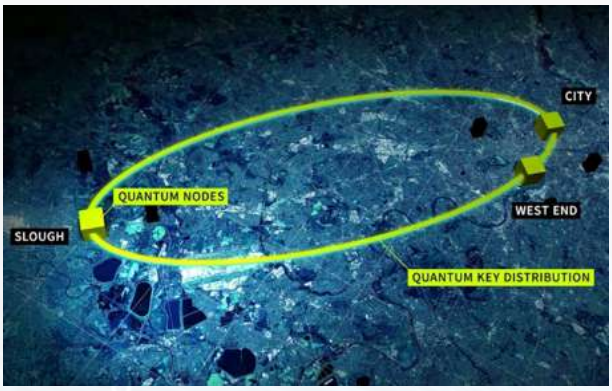
Pioneering Finance: **Top Institutions Harness Quantum Secured Networks**

Quantum Protection for AI-Powered FX Trading

HSBC processes billions of financial transactions each year for its customers, meaning the importance of securing its infrastructure from the rise of quantum is paramount.

In 2023, HSBC partnered with BT and Toshiba to become the first bank to join the London commercial quantum secure network (QSMN) to trial a real-life deployment of Quantum Key Distribution (QKD) technology. Building upon this success, HSBC, one of the world's largest FX trading providers, pioneered quantum protection for AI-powered FX trading in a world-first trial.

For the experiment, a link was established between HSBC's HQ in Canary Wharf and a data centre in Berkshire on the QSMN.



The Quantum Secure Metro Network

The QSMN itself is secured by Toshiba's Quantum Key Distribution technology, which uses the physical properties of light to prevent any unauthorised party from gaining information on the encryption keys. In the QKD protocol used in the QSMN, individual photons are transmitted across the network, delivering quantum-secure encryption keys that cannot be compromised by a quantum attack. These keys are used to encrypt and protect sensitive data.

In a world first, HSBC secured its AI Markets trading terminal using Quantum Key Distribution and safeguarded the exchange of €30 million to US dollars. AI Markets is HSBC's award-winning offering that uses the power of natural language processing (NLP) and machine learning (ML) to enhance traders' ability to analyse and interpret financial markets.

The experiment helped HSBC to better understand the practical steps involved in implementing QKD, including the underlying business processes.

Building QKD Network used to Secure Mission-Critical Blockchain Application

Permissioned blockchain networks often deal with large amounts of confidential information. While this information may be intended to be read by other parties in the network, it's critical that data confidentiality is retained while the data is in transit. Currently, the confidentiality of this data is protected through the use of standard public-key cryptographic schemes, which will not be sufficient against a quantum-capable eavesdropper in the future.

Toshiba worked with Ciena and JPMorgan Chase to conduct a joint experimental research study and demonstrated the viability of a 800 Gbps quantum-resistant QKD-secured optical channel in mission-critical, metro-scale operational environments. The joint team demonstrated the ability of the newly developed QKD network to instantly detect and defend against eavesdroppers. It also studied the impact of realistic environmental factors on the quality of the quantum channel and used a QKD-secured optical channel to deploy and secure Liink by J.P. Morgan, the world's first bank-led, production-grade, peer-to-peer blockchain network.

Quantum Cryptography for Large-Volume Financial Transaction Data

Nomura Holdings, Inc. (Nomura HD), Nomura Securities Co., Ltd. (Nomura Securities), National Institute of Information and Communications Technology (NICT), Toshiba Corporation, and NEC Corporation collaboratively examined the viability and practicality of quantum cryptography for future societal integration, focusing on stock trading operations that demand high-speed, large-volume, and low-latency data transmission.

This groundbreaking test, initiated in December 2020 and the first of its kind in Japan, evaluated the low-latency and large-volume transmission capabilities of quantum cryptography, specifically conforming to the FIX format, a standard in stock trading. The results confirmed that the throughout remains comparable to conventional systems when applying quantum cryptography, and secure, high-speed communication can be achieved even with a substantial number of stock orders without exhausting cryptographic keys. This successful trial, conducted as part of the Cross-ministerial Strategic Innovation Promotion Program.

"Photonics and Quantum Technology for Society 5.0," is anticipated to expedite the broader societal adoption of quantum cryptography across various sectors beyond finance.

Start Now: **Quantum-Secured Networks for Singapore Fintech Advancement**

Since its inception in 2021, the collaborative efforts between SpeQtral, a spin-off from the Centre for Quantum Technologies at NUS Singapore, pioneering in quantum-secure communications, and Toshiba in Singapore have been dedicated to pioneering advancements in quantum secured networks. Commencing with proofs-of-concept (POCs) in quantum communications, the partnership achieved a significant milestone by establishing the first among technical trials in Singapore for a quantum secured network. This achievement was further solidified with the launch of the Quantum Networks EXperience

Centre (QNEX), a groundbreaking platform showcasing the transformative potential of quantum technologies.

Singapore National Quantum Safe Network Plus (NQSN+)

The Infocomm Media Development Authority (IMDA) has initiated the National Quantum-Safe Network Plus (NQSN+) infrastructure to support trials of commercial technologies and assess security systems. This initiative is a key component of the Ministry for Communications and Information's Digital Connectivity Blueprint (DCB), aimed at leveraging emerging technologies such as QKD to enhance opportunities and secure digital communication infrastructure for businesses. Over the next decade, this effort aims to propel Singapore towards becoming a quantum-safe nation.

The launch of IMDA's NQSN+ marks a significant step towards realizing Singapore's vision for quantum-safe national security, bolstering the country's capabilities in this field. The collaboration between IMDA, industry partners, and government agencies underscores a commitment to building a quantum-safe nation.

As this project unfolds, Singapore fintech stands to gain substantial benefits, capitalizing on the quantum-safe infrastructure to fortify and elevate the security standards of financial transactions and communications in the nation. The collaborative endeavors exemplify a commitment to immediate action, offering tangible contributions towards the integration of quantum-safe networks and fostering a resilient future for Singapore's fintech sector.

Taking Steps
Towards Safety

Keeping data safe and secure is one of the greatest challenges posed by the rapid development of today's information technology. More and more sensitive data is stored on remote computer servers, for example in the cloud, making secure access to this data a predominant concern. Securing the transmission and retrieval relies on encryption of information sent over public networks.

By integrating QKD alongside other robust quantum security techniques, financial institutions can fortify their communication infrastructure with cutting-edge protection against today's vast array of cyber-threats, as well as those of tomorrow.

Secure our quantum future with Toshiba Quantum Key Distribution (QKD) today

To find out more about Toshiba QKD,

please visit
https://asia.toshiba.com/qkd/ or

contact us at
TAPLqkd@ml.toshiba.co.jp

References:
1) https://www.toshiba.eu/quantum/news/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network/
2) https://www.toshiba.eu/quantum/insights/hsbc-why-the-quantum-secure-metro-network-is-a-milestone-moment-for-the-financial-sector/
3)https://news.toshiba.com/press-releases/press-release-details/2022/JPMorgan-Chase-Toshiba-and-Ciena-Build-the-First-Quantum-Key-Distribution-Network-Used-to-Secure-Mission-Critical-Blockchain-Application/default.aspx
4) https://www.global.toshiba/content/dam/toshiba/ww/products-solutions/security-ict/qkd/resources/pdf/Toshiba_QKD_Blockchain_White_Paper.pdf
5)https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/22/2202-01.html
6) https://www.global.toshiba/ww/news/digitalsolution/2023/11/news-20231124-01.html
7) https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure

Committed to People, Committed to the Future.

TOSHIBA

Toshiba Asia Pacific Pte. Ltd.
20 Pasir Panjang Road, #12-25/26 Mapletree Business City, Singapore 117439 | taplqkd@ml.toshiba.co.jp
https://asia.toshiba.com/qkd/ | https://www.linkedin.com/showcase/toshiba-qt/