QUANTUM KEY DISTRIBUTION:

What is the opportunity in Finance?

The financial industry relies on being able to securely encrypt financial transactions and customers' personal data. But quantum computers may one day be able to crack current encryption, creating major risks to the integrity of the global financial system. Quantum safe approaches, including Quantum Key Distribution (QKD), will be needed to secure future communications.

Why does QKD matter to the finance sector?

Financial institutions need to protect transactions, client data and proprietary information. Private payments rely on processing card numbers, which must be encrypted to prevent identity theft. Most financial transactions, small and large, happen electronically, and rely on encryption to shield them from cyber-attacks.

All such transactions will be compromised if current encryption can be cracked by quantum computers.

The scale of the risk means that finance should start preparing soon. But even short-term, deploying quantum security will bring advantages, as it guarantees that today's data is safe from future quantum computer attacks. And it also has image benefits, assuring customers that long-term security of their data is being taken seriously.

> **"Industry must be aware of the coming threats to their security systems and the ways quantum technology can protect against them, so that organisations can make informed decisions on how best to secure their data. QKD may not be entirely practical or even necessary for another decade, but it can take a decade for a large organisation from making a decision on a new security system to the actual implementation of it."**
>
> *Quantum Technology in Finance, Knowledge Transfer Network Report*

Where are we now and where are we going?

QKD can already be delivered over private networks and has been demonstrated for securing financial transactions. A potential near-term application, where a QKD network could already be cost effective, could be for CHAPS payments.

Another application could be in two-factor transaction authentication. QKD could create multiple one-time 'passwords', which could be dispensed contactlessly to a mobile device via a 'quantum ATM'. These can verify in-person or online transactions, and are safer than passwords or PIN numbers which are frequently copied or stolen. This technology is expected to be ready for commercialisation in the next few years, but would take time to be implemented on a large scale.

QKD has already been demonstrated at chip-scale, wirelessly, and over fibre networks, paving the way for quantum secured transactions from consumer devices. These technologies may take a decade or more to realise on a practical scale, but they are coming.

WHAT IS QKD?

In conventional encryption, data is encrypted using an algorithm, making it unintelligible to anyone who steals it. The algorithm also generates a key – a long string of random numbers – which allows the intended receiver to decrypt the data. This is secure for now, but such algorithms could be cracked in future by quantum computers.

In QKD, this key is physically distributed using a sequence of photons, whose quantum state is assigned randomly to represent a 0 or a 1. The physical approach means the key cannot be cracked mathematically. It is also impossible to copy or steal the key in transit, since quantum mechanics dictates that any observation will change the quantum state – which can be detected by the receiver.

WHO'S INNOVATING IN FINANCE?

A world leading wealth management company used the move of its Swiss headquarters as an opportunity to assess long-term data protection.

The company required a fibre link between its headquarters and its Data Recovery Center. To encrypt information sent over the link, it deployed ID Quantique's encryption technology, incorporating layer 2 encryption and Quantum Key Distribution, the latter being used to ensure long term-secrecy for its most sensitive information. The first deployment was a success and the encryption platform was rolled out to other areas of the company.

How to get involved

We want the finance industry to work with The Quantum Communications Hub to shape QKD's evolution and ensure eventual commercial products meet its long-term security needs.

A number of technology partners who serve the financial industry, including BT and Toshiba, are already actively involved in QKD, but as technologies move towards commercialisation, we now need active input from end users. We invite the financial sector to talk to us about their security challenges so we can shape the commercialisation of QKD to deliver a secure future for the industry.

Those interested in being involved in these projects, receiving updates, or finding out more should contact:

enquiries@quantumcommshub.net
www.quantumcommshub.net

QUANTUM COMMUNICATIONS HUB