Unlocking quantum potential: Securing digital infrastructure

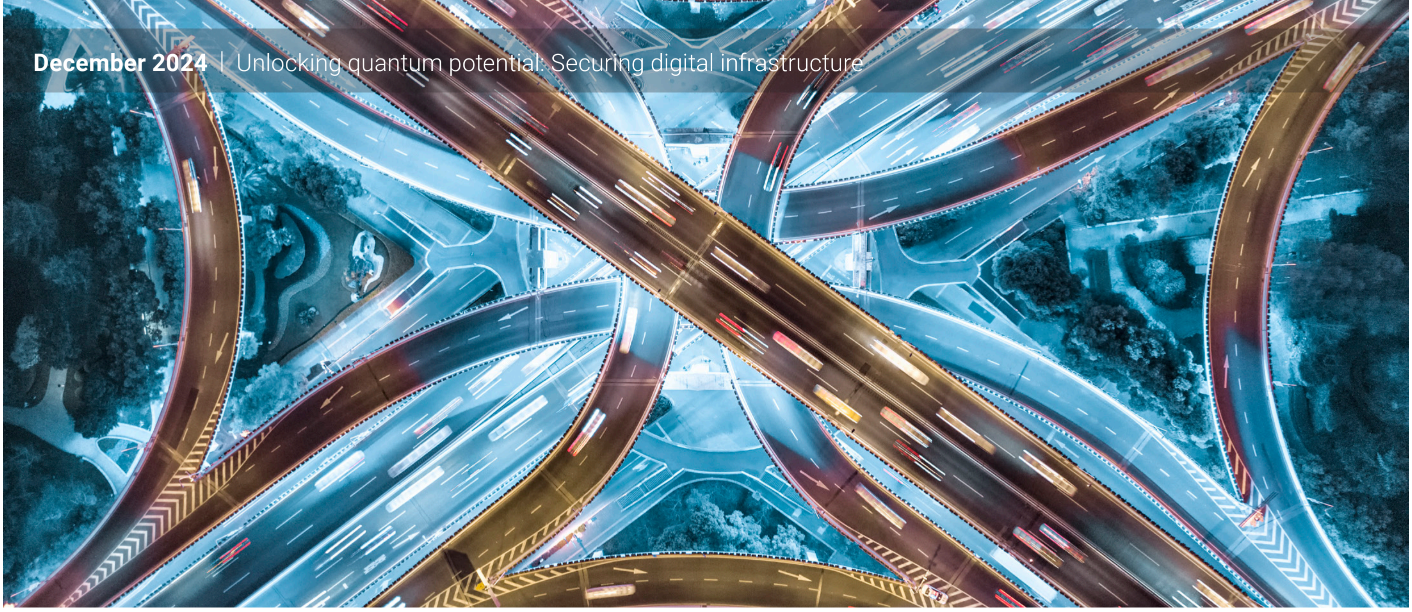
Marija Simpraga
Infrastructure Research Manager

James Tyrrell
Private Markets Research Analyst

Key points:

- The efforts to ensure data security in the quantum computing age will have significant implications for digital infrastructure investment, with an increase in quantum-secure communications potentially leading to greater demand for fibre infrastructure and an upgrade of the network
- When it comes to quantum communication technology, we think investors are likely to evaluate data-centre portfolios in terms of proximity to population centres and the relative demands of time-sensitive data operations
- Quantum-secure data centres could, in our view, see additional demand from sectors that handle highly sensitive information

Legal & General



Would it bother you if someone trawled through your private messages? Luckily, the 'classical' encryptions protecting personal data cannot be broken by traditional computers. The bad news, however, is an advanced quantum computer (QC), a type of system that leverages quantum mechanics to achieve substantially faster computing speeds, could potentially break these codes in seconds.

The rise of this technology is likely to have immense implications for national security. If you check the headlines, it's clear a quantum arms race is on, with billions invested in QCs across North America, Europe, and China[1].

Although QCs aren't yet advanced enough to break current encryptions, they're getting there. Companies like IBM are exponentially increasing their QC capabilities, and decryption could be realised in 10-15 years[2]. If data is obtained, for example by eavesdropping on our data flows, it can be stored and decrypted when the QC technology advances enough.

In our view, there are two potential solutions to this problem of our data eventually being decryptable by a QC. The first is to improve existing encryption using post-quantum cryptography (PQC), where these methods could need ongoing development as QCs improve. The second solution, called quantum key distribution (QKD), will always be secure against QCs of any size. This is because QKD can indicate if communication is intercepted between the sender and receiver. Communications, therefore, can be paused if an interception is detected, enabling them to take place only when transmission lines are fully secure and there are no eavesdroppers. Where PQC provides stronger protection against a QC cyberattack, QKD enables avoiding the attack altogether but comes with additional constraints.

	Post-quantum cryptography (PQC)	Quantum key distribution (QKD)
Description	Encryption designed to withstand cyberattacks from a QC	Encryption based on sending delicate quantum signals that enable only sending data when no eavesdroppers are present, avoiding QC attacks
Strengths	• Ability to send data long distances • Compatible with existing infrastructure (e.g., fibre optic cables)	• Fully secure data transfer • Method does not need to improve as QCs become more powerful
Weaknesses	• Developed using simulations so protection is only hypothetical against future QCs • Needs to become more sophisticated as QCs improve • Trade-off between security and efficiency[3]	• Challenging to send data at long distances using existing fibre infrastructure (> 100 km-scale) • Requires capex to integrate quantum hardware, and fibre optic cables may eventually need upgrading towards ultra-low loss

Source: LGIM research, as of June 2024

1) https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage
2) 'Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure'; Yaser Baseri, Vikas Chouhan, Ali Ghorbani; April 2024
3) Joseph, D., Misoczki, R., Manzano, M. et al. Transitioning organizations to post-quantum cryptography. Nature 605, 237–243 (2022

The main challenge with QKD is its reliance on sending delicate quantum signals[4] that quickly degrade with distance, reducing speed and range compared to current communication methods. Additionally, quantum signals cannot be copied or amplified. The only currently viable QKD method is short-range fibre optic transmission across distances ideally less than 100 km. Transmission rates exponentially decrease and are not effective at longer distances. Research is ongoing to extend transmission range[5].

QKD development has been supported by state research funding, VC funding, and company research projects across several industry sectors. Companies including EY, BT, Toshiba, HSBC and JPMorgan Chase[6] have committed capital towards commercialising QKD and have used it for quantum-secure financial transactions and video communications.

Various sectors, including defence, pharmaceuticals, healthcare, manufacturing, agriculture, and oil and gas, have also expressed interest in QKD, as highlighted by Andrew Lord, Senior Manager at BT: "I am presenting to customers weekly... in every sector, including sectors where you think, well, why would they be interested? ... All of them have their own kind of unique requirements for secrecy."[7]

4) Where a classical signal is either 0 or 1, a quantum signal can be 0 and 1 at the same time.
5) https://www.nature.com/articles/d41586-024-01445-2; https://arxiv.org/pdf/2202.07764

6) Reference to a particular company and/or the securities which it issues is on a historic basis and does not mean that the security is currently held or will be held within an LGIM portfolio. The information does not constitute a recommendation to buy or sell any security.

7) https://www.toshiba.eu/quantum/insights/toshiba-open-session-2023-chapter-4-quantum-innovations-and-collaborative-futures/

Importance of fibre and enabling technologies

While businesses may choose to invest in PQC to be able to transition to quantum-secure data exchanges, certain sectors where data security is paramount, such as financial services, will likely spearhead the deployment of the fully secure localised QKD networks in addition to PQC. Thus, the efforts to ensure data security in the quantum computing age will have significant implications for digital infrastructure investment.

Many currently available PQC solutions require extra data transfer, more computing power and have higher latency times, which is the time taken for data to travel from one point to another, compared with existing standards. This creates additional demand for digital infrastructure such as fibre networks and data centres[8].

With the current challenges in sending QKD signals with satellites, including limited transmission rates and atmospheric interference impacting the delicate quantum signals, fibre networks will likely be the backbone of quantum-secure communications, creating further demand for fibre optic infrastructure[9].

If uptake of QKD accelerates, we believe this would likely result in the expansion of fibre-based quantum-secure networks in metropolitan areas. This is because QKD processors – the technology that handles quantum signals – do not consume much power (≤500W) and have been designed to fit into data centre racks, making retrofitting of current data centres relatively straightforward. The expansion could initially see QKD processors integrated into data centres linked to current fibre networks, and then new ultra-low loss fibre networks built to maximise speed and range.

Impact of distance limitations

Given the aforementioned issues with data travelling over long distances, asset location is critical. With the transition to cloud processing and storage, secure communication lines to data centres need to have high speeds to transfer increasing amounts of data.

Edge data centres – those closest to hubs of economic activity, where most sensitive data typically is generated and consumed – will likely see increase in demand as businesses seek to ensure data integrity and high-speed secure communications. For example, inferencing large AI models requires low latency transmission, so edge data centres could see increased demand for running such models. This also means there may be a need for greater variety in the locations of data centres so that they're situated near different regional population centres.

With the lower QKD transmission rates at longer distances, remotely located data centres may concentrate their operations towards non-time-sensitive processes, for example with training new ChatGPT-like AI models. Remote data centres are primarily owned by the Big Tech hyperscalers (e.g., Microsoft, Alphabet and the like) that train those models, and training requires significant power consumption, helping to maintain demand for these facilities. Diversification between remote and edge data centres could be weighted more heavily and determined by the relative demands of time-sensitive and non-time-sensitive data operations.

With the development of quantum communication technology, we think investors are likely to evaluate their data centre positions and prospects in terms of proximity to population centres and the relative demands of time-sensitive data operations.

8) https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography
9) https://arxiv.org/pdf/2404.05668

Importance of data security

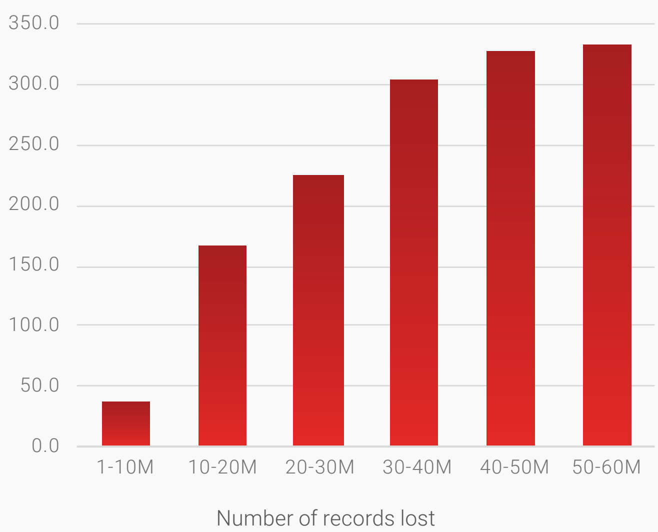
Data centre investors and developers should consider the data security requirements of end users when thinking about QKD technology.

Recognising the potential for QCs to break current encryptions, the US National Institute of Standards and Technology (NIST) has published a set of PQC encryptions designed to withstand QC cyberattacks[10]. US federal agencies will be required to use these algorithms[11], suggesting the potential for future US regulatory changes that drive the near-term corporate demand and adoption of quantum-safe solutions.

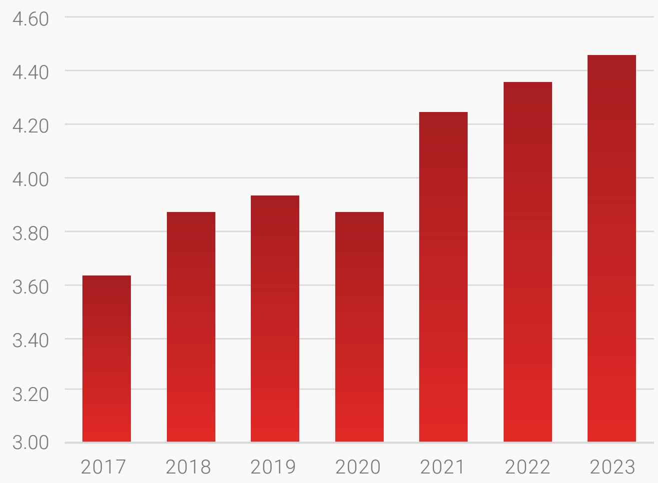
With growing costs associated with data breaches and 82% of data breaches involving data stored in cloud environments[12], data centres that already house QKD processors and are established within quantum-secure networks could, in our view, attract higher demand from companies handling highly sensitive cloud data.

For large companies handling millions of records in a public cloud, the financial costs of data breaches are significant, and could increase in the coming years. The initial cost of installing QKD technology between two users is expected to be on the $100k-scale, which is much less than the cost of an average data breach[13]. Therefore, QKD technology could enable data centres to offer quantum-secure communication as part of a specialised service, presenting opportunities for additional revenue streams.

Cost of a Mega Data Breach (USD Millions), 2023



Average Data Breach Cost (USD Millions)
(Excluding Mega Breaches)



Source: IBM, LGIM research, as of June 2024

Challenges ahead

Quantum computers could bring great benefits to society, but their arrival means ensuring the safety of data will become an ever-increasing challenge. While we expect this will increase the demand for digital assets generally, QKD's distance constraints will, in our view, likely mean that assets closest to economic hubs stand to benefit the most.

Some assets will be easier to upgrade than others. However, data centres with QKD capabilities could attract demand from data-sensitive sectors. We believe these considerations will become increasingly important for asset selection and portfolio construction in the years to come.

10) NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST, August 2024
11) US nears milestone in race to prevent quantum hacking, August 2024
12) https://www.ibm.com/reports/data-breach
13) https://www.nctatechnicalpapers.com/Paper/2021/2021-hitchhiker-s-guide-to-quantum-key-distribution/download

Assumptions, opinions, and estimates are provided for illustrative purposes only. There is no guarantee that any forecasts made will come to pass.

Contact us

For further information about LGIM, please visit lgim.com or contact your usual LGIM representative

LGIM is the global asset management business of Legal & General

Key risks

The value of an investment and any income taken from it is not guaranteed and can go down as well as up, and the investor may get back less than the original amount invested.

D009290