SLAUGHTER AND MAY/

QUANTUM COMPUTING

DIGITAL
Part of the Horizon Scanning series

The Collapse of Cryptography? Considering the quantum threat to blockchain

November 2020

In our 2019 paper *March of the Blocks* we commented on the substantial compliance hurdles that the General Data Protection Regulation (**GDPR**) presents to the ongoing development of blockchain solutions that involve storing (and transacting with) data. There, we concluded that blockchain solutions that respect the fundamental principles of data protection and privacy are achievable. But does our conclusion hold firm in light of the threat posed by quantum technology to the integrity of data recorded on a blockchain?

In this article, with help from the team at our Quantum Computing Hub, we revisit our thinking and interrogate whether quantum computers herald the end of data security in the context of blockchain solutions, or whether the reality is in fact more nuanced.

What is quantum computing?

Simply put, quantum computers are computers that make use of two laws of quantum mechanics: superposition and entanglement. They do so via quantum bits or 'qubits'. This is easiest to explain by reference to classical computers (the computers we currently use) which make use of bits, units of information which can only exist in one of two states: off or on, 0 or 1.

Because of superposition—which refers to the ability of individual units to exist in several possible states at the same time—a qubit in a quantum computer can be on, off, or on *and* off in a variety of combined states at a single point in time.

Entanglement—which describes the phenomenon whereby particles interact with each other and share their states even if separated—means that the state of a series of qubits can become linked.

These properties enable quantum computers to perform certain tasks with greater efficiency than even the most powerful classical computers. These tasks include searching through an unordered list for a specific item, identifying causal relationships, and finding the prime factors of large numbers.

Identifying the quantum threat to blockchain

A blockchain is a series of blocks of data, linked together by a cryptographic hash to form a chain. A cryptographic hash is a function that turns a block of data of any length into a fixed length output. The hash stored in each block of the chain operates like a fingerprint of the previous block, and it is possible to run a hash-checking process over the previous block to confirm that it generates the correct hash. If the previous block is changed in any

way, it will not generate the correct hash and the chain will be broken. Therefore, the data of any block in the chain cannot be modified without changing the hash of every block that comes after it in the chain.

Many blockchain solutions also deploy public-key cryptography, where both public and private keys are made up of a string of alphanumeric characters. If a user wants to send encrypted data to a recipient, it must utilise that recipient's public key (which is broadcast to the network). The sender can encrypt their data with this public key, and send the data to the recipient. Only the recipient's private key (which the recipient keeps secret) can then be used to decrypt the data. Where blockchain solutions facilitate transactions, private keys are often used to "sign" and authenticate transactions.

The fly in the ointment (and a chink in the blockchain's armour) is that many popular public-key cryptographic algorithms, including RSA encryption, are vulnerable to attack from quantum computers. This is because those cryptographic algorithms rely on mathematical calculations which break down large numbers into their prime factors (the prime numbers that, when multiplied, equal the original large number), something which is hugely time consuming for conventional computing circuits to compute. As we have already observed, this is a task that quantum computers are poised to perform with relative ease as compared to classical computers.

It has also been suggested that quantum computers increase the risk of a '51%' or 'majority' attack, whereby a bad actor seeks to take control of a majority of the nodes in a blockchain network and thereby acquires the ability to interrupt the recording of new blocks, as well as reversing records of blocks that had been completed while they were in control of the network.

What does this mean from a legal perspective?

A number of legal risks arise in a UK context, and similar obligations may well apply in other jurisdictions. In particular, the GDPR requires controllers and processors to ensure that personal data is processed in a manner that protects against unauthorised or unlawful processing and, accordingly, to implement appropriate technical and organisational security measures. Data protection should, moreover, be 'baked in' to processing activities and business practices from the design state right through the lifecycle. Should quantum computers be able to compromise data stored on a blockchain, compliance with these requirements will similarly be compromised.

Legal liability does not stop at the GDPR, however, and may vary depending on the type of entity that is storing data on a blockchain solution. For example, organisations that fall within scope of the Network and Information Security (NIS) Directive—which include operators of essential services—are subject to further requirements to manage the risks posed to the security of networks and information systems which they use in their operations.

UK financial services firms should also be mindful of proposed PRA and FCA rules to improve the operational resilience of firms, expected to be published in Q1 2021, in addition to requirements relating to appropriate systems and controls and adequate risk management systems. Senior managers within regulated firms who are responsible for data security could, moreover, come under regulatory scrutiny in the event that any data was compromised.

In addition, interference with the integrity of data recorded on a blockchain could constitute an infringement of directors' duties under the Companies Act 2006, as well as a breach of the UK Corporate Governance Code.

Appraising the quantum threat

As this survey of the legal position demonstrates, the implications of quantum computers rendering vulnerable data stored on a blockchain are significant. But, in practice, how real is this threat?

Commentators appear confident that cryptography will be able to keep pace with developments in quantum computers, which are expected to be in use by governments and companies in the 2030s. As such, current cryptographic techniques can be transitioned to cryptography that is resistant to quantum attacks (sometimes referred to as 'post-quantum cryptography'). There is, however, no proof that any of the currently recognised post-quantum methods are secure against a quantum computer.

The degree of vulnerability of incumbent blockchain systems is, moreover, subject to debate. To take one example, the blockchain solution underlying Bitcoin (which utilises a number of cryptographic techniques in addition to public-key cryptography) is considered by some to be quantum-resistant in its current incarnation, although this appears to be a minority view.

Where incumbent systems are vulnerable to quantum computers, it is certainly the case that a bad actor could steal data now and wait until advances in quantum computing enable access, irrespective of subsequent precautions put in place.

Conclusion

While the degree of the threat remains subject to debate, it is clear that quantum computing has the potential to undermine the integrity of data stored on blockchain solutions. As we have explored, this could give rise to a number of negative legal consequences, in particular under the GDPR.

Various measures can, however, be taken in order to mitigate such consequences. We have already highlighted the need to bring current cryptographic techniques up to date with post-quantum cryptography. In addition, as flagged in our *March of the Blocks* paper, the storing of personal data on a blockchain should be avoided as far as it is possible to do so.

This could potentially be achieved via middleware applications (software that sits on top of one or more underlying blockchain networks, enabling the application of those blockchain networks to particular use cases) by avoiding, for example, any free form data fields for names and contact details. These applications could also employ more advanced techniques to recognise and remove personal data from information submitted to the blockchain network.

To conclude, we remain optimistic that the GPDR and other legislation relating to data security need not stymy the development of blockchain solutions. The limitations presented by blockchain must, however, be recognised and a pragmatic approach adopted, particularly in light of the threat to data integrity posed by quantum computers.

Emily Bradley is a Financial Regulation professional support lawyer and coordinates the Quantum Computing Hub at Slaughter and May.

Emily Bradley
T +44 (0)20 7090 5212
E emily.bradley@slaughterandmay.com

Ben Kingsley is a partner in Slaughter and May and a member of the firm's Quantum Computing Hub.

Ben Kingsley
T +44 (0)20 7090 3169
E ben.kingsley@slaughterandmay.com