# Quantum computing could kill what blockchain stands for, but has a UK startup found a way to save it?

*It may be five years from now – or it could be 15 – but society, economies and the security of our digital lives are under threat from the very technology that has been positioned to save us – quantum computing.*

Temps de lecture : minute

*27 September 2021*

With global tech giants and startups aplenty racing towards a quantum future, quantum technology represents everything that's great about innovation and progression. Being able to solve complex calculations tens of millions of times faster than current computers unlocks tantalising possibilities, from eradicating disease to more acutely understanding climate change.

Drawn directly from the inner workings of nature, harnessing and simulating the power of quantum could help us identify new molecules and materials. Its capabilities could advance AI in ways we haven’t even thought of yet, to name a few benefits.

As with any significant leap, however, there comes a catch. For all the good that quantum computing promises, in the wrong hands it could pose a threat to classical computers, existing technologies and the technologies we’re pinning our hopes on for the future: namely, blockchains. *Quantum computers* could threaten the very fabric of the distributed ledger, with the ability to break everything the secure,

decentralised, transparent networks stand for.

The only way to fight this quantum threat is with quantum technology itself, and a UK startup has just taken a major step towards doing just that.

## The quantum threat

The quantum threat posed to the security of classic computers, as well as quantum computers and blockchains, isn’t new. Yet the solution to tackling this threat remains elusive.

Since 2012, academics, experts from governments and industry giants including Intel, Microsoft and Cisco have been meeting annually to discuss solutions as part of the European Telecommunications Standards Institute’s Workshop on Quantum-Safe Cryptography.

In 2016, scientists at MIT and the University of Innsbruck built a quantum computer that they claimed could – if scaled up effectively – *break RSA encryption*, an incredibly common and widely used algorithm that is used to secure almost everything from text messages to our online purchases.

This was closely followed by the launch of the National Institute of Standards and Technology's (NIST) Post-Quantum cryptography competition in early 2017, in which it called on experts to submit algorithms that are "capable of protecting sensitive information well into the foreseeable future, including the advent of quantum computers." A total of 82 initial proposals were received. As of July 2020, this has been narrowed down to 15 and it is expected that the final standard will be refined and announced by 2024.

The reason blockchains are said to be particularly at risk is because of the way they are built and what they stand for.

> *Beyond cryptocurrency, blockchains are transparent, decentralised, and offer more secure ways of storing data compared to existing, classical technologies.*

They have the power to store information about entire countries, healthcare systems, banks, businesses and so on, and have been engineered to protect these data from fraud or attack using the most advanced cybersecurity methods.

Take private enterprise blockchains for instance. When a company wants to move assets to another, they put the transaction on a block, add this block to the chain and other members of that blockchain community verify that the value and transaction are accurate. Once verified, this

transaction is locked into the chain for life. It can't be edited, it can't be removed and it means that there is always an accurate and verified way of tracking the flow of money, goods, or data from source to target.

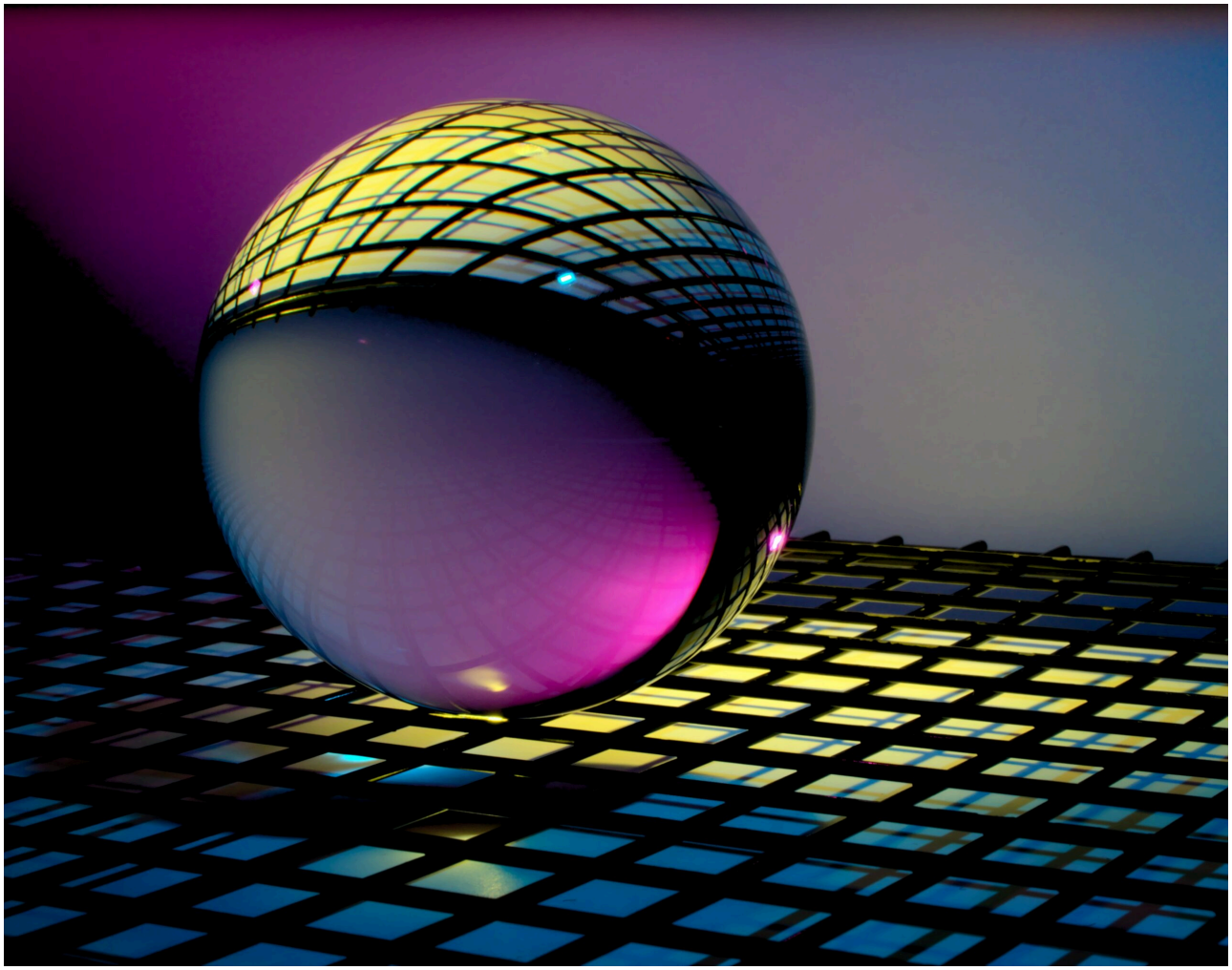
Yet, it also means that the entire history and its security is dependent on the last block placed in the chain and, given the open and transparent nature of the chain, all the blocks are freely available for criminal organisations or surveillance operatives to gather.

Right now, these criminals or operatives can't do anything with any blocks they access. Classical computers can't break the complex mathematical encryptions used to protect the blocks and in its current form, the security used to protect each of these blocks is robust and resistant to traditional cracking methods.

However, quantum computers running quantum algorithms could, and undoubtedly will, be able to in the not-to-distant future, and they will eventually be able to do so with relative ease.

When quantum computing gets cheap enough, there could be huge leaks of blockchain data. A post-quantum criminal could transmit a fraudulent block, or put a 'fork' in the chain meaning that every point forward would be based on a modified version of history. This could result in multiple versions of 'histories' that make it impossible to determine who owns valuable assets and see criminals steal what isn't theirs.

This makes blockchains a natural and potentially lucrative target for hackers and as quantum computing increases in capabilities and becomes more accessible to more people, the risk to the blockchain from hackers rises further. This means it's only a matter of time before robust quantum computers currently under development will be able to break larger and larger keys, and this could be as little as five years from now.



## Fighting quantum with quantum

One avenue being explored is to fight quantum with quantum: to prevent quantum algorithms cracking the codes by generating the encryption keys themselves using quantum physics.

Each threat area identified in blockchains, including the communication between network nodes and the integrity of digitally signed transactions, relies on cryptography and keys. It’s these keys that are vulnerable to attacks by quantum computers. To protect these areas, the generation of these keys needs to be improved and advanced, in order to ensure the security and integrity of entire blockchain networks, an improvement – and breakthrough – that was recently achieved by UK startup Cambridge

Quantum.

In collaboration with the Inter-American Development Bank (IDB) and Tecnológico de Monterrey, the Cambridge-based firm has *developed a proof-of-concept* that can be built as a post-quantum cryptography layer. The beauty of this layered solution not only means that the algorithms used by the internet or blockchain protocols can remain as they are – they don't need to be modified in order to be protected – but the layer can be placed on top of any and all existing blockchain technologies to provide quantum security.

The layer relies upon the generation of "quantum-proof" keys; keys that are generated using quantum computers and which harness the innate randomness of quantum mechanics and create keys that are unpredictable, even for advanced algorithms. For the proof-of-concept, IDB used CQs existing IronBridge platform to generate these keys and then used the keys to protect transactions and communications on the LACChain Besu blockchain network, based on Ethereum technology.

"While digital computers may produce numbers which appear to be random, they are actually just using a complicated formula to produce a series which is completely predictable and thus possibly known to an eavesdropper or adversary," Cambridge Quantum's head of cybersecurity, Duncan Jones, explains.

> *"The only way to generate truly certifiable random numbers is by using quantum physics.*

"IronBridge uses current-generation quantum computers and a process known as quantum entanglement to produce random numbers. The elegance of the solution is that it is naturally self-testing, which makes

sure every key is perfectly random. Only keys generated from certified quantum entropy can be resistant to the threat of quantum computing."

By using existing technologies, the proof-of-concept works on even the limited quantum computers that exist and without interfering with a blockchain's functionality. This represents the first time ever such a solution has been built and proven in this way, and it advances the previous, theoretical work done in this field.

It also has much further, far-reaching and vast potential because the methods used in this research can be applied to other forms of technology that rely on keys and cryptography in this way. For example, IronBridge's cloud-hosted software-as-a-service product can also be configured to work with appropriate protocols for communication systems.

Yet while a layered approach works for protecting current systems in an effective and scalable way, as Duncan continues: "In the development of this proof-of-concept, we've established that while a layered, retrofitted approach is significantly better than no quantum security, it's far more efficient for quantum cryptography to be built into the very bones of blockchain technology. All networks built from this point on must both be attuned to the threat quantum computing presents, and ready to address this threat head on, from the outset."

A point that is even more pressing in light of recent – and ongoing quantum developments – being made at pace by the likes of Google and IBM which highlight just how quickly this threat could become a reality.

Quantum computing won't destroy blockchains themselves but by threatening the security features that underpin them, they threaten all that they stand for. Fighting quantum with quantum may be the only way to preserve it.

Article by Vicky Woollaston