Quantum computers could threaten blockchain security. These new defenses might be the answer

To protect sensitive data from future quantum computers, new security protocols will be needed. This blockchain is getting ready.

By Daphne Leprince-Ringuet | August 11, 2021 -- 11:11 GMT (04:11 PDT) | Topic: Security

CQ implemented a quantum-safe security layer to LACChain that has made the system secure from future quantum computers.

Image: Shutterstock

It might be only a matter of time before quantum computers crack the cryptography keys that support sensitive data and cryptocurrencies on blockchain networks. Now quantum software company Cambridge Quantum (CQ) says it has developed a "quantum-safe" method (https://arxiv.org/abs/2106.06640) that could future-proof any blockchain by making the system invulnerable to quantum attacks.

QUANTUM COMPUTING

Quantum computers are coming. Get ready for them to change everything (https://www.zdnet.com/article/quantum-computers-are-coming-get-ready-for-them-to-change-everything/)

What is quantum computing today? The how, why, and when of a paradigm shift (https://www.zdnet.com/article/what-is-quantum-computing-understanding-the-how-why-and-when-of-quantum-computers/)

Quantum supremacy 'milestone' achieved by light-emitting quantum computer (https://www.zdnet.com/article/quantum-supremacy-milestone-achieved-by-light-emitting-quantum-computer/)

What CIOs need to know about quantum computing (free PDF) (https://www.zdnet.com/article/what-cios-need-to-know-about-quantum-computing-free-pdf/)

What classic software developers need to know about quantum computing (TechRepublic) (https://www.techrepublic.com/article/what-classic-software-developers-need-to-know-about-quantum-computing/?ftag=CMG-01-10aaa1b)

CQ partnered with the Inter-American Development Bank (IDB) and its innovation laboratory IDB Lab, which has been actively investing in blockchain technology to support social and economic applications in Latin America and the Caribbean.

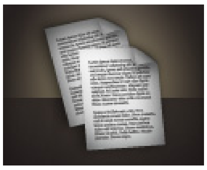
Specifically, IDB Lab has developed LACChain (https://www.lacchain.net/home), a blockchain platform leveraged by more than 50 organizations in the region for use cases ranging from cross-border e-money payments to exchanging data between different countries' customs administrations.

SEE: What is quantum computing? Everything you need to know about the strange world of quantum computers (https://www.zdnet.com/article/what-is-quantum-computing-everything-you-need-to-know-about-the-strange-world-of-quantum-computers/)

CQ implemented a quantum-safe security layer to LACChain that has made the system s [illegible] quantum computers.

To do so, CQ deployed its own commercially available platform to protect against quantum threats, called IronBridge, to LACChain.

Blockchain's vulnerability to quantum computers comes from its extensive reliance on cryptography.



The technology, also called a distributed ledger, is essentially a computational system in which information is securely logged, shared and synchronized among a network of participants. The system is dynamically updated through messages called transactions, and each participant can have a verified copy of the system's current state and of its entire transaction history.

For this type of decentralized data-sharing system to work requires strict security protocols – not only to protect the information and communications in the blockchain, which are often sensitive, but also to confirm the identity of participants, for example thanks to digital signatures.

These protocols, for now, rely on classical cryptography keys, which transform information into an unreadable mush for anyone but the intended recipients. Cryptography keys are used to encrypt data – data that can in turn only be read by someone who owns the right key to decode the message.

The strength of encryption, therefore, depends on how difficult it is for a malicious actor to decode the key; and to make life harder for hackers, security protocols currently rely on algorithms such as RSA or the digital signature algorithm to generate cryptography keys that are as complex as possible. Those keys, in principle, can only be cracked by crunching th unts of numbers.

This is why most current cryptography protocols are too hard to decode – at least with a classical computer. But quantum computers, which are expected to one day possess exponential compute power, could eventually crack all of the security keys that are generated by the most established classical algorithms.

Quantum computers are still an emergent technology, and they are nowhere near mature enough to reveal any secrets just yet (https://www.zdnet.com/article/quantum-computers-could-one-day-reveal-all-of-our-secrets/). But scientists have already identified some quantum algorithms, namely Shor's algorithm, which have the potential to eventually break existing security protocols.

SEE: Supercomputers are becoming another cloud service. Here's what it means (https://www.zdnet.com/article/supercomputers-are-becoming-another-cloud-service-heres-what-it-means/)

Alexander Lvovsky, professor at the department of physics at the University of Oxford, says that quantum computers, therefore, pose a threat to blockchain security processes like digital signatures.

"By using Shor's algorithm, a quantum attacker is able to calculate the private key of a user on the basis of their signed message, which is impossible to do with classical computers, and in this way, impersonate any party they want," Lvovsky tells ZDNet.

Quantum computers in the hands of a hacker could have dramatic consequences for the critical information that is currently stored. For example, hundreds of billions of dollars denominated in cryptocurrencies rely on blockchain ledgers, and the World Economic Forum estimates that 10% of GDP may be stored in blockchains by 2027 (http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24).

This could one day be at risk from quantum attacks. Recent analysis by Deloitte estimates that a quarter of all bitcoins could be stolen with a quantum attack (https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html), which currently represents over $40 billion.

CQ and IDB, therefore, teamed up in an effort to deploy what is known as "post-quantum cryptography" to the blockchain – a form of cryptography that is adapted to a world in which quantum computers are no longer a thing of the future.

There are various ways to address post-quantum cryptography, but all approaches e [illegible] of making cryptography keys harder to crack, even for quantum computers. To do so requires an extra dose of randomness, or entropy. A key that is generated purely randomly, indeed, is much harder to decode than one that is the product of a mathematical operation – which can be reverse-engineered by a powerful computer.

And while classical algorithms rely on mathematics, quantum computers can harness a special, non-deterministic property of quantum mechanics to generate this true randomness. CQ has leveraged this to create the IronBridge platform, which taps those quantum processes to create random numbers and make extra secure cryptography keys.

SECURITY

Kaseya ransomware attack: What you need to know (https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/)

Surfshark VPN review: It's cheap, but is it good? (https://www.zdnet.com/article/surfshark-vpn-review/)

The best browsers for privacy (https://www.zdnet.com/article/best-browser-for-privacy/)

Cyber security 101: Protect your privacy (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

The best antivirus software and apps (https://www.zdnet.com/article/best-antivirus/)

The best VPNs for business and home use (https://www.zdnet.com/article/best-vpn/)

The best security keys for 2FA (https://www.zdnet.com/article/best-security-key/)

How victims who pay the ransom encourage more attacks (ZDNet YouTube) (https://www.youtube.com/watch?v=jGqHliuqWmc)

IronBridge was successfully used in LACChain to protect communications as well as to secure digital signatures. "LACChain blockchain was an ideal target for keys generated by our IronBridge platform," says Duncan Jones, head of quantum cybersecurity at CQ. "Only keys generated from certified quantum entropy can be resistant to the threat of quantum computing."

SEE: **Bigger quantum computers, faster: This new idea could be the quickest route to real world apps** (https://www.zdnet.com/article/quantum-computing-this-new-approach-could-be-the-fastest-path-to-real-applications/#link=%7B%22role%22:%22standard%22,%22href%22:%22https://www.zdnet.com/article/quantum-computing-this-new-approach-could-be-the-fastest-path-to-real-applications/%22,%22target%22:%22%22,%22absolute%22:%22%22,%22linkText%22:%22%3Cstrong%3EBigger%

CQ deployed IronBridge as a "layer-two" service, meaning that it comes on top of the original architecture of the LACChain blockchain and could, therefore, be adapted to other systems.

Even if large-scale quantum computers are still some way off, the announcement is likely to address the concerns of blockchain users. Whether it is in five, 10 or 15 years, a quantum computer could crack the security protocols that are protecting information now – meaning that sensitive information that is currently being stored on the blockchain is still at risk from future hacking.

"The security currently used in most blockchains is vulnerable to quantum attack," Itan Barmes, quantum specialist at Deloitte, tells ZDNet. "No one knows when these attacks are going to become feasible. Estimates range between five and 30 years. On the other hand, migrating to a quantum-safe solution is also expected to take years, so ignoring the problem is taking an unnecessary risk."

Blockchain is not alone in helping to prepare for the future of cryptography. Governments around the world are also rushing to develop post-cryptography protocols, as concern mounts that information about defense and national security might one day be revealed by quantum computers.

The UK's National Cyber Security Centre has been saying for many years that reliance on classical cryptography needs to end, for example; while in the US, the National Security Agency is currently investigating a number of algorithms that could improve the resilience of cryptography keys.

HARDWARE

Lenovo's X1 Titanium Yoga is the thinnest ever ThinkPad (https://www.zdnet.com/article/lenovos-x1-titanium-yoga-is-the-thinnest-ever-thinkpad/)

Intel's flagship Rocket Lake-S processors pack a big performance boost (https://www.zdnet.com/article/intels-flagship-rocket-lake-s-processors-pack-a-big-performance-boost/)

HP updates home office line-up with Elite Dragonfly G2 and Folio headlining (https://www.zdnet.com/article/ces-2021-hp-updates-home-office-line-up-with-elite-dragonfly-g2-and-folio-headlining/)

Best security keys in 2021 (https://www.zdnet.com/article/best-security-key/)

Dell launches monitors, Latitude, OptiPlex, Precision devices aimed at work's new normal (https://www.zdnet.com/article/ces-2021-dell-launches-monitors-latitude-optiplex-precision-devices-aimed-at-works-new-normal/)