Quantum is key to securing blockchain, say researchers

June 1 2018

Credit: CC0 Public Domain

Although blockchain is traditionally seen as secure, it is vulnerable to attack from quantum computers.

Now, a team of Russian researchers has developed a solution to the quantum-era blockchain challenge, using quantum key distribution (QKD).

Writing in the journal Quantum Science and Technology, the researchers set out a quantum-safe blockchain platform that uses QKD to achieve secure authentication.

The blockchain is a distributed ledger platform that allows consensus in a large decentralized network of parties who do not trust each other. Transactions are accountable and transparent, making it useful for a variety of applications from smart contracts and finance, to manufacturing and healthcare. One of the most prominent applications of blockchains is cryptocurrencies, such as Bitcoin.

Lead author Dr. Evgeniy Kiktenko, from the Russian Quantum Center, Moscow, said: "Blockchain is promising for a wide range of applications. But current platforms rely on digital signatures, which are vulnerable to attacks by quantum computers. This also applies to the cryptographic hash functions used in preparing new blocks, meaning those with access to quantum computation would have an unfair advantage in procuring mining rewards, such as Bitcoins. These risks are significant – it is predicted that 10 percent of global GDP will be stored on blockchains or blockchain-related technology by 2025.

To overcome these risks, the researchers developed a blockchain platform combining original state-machine replication – a general method for implementing a fault-tolerant service by replicating servers and coordinating client interactions with server replicas – without use of digital signatures, and QKD for providing authentication

They then ran an experiment to test its capability in an urban QKD network.

Co-lead author Dr. Aleksey Fedorov, from the Russian Quantum Center, said: "Using QKD for blockchains may appear counterintuitive, as QKD networks rely on trust among nodes, whereas many blockchains lack such trust. More specifically, one may argue that QKD cannot be used for authentication because it requires an authenticated classical channel for operation itself.

"However, each QKD communication session generates a large amount of shared secret data, part of which can be used for authentication in subsequent sessions. Therefore, a small amount of 'seed' secret key that the parties share before their first QKD session ensures their secure authentication for all future communication. This means QKD can be used in lieu of classical digital signatures."

In addition to using QKD for authentication, the researchers redefined the protocol of adding new blocks in a different way from modern cryptocurrencies. Rather than concentrating the development of new blocks in the hands of individual miners, they employed the information-theoretically secure broadcast protocol, where all nodes reach an agreement about a new block on equal terms.

Co-lead author Prof. Alexander Lvovsky said: "A crucial advantage of our blockchain protocol is its ability to maintain transparency and integrity of transactions against attacks with quantum algorithms. Our results therefore open up possibilities for realising scalable quantum-safe blockchain platforms. If realised, such a blockchain platform can limit economic and social risks from imminent breakthroughs in quantum computation technology."

More information: E O Kiktenko et al. Quantum-secured blockchain, *Quantum Science and Technology* (2018). DOI: 10.1088/2058-9565/aabc6b

Provided by ResearchSEA

Citation: Quantum is key to securing blockchain, say researchers (2018, June 1) retrieved 18 April 2024 from https://phys.org/news/2018-06-quantum-key-blockchain.html