Quantum computers threaten Blockchain security

Encryption tools and cryptocurrencies will flounder within a decade unless they integrate quantum cryptography and communications technologies, warn A.K. Fedorov, E.O. Kiktenko and A.I. Lvovsky

[Please change references to "the Blockchain" to refer to "blockchain", "blockchains" or "a blockchain" as appropriate.]

When "information is money", data security, transparency and accountability are crucial. The Blockchain is a digital tool based on cryptography techniques that protects information from unauthorized changes. It lies at the root of the Bitcoin cryptocurrency [1]. Blockchain-related products are also used everywhere from finance to manufacturing and healthcare in a market currently worth over 150 billion USD.

The Blockchain is a secure digital record or ledger. It is maintained by users around the globe, rather than a central administration. Decisions, such as whether to add an entry (or block), are based on consensus – so personal trust doesn't come into it. A network of computer centres performs powerful calculations to verify entries and assign a unique number, or hash, to blocks. Any party, inside or outside the network, is able to check the integrity of the ledger by means of a simple calculation.

By 2025, analysts predict that up to ten percent of global GDP will be stored on blockchains [2]. Yet another forthcoming technical advance threatens this development --- quantum computers will be able to break Blockchain's cryptographic codes. Here we highlight how quantum technology, on the one hand, makes blockchains vulnerable, and on the other, can help make them more secure.

One-way codes

Blockchain security relies on 'one-way' mathematical functions. These are straightforward to run on a conventional computer but difficult to calculate in reverse. For example, multiplying two large prime numbers is easy, but finding the prime factors of a given product is hard.

Such functions are used to generate digital signatures that blockchain users cite to authenticate themselves to others**.** These are easy to check but extremely hard to forge. One-way functions are also used to validate the history of transactions in the blockchain ledger. The hash, a short sequence of bits, is derived from a combination of the existing ledger and the block that is to be added; this alters whenever contents are changed. Again, it is relatively easy to find the hash of a

block (to process information to add a record) but difficult to pick a block that would yield a specific hash value (reversing the process to derive the information that generated the hash).

Bitcoin also requires that the hash meets a mathematical condition. Anyone who wishes to add a block to the ledger must keep their computer running a random search until the condition is reached. This process slows the addition of blocks to the network, giving time for everything to be recorded and checked by everyone. It also prevents any individual from monopolizing the administration of the network, because anyone with sufficient computational power can contribute blocks.

Yet within a decade, quantum computers will be able to calculate one-way functions currently used to secure the internet and financial transactions, including blockchains. Widely deployed one-way encryption will instantly become obsolete. There are many precedents of such "mass extinction" event in information security. One of the examples is the breaking of the Enigma ciphering system, which enabled the western Allies in World War II to read substantial amounts of communications of the Axis powers that had been enciphered using this machine. The Allies not only created a machine for cryptanalysis of the Enigma, but also had a strategic advantage because Nazi Germany wasn't aware about the fact of breaking the Enigma. A more recent example is the breaking of the then-state-of-the-art Data Encryption Standard (DES) in early 2000, which gave rise to a competition in 2001 for a new cryptographic standard, which became today's Advanced Encryption Standard (AES).

Quantum challenge

Quantum computers take advantage of physical effects like superpositions of states and entanglement to perform computational tasks. To date, they are still much less powerful than conventional computers. But within a few years quantum devices will emerge that are capable of outperforming computers on certain tasks. Breaking security protocols based on cryptographic algorithms is one of them, as mathematician Peter Shor pointed out in 1994. The Blockchain is at particular risk because one-way functions are their only line of defence. Bank clients are protected by plastic cards, security questions, ID checks and human tellers, blockchain users only by their digital signature.

Cracking digital signatures is the most imminent threat. A wrongdoer equipped with a quantum computer could use Shor's algorithm to forge any digital signature, impersonate that user and appropriate their digital assets. While most experts believe that performing this feat would

require a large-scale universal quantum computer (one capable of performing a wide variety of calculations rather than a few), which is at least a decade away, some researchers suggest that this could happen sooner using emerging quantum computational devices with more limited capabilities [4]. It is also a subject of ongoing research by quantum computing companies, such as Zapata Computing Inc. and D-Wave Inc.

Quantum computers will also find solutions much faster, enabling a few users with them to censor transactions and monopolize Bitcoin mining. These parties would be able to sabotage transactions, enabling them to thwart legitimate business, or prevent their own from being recorded in the blockchain, enabling them to double-spend. Realistic scenarios for such attacks were considered in recent research reports from Singapore, Austria, France, and the United Kingdom [3].

If nothing is done to update the protocols, cryptocurrencies will crash once quantum computers become available. Fortunately, quantum technologies also offer two opportunities to enhance the security and performance of blockchains.

Quantum-enhanced Blockchains

1. Quantum-safe Blockchains

Quantum cryptography can strengthen blockchain security. Quantum communication is inherently authenticated --- no user can impersonate another. Such technologies use states of individual particles of light (photons) to encode bits and communicate them. Fundamental physics stipulates that quantum states cannot be copied or measured without being altered. Any eavesdropper will be immediately uncovered.

Quantum cryptography can be used to replace classical digital signatures and to encrypt all peer-to-peer communications in the blockchain network. In 2017**,** our group demonstrated a simple system like this in Moscow [5]. However, the complexity and cost of quantum cryptography networks will limit their adoption. It would appear that, in order this approach to be safe in the framework of blockchains, all nodes must be connected in a pairwise fashion, as there is no trust in any particular node and hence all communications must be direct. This is different from how it works currently in the Internet, where communications are secured by one-way cryptography methods and routed through multiple intermediate nodes. However, the recently developed device-independent quantum communication protocols allow untrusted intermediary quantum stations to relay quantum secured signals between two parties. If we

find ways to apply these protocols to blockchains, this will greatly simplify the quantum network architecture and make it accessible to consumers.

Photon losses in optical fibers are another challenge. These limit the range of modern quantum key distribution systems to a few tens of kilometres. The solution is to develop a quantum repeater, which uses quantum teleportation and quantum optical memory to distribute quantum entangled states between the communicating parties. Research is progressing but far from delivering a practical device.

In the interim, one-way functions could be tightened. Some have been proposed that are equally hard to reverse with both classical and quantum computers. Although not completely secure, these could be run on existing hardware and would buy time. However in the long run they too would be deciphered.

2. Quantum Internet for blockchains

Running Blockchain processes on quantum networks would address both the security issue and enable blockchains to become faster and more efficient. This step requires a “quantum Internet" [7], connecting quantum computers across a quantum communications network. It would then become possible to run fully quantum blockchains. These would bypass some computationally-intensive steps of the current verification and consensus processes and thus be more efficient and more secure, as it was shown in a series of preprints by researchers from Sweden, Israel and Russia. The Quantum Bitcoin currency could be realized, with its security assured by the no-cloning theorem of quantum mechanics [8]. Bank notes could be made impossible to forge by containing quantum information records.

The quantum Internet is several decades away. As well as developing full-scale quantum computers, which are capable of processing large amounts of data, it will require a quantum communication network. ‘Blind quantum computation’ is the next step. Here, a user with a classical computer may run an algorithm on a remote quantum computer without sharing the input data or algorithm. This technology would enable public cloud quantum-computing platforms, making blockchains cheaper and more accessible.

Next steps

First, the blockchain business needs to update its existing software to use one-way cryptographic functions that are equally hard to reverse with both classical and quantum computers, which would be a readily-affordable solution [8]. Because these post-quantum solutions are not yet fully established or standardized, platforms must be flexible and capable of changing cryptographic algorithms on the fly [9].

However, post-quantum algorithms will provide only a short-term solution. The only way to ensure long-term protection is to use quantum communication networks. Developing and scaling up the quantum internet will take long-term investments from governments [10]. However, states will benefit from the greater security offered. For example, Canada's census data are kept secret for 92 years, and only with quantum cryptography can such a term be ensured. Government agencies could use quantum-secured blockchain platforms to protect citizens' personal financial and health data.

Countries leading major research efforts in quantum technologies, such as China, the USA and the European Union states, should focus their attention on blockchains and distributed ledgers as first adopters of quantum communications systems and increase investment in this segment. In particular, quantum-secured blockchain can be considered as a use-case for recently announced project for a Quantum Key Distribution Testbed in Europe. At the latest conference on quantum-safe cryptography in Beijing organized by the European Telecommunications Standards Institute (ETSI), one of the largest standardization organization in the telecommunications industry, quantum-safe blockchains were a subject of special discussion session. The impact of the quantum-secure blockchain may be as great as the internet itself.

[Please give all your positions at the below institutions]

A.K. Fedorov,1, _ E.O. Kiktenko,1, y and A.I. Lvovsky1, 2, z
1Russian Quantum Center, Skolkovo, Moscow 143025, Russia
2 Department of Physics, Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, UK

akf@rqc.ru
y e.kiktenko@rqc.ru
z Alex.Lvovsky@physics.ox.ac.uk

A.K.F. is a Quantum Information Technology Group Leader at the Russian Quantum Center.
E.O.K. is a Leading Research Fellow at the Russian Quantum Center.

A.I.L. is a Quantum Optics Group Leader at the Russian Quantum Center & Professor at University of Oxford.

[1] Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system (2008).
[2] Marr, B. How Blockchain Technology Could Change The World. Forbes, May 27, 2016.
[3] Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M.F. & Knottenbelt, W.J. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. R. Soc. open sci. 5, 180410 (2018).
[4] Peng, X., Liao, Z., Xu, N., Qin, G., Zhou, X., Suter, D. & Du, J. "A quantum adiabatic algorithm for factorization and its experimental implementation", Phys. Rev. Lett. 101, 220405 (2008).
[5] Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I. & Fedorov, A.K. Quantum-secured blockchain. Quantum Sci. Technol. 3, 035004 (2018).
[6] Kimble, H.J. The quantum internet. Nature 453, 1023 (2008).
[7] Broadbent, A. & Schaffner, C., Quantum cryptography beyond quantum key distribution, Designs, Codes and Cryptography 78, 351 (2016).
[8] Bernstein, D.J. & Lange T. Post-quantum cryptography. Nature 545, 403 (2017).
[9] Gheorghiu,V., Gorbunov, S., Mosca, M., & Munson, B. Quantum-Proofing the Blockchain. A Blockchain Research Institute Whitepaper (2017).
[10] Chapron, G. The environment needs cryptogovernance, Nature 545, 403 (2017).