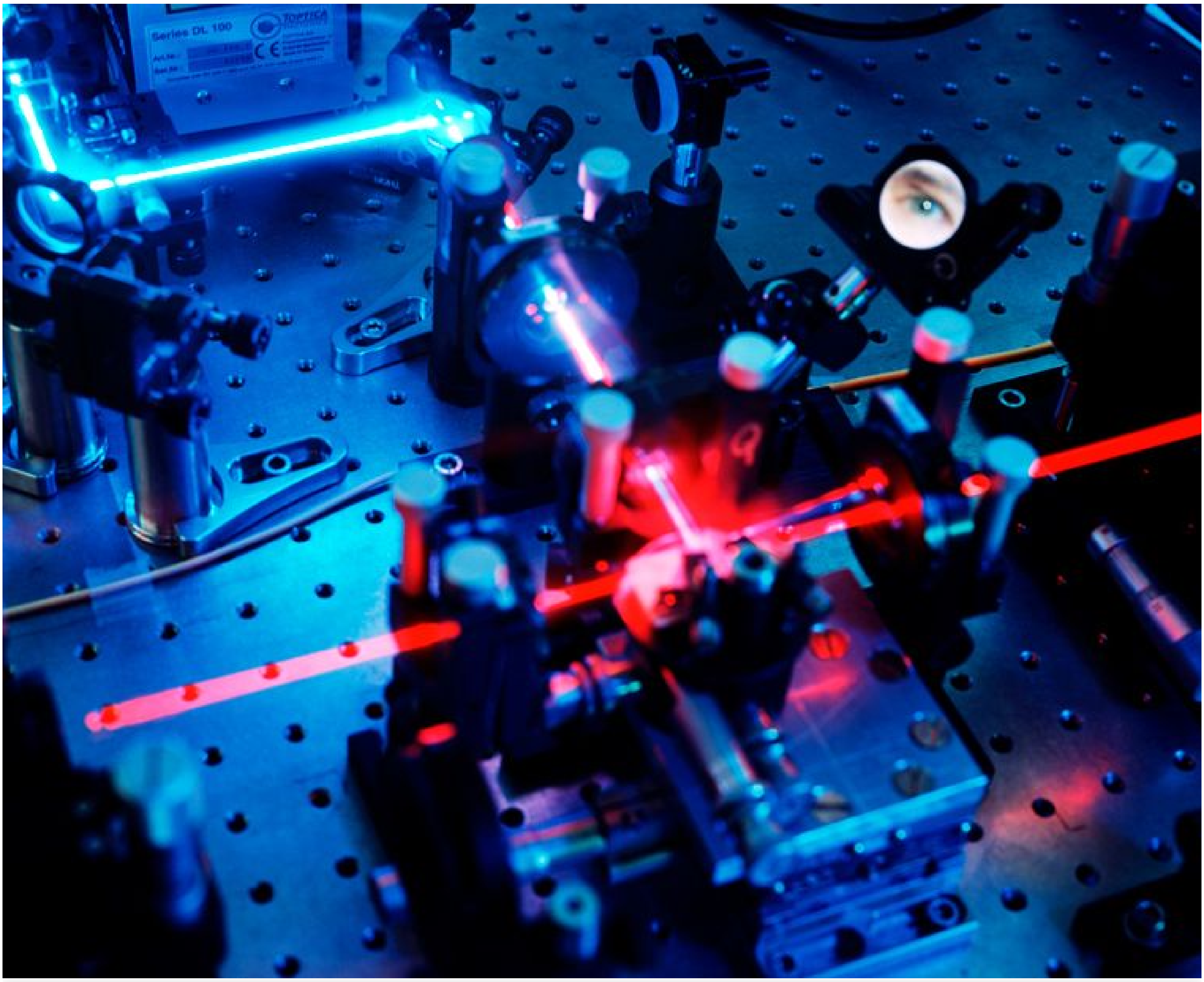
COMMENT · 19 NOVEMBER 2018

Quantum computers put blockchain security at risk

Bitcoin and other cryptocurrencies will founder unless they integrate quantum technologies, warn Aleksey K. Fedorov, Evgeniy O. Kiktenko and Alexander I. Lvovsky.

Aleksey K. Fedorov , Evgeniy O. Kiktenko & Alexander I. Lvovsky



By 2025, up to 10% of global gross domestic product is likely to be stored on blockchains[1]. A blockchain is a digital tool that uses cryptography techniques to protect information from unauthorized changes. It lies at the root of the Bitcoin cryptocurrency[2]. Blockchain-related products are used everywhere from finance and manufacturing to health care, in a market worth more than US$150 billion.

When information is money, data security, transparency and accountability are crucial. A blockchain is a secure digital record, or ledger. It is maintained collectively by users around the globe, rather than by one central administration. Decisions such as whether to add an entry (or block) to the ledger are based on consensus — so personal trust doesn't come into it. Any party inside or outside the network can check the integrity of the ledger by making a simple calculation.

But within a decade, quantum computers will be able to break a blockchain's cryptographic codes. Here we highlight how quantum technology makes blockchains vulnerable — and how it could render them more secure.

One-way codes

Blockchain security relies on 'one-way' mathematical functions. These are straightforward to run on a conventional computer and 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 — it can take a conventional computer many years to solve.

Such functions are used to generate digital signatures that blockchain users cite to authenticate themselves to others. These are easy to check and extremely difficult 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 the contents of the entry 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. That would require reversing the process to derive the information that generated the hash.

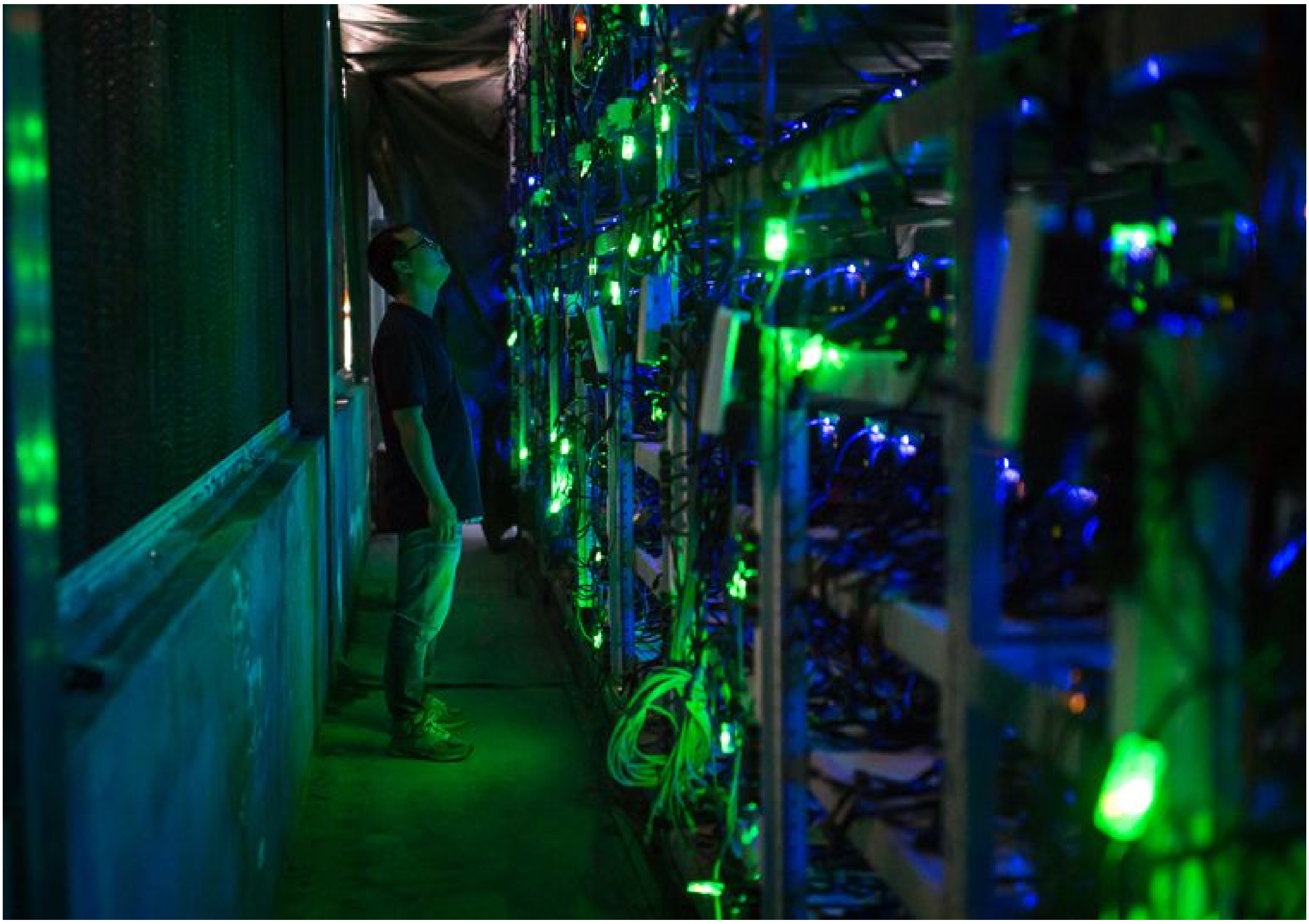
Bitcoin also requires that the hash meets a mathematical condition. Anyone who wishes to add a block to the ledger must keep their computer running a random search until that

Yet, within ten years, quantum computers will be able to calculate the one-way functions, including blockchains, that are used to secure the Internet and financial transactions. Widely deployed one-way encryption will instantly become obsolete.

Information security has faced such mass extinctions before. For example, during the Second World War, German military messages were encoded and decrypted using Enigma machines, initially giving the Axis powers an advantage until the Allies cracked the Enigma code. And in 1997, the Data Encryption Standard, an algorithm for encrypting electronic data that was then state of the art, was broken in a public contest to prove its lack of security. That gave rise to a second competition to develop a new protocol, resulting in today's Advanced Encryption Standard.

Quantum advantage

Quantum computers exploit physical effects, such as superpositions of states and entanglement, to perform computational tasks. They are currently much less powerful than conventional computers, but will soon be able to outperform them on certain tasks. One such example is breaking security protocols that are based on cryptographic algorithms, as mathematician Peter Shor pointed out in 1994[3]. A blockchain is particularly at risk from this because one-way functions are its sole line of defence — a user's only protection is their digital signature, whereas bank clients are protected by plastic cards, security questions, identity checks and human cashiers.



Conventional computer equipment inside a Bitcoin mine near Sichuan, China. Credit: Paul Ratje/The Washington Post/Getty

Cracking of digital signatures is therefore 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. Most specialists think that this feat would require a universal quantum computer (one capable of performing a wide variety of calculations), which is more than a decade away. Yet some researchers suggest that this could happen sooner, using emerging quantum computational devices that have more limited capabilities, such as those being developed by the computing firms D-Wave, Google and others[4,5].

Quantum computers will find solutions quickly, potentially enabling the few users who have them to censor transactions and to monopolize the addition of blocks to the Bitcoin ledger (known as mining). These parties could sabotage transactions, prevent their own from being recorded or double-spend. An international team of researchers has highlighted the possible

If nothing is done to update the protocols, cryptocurrencies will crash once quantum computers become available.

Improving security

Fortunately, quantum technologies also offer opportunities to enhance the security and performance of blockchains.

Quantum-safe encryption. Quantum communications are 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. Our group has demonstrated such a simple system[8]. However, the complexity and cost of quantum cryptography networks will limit their adoption. In particular, current protocols require that each node in the network be connected to every other through optical fibre channels, because there is no trust in any intermediary node and hence all communications must be direct. Protocols will be needed to maintain secure communications even when information flows through untrustworthy nodes; these systems have been developed but need to be made more accessible for consumers.

Photon losses in optical fibres 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 entangled states between the communicating parties. Research is progressing, but is a long way from delivering a practical device.

In the interim, one-way functions should be tightened. Some alternative encryption functions have been proposed[9] that should be equally difficult to reverse using conventional or quantum computers. Although not completely secure, these could be run on existing hardware and would buy time, but they, too, could be deciphered in the long term.

Quantum internet. Using quantum technology for communicating as well as for the computationally intensive steps of the current verification and consensus processes, and thus be more efficient and more secure. The proposed Quantum Bitcoin currency could be realized, with its security assured by the no-cloning theorem of quantum mechanics. Such quantum 'bank notes', if they still prove necessary in future, could be made impossible to forge by containing quantum information records[11].

The quantum internet is several decades away, so 'blind quantum computation' is an interim step. In this, a user with a conventional computer could 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

The blockchain business needs to update its existing software to use one-way cryptographic functions that are equally hard to reverse using conventional or quantum computers[9]. Until these post-quantum solutions are established or standardized, platforms must be flexible and capable of changing cryptographic algorithms on the fly[12].

The longer-term answer is to develop and scale up the quantum communication network and, subsequently, the quantum internet. This will take major investments from governments. However, countries will benefit from the greater security offered[13]. For example, Canada keeps its census data secret for 92 years, a term that only quantum cryptography can assure. 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 United States and members of the European Union, will be among the early adopters. They should invest immediately in research. Blockchains should be a case study for Europe's Quantum Key Distribution Testbed programme, for example.

Much greater urgency needs to be given to these risks — their impact could be grave.

Nature 563, 465-467 (2018)

doi: 10.1038/d41586-018-07449-z

1. Marr, B. ‘How Blockchain Technology Could Change The World.’ (Forbes, 27 May 2016).
2. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System* (Bitcoin, 2008).
3. Shor, P. W. in *Proc. 35th Ann. Symp. Found. Comp. Sci.* 124–134 (IEEE Comp. Soc. Press, 1994).
4. Peng, X. *et al. Phys. Rev. Lett.* **101**, 220405 (2008).
5. Anschuetz, E. R., Olson, J. P., Aspuru-Guzik, A. & Cao, Y. Preprint at https://arxiv.org/abs/1808.08927 (2018).
6. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M. & Tomamichel, M. Preprint at https://arxiv.org/abs/1710.10377 (2017).
7. Stewart, I. *et al. R. Soc. Open Sci.* **5**, 180410 (2018).
8. Kiktenko, E. O. *et al. Quantum Sci. Technol.* **3**, 035004 (2018).
9. Bernstein, D. J. & Lange, T. *Nature* **549**, 188–194 (2017).
10. Kimble, H. J. *Nature* **453**, 1023–1030 (2008).
11. Broadbent, A. & Schaffner, C. *Des. Codes Cryptogr.* **78**, 351–382 (2016).
12. Gheorghiu, V., Gorbunov, S., Mosca, M. & Munson, B. *Quantum-Proofing the Blockchain* (Univ. Waterloo, 2017); available at https://go.nature.com/2b2uvft
13. Chapron, G. *Nature* **545**, 403–405 (2017).

Nature ISSN 1476-4687 (online)