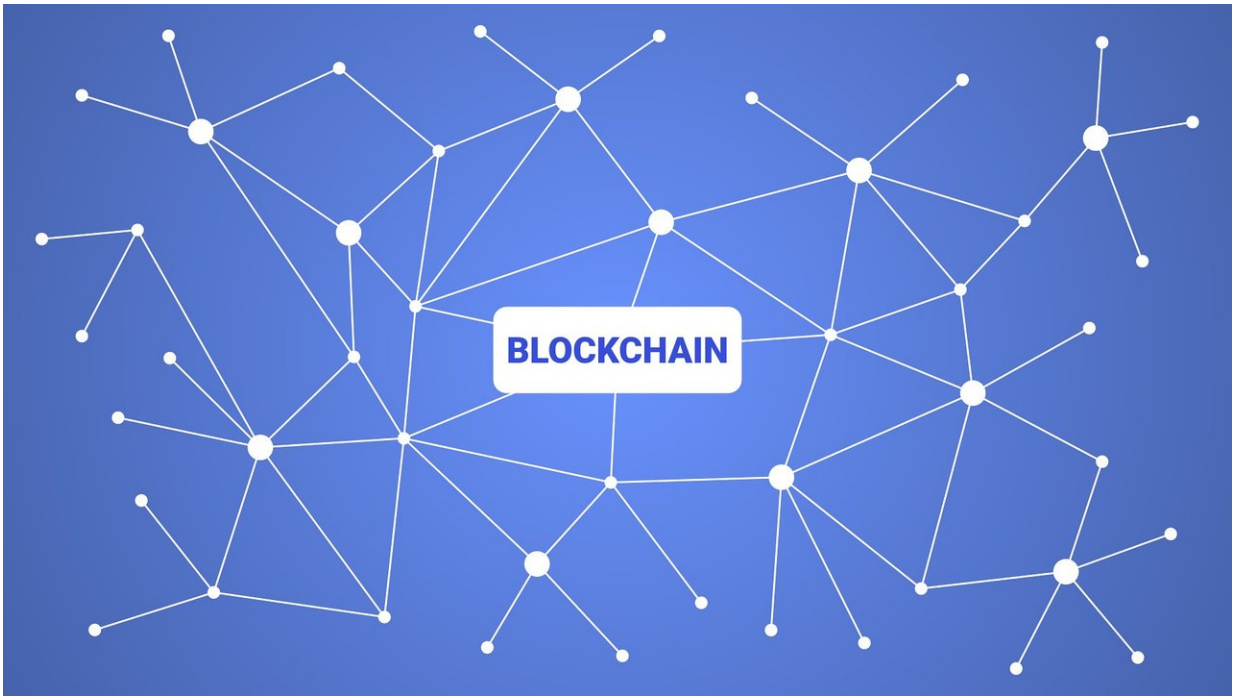
Using a quantum blockchain to protect blockchains of the future

April 25 2018, by Bob Yirka



Credit: CC0 Public Domain

A pair of researchers with Victoria University of Wellington has suggested that the way to prevent future blockchains from future hackers using quantum computers is to use quantum blockchains. Theoretical physicists Del Rajan and Matt Visser explain their idea in a paper they have uploaded to the *arXiv* preprint server.

A blockchain is a digital ledger recording transactions between different entities. These ledgers are stored both publicly and chronologically. The most famous example is BitCoin. For now, BitCoin and other cryptocurrencies like it are considered to be safe from disruptive hackers due to their encryption methods and decentralized nature. But, it has been noted, that could change if quantum computers are fully realized. Rajan and Matt Visser note, however, that this development may not spell the end of the blockchain. They believe they have found a way to prevent quantum computers from being used as a disruptive force by using quantum blockchains.

A quantum blockchain, the pair suggests, would take advantage of entanglement, which in most cases, applies to situations regarding space. But it could also be useful for situations involving time, such as blockchains. In such a blockchain, the pair explains, transaction records could be represented by pairs of entangled photons linked in chronological order. When transfers take place, photons would be created and absorbed by the hubs that comprise a network. But since entangled photons are linked across time, they can be caused to have never existed at the same time.

Thus, any measurements of the more recent photon in a record would be influenced by the photon that came first, in the past, before it was measured—which would mean if a hacker tried to access such a record or block of records, they would find it impossible, because the entangled photon that represented it no longer existed in the current time. That means a hacker would only ever be able to access the most current record blocks—and if they did, it would invalidate the others, which would alert users of the network to an intruder. Rajan and Visser note that such a blockchain could be viewed as an example of a quantum time machine.

More information: Quantum Blockchain using entanglement in time,

arXiv:1804.05979 [quant-ph] arxiv.org/abs/1804.05979

Abstract

A conceptual design for a quantum blockchain is proposed. Our method involves encoding the blockchain into a temporal GHZ (Greenberger-Horne-Zeilinger) state of photons that do not simultaneously coexist. It is shown that the entanglement in time, as opposed to an entanglement in space, provides the crucial quantum advantage. All the subcomponents of this system have already been shown to be experimentally realized. Perhaps more shockingly, our encoding procedure can be interpreted as non-classically influencing the past; hence this decentralized quantum blockchain can be viewed as a quantum networked time machine.