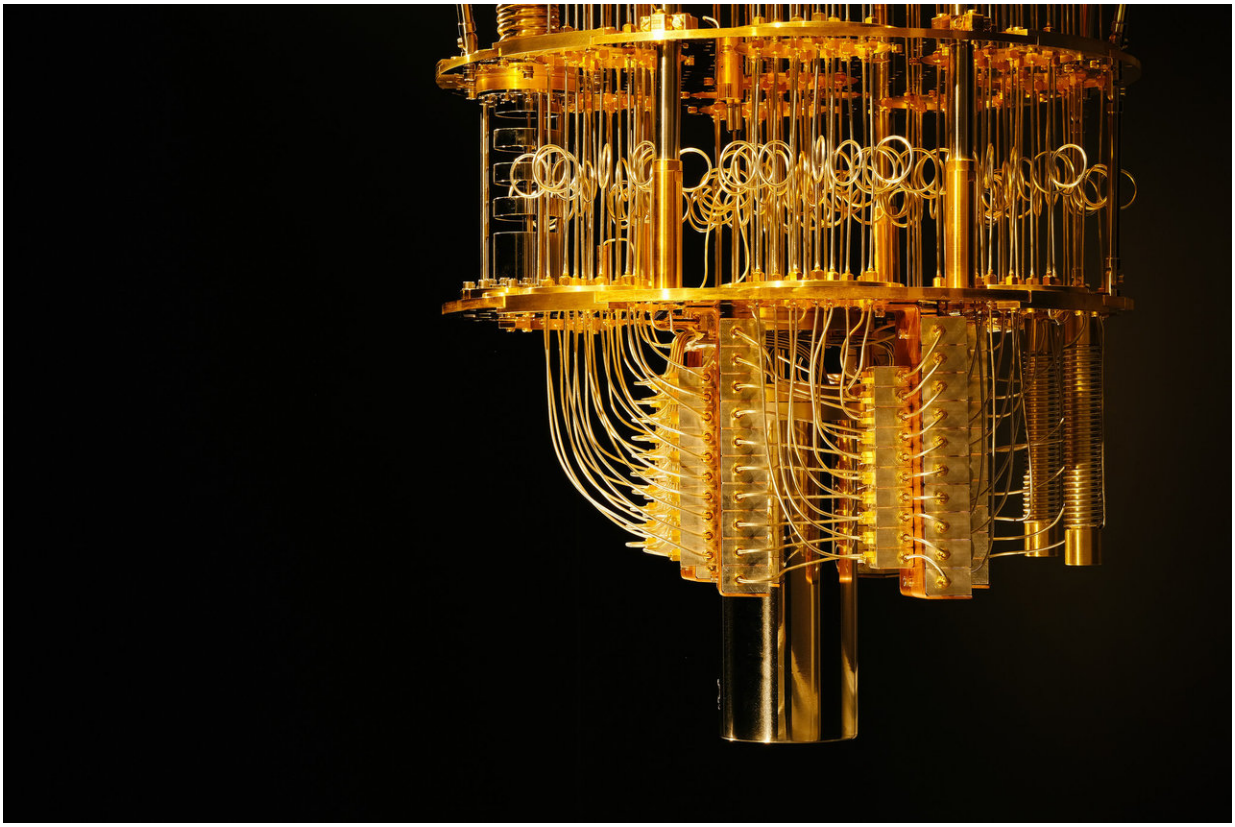
How quantum computers could steal your bitcoin

July 16 2018, by Marco Tomamichel



Part of IBM Research's quantum computer. Credit: IBM Research/Flickr, CC BY-ND

Cryptocurrencies like bitcoin have recently captured the public's imagination because they offer an exciting alternative to traditional

monetary systems.

Bitcoin transactions are essentially a series of puzzles stored in public on the blockchain. The puzzles used to protect bitcoin are so complex that current computer technology isn't powerful enough to crack them.

But quantum computers could crack these puzzles in coming decades. Here's how it could happen to your bitcoin.

How does the encryption behind bitcoin work?

Traditional currencies rely on trusted intermediaries like banks to verify and record all monetary transactions. The cryptocurrency economy instead relies on a public ledger – the blockchain – which is maintained by all honest participants of the bitcoin network.

Banks are usually required by law to authenticate the sender and recipient of any transaction. But cryptocurrency transactions can, in principle, be performed anonymously.

Imagine a hypothetical potential bitcoin recipient called Alice. She must first create a unique and extremely difficult puzzle that can only be easily solved using a secret hint (called a private key) that she keeps to herself. Moreover, it must be easy to verify that the solution is correct. This is done using another hint (called a public key). After this happens, Alice sends the puzzle out to anybody who would like to send bitcoins to her.

Now imagine a sender; let's call him Bob.

If Bob wants to send bitcoin to Alice, he will submit a transaction to the network that contains two ingredients: Alice's puzzle and a solution to a puzzle unlocking funds sent to Bob in a previous transaction. He'll also

reveal the public key used to verify the solution. If the solution is verified by the different participants of the network, they will assume that Bob is indeed authorised to spend his bitcoin and accept the transaction into the blockchain. Alice can now spend the funds by revealing a solution to her puzzle.

In this way, the full ledger of bitcoin transactions is entirely public, while the identities of the bitcoin owners are protected.

Can you access bitcoin without the private key?

In fact, anybody who can solve one of the puzzles on the blockchain without the secret hint can access the funds stored there. Hence the only distinguishing feature of the intended recipients is that they can solve these puzzles more efficiently than others, thanks to the secret hint only they know.

Most puzzles used for bitcoin take the form of signatures. Namely, bitcoin transactions are electronically signed using a really complicated algorithms based on what mathematicians call elliptic curves. The idea is that creating such a signature is prohibitively difficult for any computer unless one holds the secret key, and that it can be verified easily using the public key.

However, while these signatures indeed appear impossible to fake for today's computers, quantum computers can potentially solve them very efficiently. This is possible because quantum computers are not restricted to processing digital information, but instead perform calculations directly using the quantum mechanical interactions that dominate physics at a microscopic scale.

Researchers are still trying to find out exactly what kind of problems quantum computers are superior at solving. But we do know that two

problems underlying much of today's cryptography happen to be ones that tomorrow's quantum computers may be able to solve quite efficiently (for the experts at home, in addition to solving elliptic curves, the other problem is finding the prime factors of a number).

In particular, elliptic curve cryptography can be broken running a variant of Shor's algorithm. This algorithm is able to compute the secret key from the public key efficiently, and thus is able to create signatures quickly once the public key is revealed. This can't be done using today's computers. In fact, we believe that only quantum computers will ever be able to perform this computation.

How would a thief with a quantum computer steal bitcoin?

The current mechanics of bitcoin mean the public key is only revealed with the signature when a transaction is proposed to the network. Hence there is a very short window of opportunity for a quantum computer to calculate the private key from the public key and present an alternative signed transaction (for example, making Bob's money go to the thief instead of to Alice).

We can think of this attack as analogous to robbing a customer just before he enters a bank to deposit money.

Making things worse, for many bitcoin transactions the public key is actually already known and stored on the blockchain. This removes the timing constraint for the above attack and allows a thief to steal funds even if no transaction is proposed. This affects approximately a third of the bitcoin market capital, or several tens of billions of dollars.

This is more like a traditional bank robbery where the thief doesn't have

to wait for a customer to make transactions.

It is hard to predict when quantum computers will be strong and fast enough to perform these attacks, but it is fair to assume that we are safe for at least the next ten years.

Can we make bitcoin safe?

It is important that researchers find alternatives to elliptic curve cryptography that are resistant against attacks by quantum computers.

And although no standard has emerged yet, alternative cryptocurrencies that take quantum computers into account are being developed right now . So even if bitcoin might ultimately succumb to quantum computers, blockchain and cryptocurrencies will certainly live on.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How quantum computers could steal your bitcoin (2018, July 16) retrieved 25 April 2024 from https://phys.org/news/2018-07-quantum-bitcoin.html