Crypto, Quantum Computing, and You

Author	josh
Date	2020-07-19 19:48:24

Overview

Many have asked a valid question about Bitcoin and other cryptocurrencies - will they be rendered useless by the advent of quantum computing? Bitcoin is ultimately a software protocol, with several cryptographic algorithms securing it from attackers. But what if attackers can easily break those algorithms once thought to be perfectly secure?

Quantum, Cryptography, and Bitcoin

What is Quantum Computing

First, lets dive into an explanation of what quantum computing actually is. The term may be confusing - what exactly makes quantum different than other forms of computation that we are used to?

In computers, all data is ultimately represented by units called *bits* - simply 0 or 1. Electronically, these can be thought of as a series of on-off switches. Bits can be built up into any form of data you would like to represent - numbers, strings, spreadsheets, videos, and of course, Bitcoin keys! Inside the machinery of a computer, a bit can only be 0 or 1, and a bit must be "flipped" to represent a different kind of data - an operation that takes some amount of (miniscule) time.

In a quantum computer, however, bits referred to as *qbits* have the ability to represent 0 or 1 *at the exact same time.* Confused? Yea, me too - but we don't have to understand how this works to understand the importance of quantum computing. This fact means that computations can be done *dramatically faster* than with a typical computer. Operations that might take the lifetime of the universe on a supercomputer could be broken in a practical amount of time using a quantum machine.

Bitcoin Cryptography

So what does this have to do with Bitcoin and other cryptocurrencies? This means that some of the cryptographic algorithms underpinning the Bitcoin system could be broken by quantum computing! But which ones specifically?

Hashing algorithms are used primarily for mining Bitcoin and also in the process of generating addresses. SHA-256 and RIPEMD160 are the primary algorithms used in Bitcoin, with others such as Scrypt (technically a key-derivation function) and SHA-3 (Keccak) used in Litecoin, Ethereum, and others. Thankfully, these cryptographically secure hashes are *not* vulnerable to quantum computing - we don't have to worry about them.

Elliptic curve digital signature algorithms (ECDSA) are also critical to making Bitcoin work. These are used to generate addresses (taking a private key to a public key) and used to *sign* Bitcoin transactions (proving one is the owner of funds spent in the tx). ECDSA *is, unfortunately, vulnerable to quantum computing.* In the future, a sufficiently powerful quantum computer could be used to reveal a user's private key from a public key, and operation normally not possible.

So What Can We Do?

Thankfully, this quantum vulnerability won't be the end of Bitcoin, not at all!

First, we can buy time in the event of a vulnerability by *avoiding address reuse*. A Bitcoin address is not a raw public key, but rather a hash of a public key. Since SHA-256 isn't vulnerable to quantum, and address that's only used for receiving (hasn't been spent from yet) is shielded from the ECDSA vulnerability. The raw public key is only revealed when the user creates a transaction to *spend* funds at that address. If a user only uses an address once, they would avoid potentially losing funds.

That's not a permanent solution, however, and is a usability nightmare. The real long term solution is to *hard-fork* the Bitcoin network, requiring users to upgrade their software to a new version. This new software would replace ECDSA with a digital signature algorithm that isn't vulnerable to quantum computing instead.

Quantum Panic? Nah, Bitcoin's Got This!

Although Bitcoin *is* vulnerable to future quantum computing breakthroughs, not all hope is lost. We have time, as quantum computing is not there yet. And in the future, there are stop-gap solutions and long term changes to the protocol that will keep the crypto world running smoothly in a post-quantum world.