Top 3 reasons why the crypto community shouldn't be afraid of quantum computers

Quantum computers have been received as the cryptocurrency killers because they are great at solving multiple tasks at the same time. Many fear that the Bitcoin network among many others will fail.

However that's not the entire truth, there are many more aspects to consider. In this article you'll understand why quantum computing is not there yet and what you can expect from our current advances in computing.

Before understanding why quantum computing is not capable of breaking any cryptocurrencies yet, we have to understand a major key aspect of this technology: Quantum computers are really good at a few selected tasks while being extremely bad at many others.

Specifically current implementations are too specialised to be used on a commercial level. They are the result of ongoing investigations and are just not good at 99% of the things we are interested in.

We need a more complete type of quantum computer to even consider the possibility of cracking blockchain encryption.

See, quantum computers are based on the direction of atoms when you measure them. There are laws in physics that allow computers to measure atoms knows as qubits at massive rates. You can easily calculate the position of many qubits at the same time.

This allows us to execute parallel computing at insanely fast speeds compared to traditional computers, it's like moving at light speed. So, if they are so fast at testing multiple possible results for a given encryption algorithm, shouldn't we be afraid of them breaking Blockchain's algorithms? No, here's the first reason why:

Innovation is still slow in quantum computing

There aren't good quantum computers yet and that kind of innovation will take us years to attain. Even a good quantum computer can only halve the difficulty of the SHA-256 algorithm used on the entire Bitcoin network among many other Blockchains.

Which means, the SHA-256 algorithm will become equivalent to the SHA-128, which is still unbreakable so there's nothing to worry about. Yet.

You see, quantum computers are measured by how many qubits they can process at a given moment which is a entire new system based on physics at the atomic level. Even if we had the most theorically powerful quantum computer right now, it would be almost impossible to break those existing algorithms.

SHA-256 and others are so incredibly strong that we can't event fathom how many iterations we need to generate our desired hash. Besides, even if such a strong computer existed on the hands of big corporations and agencies, we wouldn't know until they had no other choice but to use that technology.

They will keep their advances as a secret to protect their inventions because the moment people know they have those quantum computers, Bitcoin and other blockchains will simple hard-fork into a more reliable system that can't be broken that easily since cryptocurrencies are based on trust at the core.

Cryptocurrencies are based on people's trust
If the majority of the people using crypto decide to not use the current implementation, it will simply be changed in a matter of hours, rendering all those quantum computers useless for this particular use case.

What's interesting is that we can detect when quantum computers are implemented properly by just watching if the wallets of dead people holding major coins suddenly make moves since nobody else knows their keys.

On the other hand, those agencies capable of creating such a strong computer won't focus their attention on Bitcoin and blockchain because if you think about it, they have more than enough funds to not care about the money they could possibly make out of crypto hacking.

Big companies won't have the need to hack cryptocurrencies

If you have so much capital to create a computer that breaks one of the strongest algorithms in existence, then you probably don't care about cracking a blockchain, you'll probably focus on other aspects related to security and surveillance or whatever interests you.

These computers are good at solving algorithms based on elliptic curves such as ECDSA which is an elliptic curve type of algorithm for encrypting your digital signature on the blockchain for the purpose of generating unique accounts.

Theoretically, quantum computers will be able to crack and access accounts that have been used at least once because they are able to generate the private key from your public key and signature.

That means accounts that have made at least one transaction are at risk because their public keys and signatures are stored permanently on the blockchain. Even if that happens, you can simply move your funds to another wallet and you'll be safe.

Accounts on the blockchain are very easy to generate, cost nothing and are limitless so you will be able to make moves before having your accounts hacked.

As a general recommendation, you should use your addresses only once to prevent these types of attacks even thought they are not possible yet. It may take 10 years to create such powerful quantum computers because much research needs to be done around the topic.

Banks also use SHA-256 which means they are also safe from quantum computing although they have other encryption systems that may be vulnerable so it's up to each bank's software system.

In the blockchain, the private keys are passed through many layers of encryption, something known as hash-chaining to increase the security of these keys making them even more unlikely to be hacked.

By the nature of encryption algorithms, every hash has a corresponding key that can be calculated by brute force, testing all the possible combinations in the universe until you find one matching your expected key.

The algorithms used to generate public keys can be cracked using Shor's algorithm, which uses quantum positioning to make multiple guesses at once on quantum computers. That way you can un-encrypt an RSA or ECDSA type of algorithm without waiting years.

In summary, there will pass at least a decade before we have to seriously consider the dangers of quantum computers. You can keep using your accounts without repercussions for now. If you're paranoid about the consequences, simple generate a new Bitcoin address everytime you make a transfer to avoid being affected by elliptic curve un-encryption hacks.

Remember, quantum computers are not a threat because:

- Innovation is still slow in quantum computing
- Cryptocurrencies are based on people's trust
- Big companies won't have the need to hack cryptocurrencies