Is it possible to hack a Bitcoin wallet with a quantum computer

Experts predict quantum computers will be able to break through the defenses of Bitcoin wallets in the next few years.

Operating on blockchain technology, Bitcoin is one of the most secure systems available today, leaving many seasoned hackers with no hands when trying to crack electronic wallets containing Bitcoin. From here, there are cases of crying and laughing like the story of "missing millionaire" Stefan Thomas - a German programmer. Just because he forgot the e-wallet password, this person could not access his 7,002 Bitcoins, currently worth the equivalent of 265 million USD.

But with the prospect of quantum computing, Stefan Thomas can completely think about applying this technology to get his Bitcoin wallet back in the future.

Currently, quantum computing is a very early field, but the government and companies like Microsoft and Google are working to make it a reality.

Within 10 years, quantum computers could be powerful enough to break the cryptography that protects cell phones, bank accounts, email addresses, and even Bitcoin wallets.

Fred Thiel - CEO of Marathon Digital Holdings said: "If you have a quantum computer today and it is funded by the state, say the Chinese state, in about 8 years you can crack a wallet on the blockchain." .

This is precisely why cryptographers around the world are racing to build quantum resistant encryption protocols.

Currently, much of the world is using asymmetric cryptography, whereby each user uses a pair of private and public keys to access email and digital wallets.

This key pair allows the user to create a digital signature. In the case of cryptocurrencies like Bitcoin, this digital signature is called "Elliptic Curve Cryptosystem" (ECDSA) which ensures that only the owner can open a Bitcoin wallet.

"Every financial institution, every login on your phone - it's all based on asymmetric cryptography, easily hacked by quantum computers," says Fred Thiel. Thiel was a former director of Utimaco - one of the largest crypto companies in Europe. He has worked with Microsoft, Google and many other companies to research post-quantum encryption - cryptographic algorithms that cannot be attacked by quantum computers.

Theoretically, using quantum computing, a bad guy could change your private key, forge your signature, and then drain the wallet.

Thorsten Groetker - former CTO of Utimaco, one of the leading experts in the field of quantum computing, said: "The first type of electronic signature that can be broken by a quantum computer is an elliptic curve-based signature. which we use today for Bitcoin wallets. But that will only happen if we don't act."

Strengthen Bitcoin Wallet

However, many crypto experts are not worried about the risk of Bitcoin wallet being hacked. Nic Carter, a partner at Castle Island Ventures, believes that quantum computing is far from mature, so Bitcoin wallet hacks cannot happen overnight.

There is still time for cryptographers to find ways to prevent future attacks by quantum computers. "The National Institute of Science and Technology (NIST) has been developing a new standard for quantum computer attack-proof encryption," Thiel said.

According to Thorsten Groetker, there will be new algorithms for digital signatures. He hopes that the algorithm that makes the cryptocurrency resistant to quantum attacks will be available in 2024, before the prospect of a hacked Bitcoin wallet becomes a reality.

As new post-quantum cryptography is standardized, Bitcoin or Ethereum owners will be able to transfer funds from their old wallet to their new wallet, secured with a new, more secure key.

However, this type of security upgrade requires users to be proactive. Since cryptocurrencies operate on a decentralized network, each owner has to automatically update his or her system, there will inevitably be cases like the owner still keeping the money in the old wallet, forgetting the wallet password. , or die without sharing the password with anyone.