Cryptocurrency security needs a makeover – here is the start.

In May 2021, Deutsche Bank announced Bitcoin as the third-largest global currency in circulation. More only the euro and the US dollar.[1]

In 2020, the total market capitalization of cryptocurrencies was $ 330 billion, and today it is approaching $ 2 trillion. Institutional investors account for 63% of cryptocurrency trading, up from 10% in 2017[2], which means the fall in its value is bound to reflect in balances across Wall Street and worldwide.

Over time, cryptocurrencies have gained recognition as an alternative to fiat currency, and many businesses are using crypto to transact. This reliance on cryptocurrency needs to be backed by the stable infrastructure these cryptocurrencies operate on. In recent years, cryptocurrencies have been under cyber-attacks as the attackers are exploiting the moving parts of the cryptocurrency's technical infrastructure, such as crypto exchanges, wallets, networks, to name a few.

In a recent attack, Crypto.com, Singapore based company confirmed that about 400 users' coins were withdrawn amounting to $31M lost[3]. In January 2018, Japan-based Coincheck had its NEM (XEM) tokens stolen to the tune of more than $530 million. Hackers exploited that the currency was being kept in a "hot" wallet[4]. And in August 2021, a hacker attacked Poly Network by exploiting a vulnerability in its system and managed to steal funds worth over $600 million[5]. These are just few examples of attacks, and these attacks are on rise.

The advancement in the development of Quantum computers can be an existential risk for the cryptocurrency infrastructure. "Everything we do over the internet today," says Harri Owen, chief strategy officer at the company Post Quantum, "from buying things online, banking transactions, social media interactions, everything we do is encrypted. "But once a functioning quantum

[1] https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000516270/The_Future_of_Payments%3A_Series_2_-_Part_II__When_d.pdf

[2] https://twitter.com/theeconomist/status/1425497007041482758

[3] https://mothership.sg/2022/01/crypto-hacked-reimburse-ethereum/?fbclid=IwAR30DX5CvFbMqQdZXocN3W4GSL2ebl53CVzjSdfcZV_3pdxpFLwjOZlrGyQ

[4] https://www.reuters.com/article/us-japan-cryptocurrency/japan-raps-coincheck-orders-broader-checks-after-530-million-cryptocurrency-theft-idUSKBN1FI06S

[5] https://www.zdnet.com/article/poly-network-hackers-potentially-stole-610-million-is-bitcoin-still-safe/

computer appears that will be able to break that encryption... it can almost instantly create the ability for whoever's developed it to clear bank accounts, to completely shut down government defense systems - Bitcoin wallets will be drained."[6]

By the time a large-scale quantum computer arrives in the foreseeable future and gets into the mainstream business, cryptocurrencies will be even more integrated into the global financial system, and the losses will be even more significant. Overall, we expect a $ 3.3 trillion hit to the US economy in the event of an attack on cryptocurrencies. The calculation is based on the current value of the cryptocurrency. Also, some state actors are investing time and money to allow cryptocurrencies to be hacked and stolen. Additionally, the advancement of quantum computing by these state actors is unknown. This easy theft of money needs to stop. So, where do we start!

Let's take a closer look at what parts of cryptocurrencies are and how they are susceptible to attacks by quantum computers.

Cryptocurrency reliance on PKI (public key – private key)

The blockchain accounting technology that cryptocurrencies rely on today is protected by the public key cryptography. The system is ubiquitous, protecting your online purchases and encrypting your messages from everyone but the intended recipient. The technology works by combining a public key that anyone can see with a private key that is only available to your eyes. In the case of cryptocurrencies such as Bitcoin, this digital signature uses an elliptical curve-based digital signature algorithm and ensures that the rightful owner can only spend Bitcoin. The quantum computers can break this protection mechanism as they can theoretically use Shor's algorithm to break into the PKI based on prime factorization.

If current progress continues, quantum computers will crack public-key cryptography, potentially posing a serious threat to the crypto world. Some currencies are valued at hundreds of billions of dollars. If the encryption is compromised, attackers can impersonate the legitimate owners of cryptocurrencies, NFTs, or similar digital assets.

The good news is that the CypherShield platform provides a quantum-resistant and proprietary way of 3-pass exchange on the secret key between the two parties. Even powerful quantum computers will find it extremely difficult to hack the secret key except for brute force. The CypherShield algorithms is based on computational impossibility (Hilbert's tenth problem and Diophantine equations) versus computational difficulty (RSA algorithm).

[6] https://www.bbc.com/news/technology-60144498

Crypto Wallets – weak link in the crypto infrastructure

Crypto wallets are a storage mechanism for investor to store their cryptocurrency. These wallets are broadly classified as hot wallets and cold wallets. Hot wallets store the crypto on the Crypto exchanges and can be accessed over the internet. Cold wallets are hard wallets or physical devices that the investor can use to store the crypto coins offline.

These crypto wallets that people use to track their digital assets can also be vulnerable to quantum computing. These wallets store private keys that people need to access their blockchain assets, and a successful attack can empty your wallet.

These attacks and possibly other, more unpredictable ones may appear, so timely planning is necessary for the readiness of the emergence of quantum computers - and with the help of forking, cryptocurrencies can be updated to use post-quantum encryption and protect against these shortcomings. Wallet safety is essential, as cryptocurrencies are high-value targets for hackers.

CypherShield currently is working in Post Quantum Crypto Wallet (PQCW), which uses Undefined Algorithm Technology (UAT) to encrypt a private key. The PQCW does not contain the private key directly. Therefore, wallet hacking does not give the attacker secret key data, and it includes a one-time Stamp that the user owns. Using CypherID technology, the user has access to one-time Tables for the operators of the used algorithm. Using both the one-time table CypherID and User Stamp at the same time, the user gains access to his private key via PQCW and UAT.

Today, cryptocurrencies have a lot of promise to deliver, and the world realizes the potential value of these digital coins. Though, these crypto needs to be secured and protected from hackers. The core infrastructure of these cryptocurrency platforms needs to be redesigned. Even future technologies such as quantum computers will find it extremely difficult to hack and steal cryptocurrency. This problem's core is the public key infrastructure these exchanges, wallets, and networks rely on. CypherEye is positioned to address this problem using its patented and proprietary CypherShield platform.