As the SEC Launches Crypto Office, Blockchain Security Brings Out Its Big Guns

January 13, 2021 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

When they say “the love of money is the root of all evil,” it’s not just a biblical verse intended to guide impressionable children. It’s a clear reminder that wherever financial gain is possible, those with malicious intent lurk not too far behind.

Recent events have proven there’s financial gain in cryptocurrency, if that wasn’t clear enough already. Shortly after PayPal announced it would allow its users to buy, sell, and hold cryptocurrency and Joe Biden won the U.S. presidency, Bitcoin’s price shot up to record highs, eventually breaching the $37k mark. Other cryptocurrencies followed suit. While the latter doesn’t necessarily indicate causation, Bitcoin held its highs, and Ethereum, the second-largest cryptocurrency, boomed after the president-elect appointed cryptocurrency-savvy Gary Gensler to lead his financial policy transition team.

And the icing on the cake? The U.S. Securities and Exchange Commission (SEC) announced earlier this month the launch of a new standalone office dedicated solely to blockchain and digital assets to keep up with the technological advancements.

Related: How to Buy, Sell and Keep Track of Bitcoin

These are only the latest developments, as institutional

investors put their money in crypto and digital assets exchanges sprout all over the world. Now that these novel assets are joining the big leagues, so must the security protocols entrusted to protect everyone’s money. And the security heavyweights are bringing out the big guns.

In early December, cyber startup GK8 brought its high-security vault for digital assets to the Spain-based Prosegur, one of the world’s largest custodians in the field of physical security for traditional banks. The vault will power Prosegur’s new service for custody and management of digital assets, representing the first time a cash-management company enters the digital asset space and offers custody of cryptocurrency.

Blockchain is secure, but digital assets can be stolen

For those less acquainted with the cryptocurrency industry, this development raises several questions. Firstly, if blockchain is so secure, why does one need an ultra-secure vault to store it? Secondly, isn’t cryptocurrency digital? Why the need for physical armor?

Cryptocurrency is known, especially by industry outsiders and average people, as an inherently secure currency because it is powered by blockchain technology, a notoriously secure framework for record-keeping on an online ledger. While that’s not wrong, there are blind spots and weaknesses that hackers can, and do, exploit. According to blockchain analytics firm CipherTrace, malicious hackers have amassed $1.36 billion in stolen crypto through the first five months of 2020 alone. That heist puts 2020 on a fast track to become the second-costliest year in crypto history, behind 2019’s record $4.5 billion.

Most often, hackers reach the cryptocurrency by attacking the

endpoints using wallets to create and sign transactions before they are sent to the blockchain. To hack the blockchain itself, they have to gain control of more than half of the network's computing power and rewrite the transaction history—a challenging, though not impossible, task. It has happened in the past, perhaps most notably when Ethereum Classic (ETC), one of the cryptocurrencies people can buy and sell on Coinbase's popular exchange platform, was attacked in this manner. Almost $1.1 million in crypto was stolen.

Related: 5 Crypto Investment Mistakes You Should Avoid in 2021

Why a physical wallet for digital assets?

However, the wallets and vaults where the cryptocurrency is stored are the targets, not the blockchain itself. This ties into the second question posed above, regarding crypto being stored in a physical wallet. It's true people buying Bitcoin, XRP and the like often store their currencies in digital wallets, but often the most secure wallets are physical, "cold" wallets that aren't connected to the internet, such as the famous Trezor. The hardware wallet has earned itself quite the reputation among crypto enthusiasts for its top-notch security, with reviews such as the one published in Coindesk in the early days of the walled titled "Bitcoin 'Vault' Trezor Lives Up to its Name."

Related: 5 Types of Cryptocurrency Entrepreneurs Should Know About

Such wallets are almost—but not fully—impossible to hack. The weak point is that they connect to the internet when executing transactions, and that's when hackers can theoretically strike. For individual use, wallets like the Trezor and the Ledger Nano X are the crème de la crème, consistently

appearing in top hardware wallet lists across the web. However, Custodial use requires a different level of security, known as a vault, rather than a wallet.

GK8’s institutional-grade vault being implemented by Prosegur takes the “cold” aspect a step further, letting institutions transact on the blockchain while being totally offline. The vault accomplishes this feat through patented cryptography that enables it to create, sign and send blockchain transactions through a unidirectional connection without receiving any digital input that can include malicious code.

“Prosegur built its business around cash management and physical security services, and wanted to expand into digital-asset custody and get a foothold in the exploding crypto-economy,” GK8 CEO and Co-Founder Lior Lamesh said. “Custody of cash, gold, jewelry and physical assets requires very different security measures than crypto custody. With our cyber expertise and end-to-end platform, we enabled Prosegur to accomplish this transformation while adhering to the highest security standards.”

The development of high-security digital-assets storage marks the next step in the natural evolution of cryptocurrency, as much of the premise behind Bitcoin, the world’s first cryptocurrency, centered around the privacy and security inherent in blockchain. We can expect hackers to up the ante and security experts to continue to respond in the future. Hopefully, the good guys stay ahead of the game.

https://www.entrepreneur.com/article/361499