How thieves manage to steal cryptocurrency

February 9 2022, by Joseph Boyle, Lucie Lequier

US officials announced they had recovered $3.6 billion of bitcoin stolen in a 2016.

US officials announced on Tuesday they had recovered $3.6 billion of bitcoin stolen in a 2016, throwing a light on the scams that surround cryptocurrency.

But how exactly do criminals steal in the virtual world?

Hacking the exchanges

Bitcoin and other cryptocurrencies are bought, sold and stored on exchanges, just like commodities in the non-virtual world.

But crypto investors, and those who organize exchanges, often object to centralized control and reject stringent oversight—and that sometimes leads to lax security.

"Exchange sites have stocks that are relatively large at any given time in crypto," says Manuel Valente of Coinhouse, a French company that manages crypto transactions.

"But these are servers, machines—and malicious people sometimes manage to get into their servers and steal money."

Most of these problems are caused by weak security, he says.

Alexander Stachtchenko of KPMG agrees, pointing out that some platforms still store passwords on their servers.

"If you can get into the server you can steal the passwords," he says. "Once you have the passwords, you move the bitcoins from one address to another and then people don't have access to those bitcoins."

Hacking the blockchain

All things crypto rely on the blockchain—a chain of code composed of interlocking blocks. It stores the details of all transactions made in cryptocurrency.

Because each block is linked, it is impossible to change a block of code without altering the whole chain—the basis of the security claims made by those who trumpet the benefits of crypto.

However, there is a theory that if a group was to obtain more than 50% of a particular blockchain, it could start rewriting transactions, blocking new ones and double-spending coins.

An exchange called Gate.io alleged it lost $200,000 in an attack like this in 2019, but experts think it would be impossible to target major players like bitcoin.

Such an attack "would be incredibly hard and incredibly energy intensive," says Erica Stanford, author of "Crypto Wars: Faked Deaths, Missing Billions & Industry Disruption."

"With bitcoin now it wouldn't be possible because of how much energy it would use."

Crypto-adjacent crime

Many of the scams around crypto are less to do with the technology and more linked to old-fashioned confidence tricks or extortion where the criminals asked for payment in crypto.

The main family of scams have been Ponzi-style schemes, where a new coin is hyped and its value inflated by the creators, who then dump all their coin when the price reaches its highest point, leaving many investors penniless.

Such frauds, while not unique to crypto, netted $7 billion for scammers in 2019 but dropped massively the following year, according to analysis firm Chainalysis.

"The main scam hasn't been about crypto so much as about using the belief that people will get rich quick to trick people into investing," says Stanford.

She concedes, however, that the newness of crypto and its allure as a get-rich-quick idea has helped the scammers to no end.

The net closes

While cryptocurrencies became notorious for these Ponzi-style schemes, Stanford points out that the high point of the scams was between 2016 and 2018.

She says the market has now matured, people are more knowledgable, law enforcement and regulators are more involved and analytical tools abound, allowing the currencies to be traced.

Chainalysis reported that overall crime related to crypto fell hugely last year.

Stachtchenko points out that many of the major platforms have now ramped up security to combat hackers.

"Some have even bought 'bunkers'—a kind of digital safe," he says.

Valente agrees, saying that monitoring has been ramped up to such an extent that criminals will not be able to spend their crypto even if they hide it for years.

"As soon as the stolen bitcoins start moving again, everyone knows," he says. "Now, almost no company will deal with bitcoins that have been stolen."