Overshadowed by failures, crypto hacking exacts higher price

December 7 2022, by Peter Feltman

Credit: Unsplash/CC0 Public Domain

The cryptocurrency industry is circling the wagons in defense as hackers siphon more money from the sector each year.

Hackers made off with more than $3 billion in digital assets so far this year, according to research firm Chainalysis. In October alone, $718 million was taken in 11 different hacks, making it the worst month in the worst year for crypto hacking, the firm said.

That included $100 million from the largest cryptocurrency exchange in the world, Binance, when its blockchain network, Binance Smart Chain, was exploited.

Experts in academia, crypto exchanges, the research community and the legal industry are speaking out, in the face of increasingly massive losses, to say that hacking does not present an existential risk to crypto as a concept.

Their efforts come as the industry faces more prominent blows—including the bankruptcy filing last month of the FTX exchange and the resignation of FTX CEO Sam Bankman-Fried, a figure who had become a spokesman for cryptocurrency and an influential voice in Washington—and as legislators and regulators struggle to come up with rules. FTX reportedly lent billions of dollars to an affiliated trading business, and now faces several investigations.

In the shadow of FTX and other company failures, the industry is facing a growing hacking problem.

Matthew Green, a professor of cryptography at Johns Hopkins University in Baltimore, said the technology is sound, even if the companies employing it may falter.

"You do not see hacks of bitcoin the currency, and you do not see hacks of ethereum the blockchain," he said during an interview. He noted crypto exchanges that were once big targets for hackers are suffering far fewer hacks than in the past.

"They used to get knocked over all the time," Green said, giving the example of Mt. Gox, which filed for bankruptcy in 2014. At the time, it was the largest crypto platform, and hackers stole about 700,000 bitcoins from its digital wallets, the computer processes used to store crypto.

The industry has adapted and has implemented much better security, Green said.

Hackers naturally look for weaknesses, and they are finding them in decentralized finance. DeFi is a system for conducting financial activity such as borrowing and lending without the need for a traditional central intermediary, like a bank or broker.

DeFi advocates say they offer a way to move currency more quickly than banks, and for lower fees. They have attracted interest and money—as well as powerful adversaries, such as hackers in North Korea. "And these things tend to have a lot of bugs," Green said.

Chainalysis reported in April that 97 percent of crypto stolen during the first three months of this year was from DeFi platforms, a higher figure than the 72 percent in the first quarter of 2021 and the 30 percent in the same period in 2020.

Investment in security

Officials at Coinbase, a large publicly traded crypto exchange, said they are confident in the platform's security. "We've never lost customer funds from our cryptocurrency storage system," chief security officer Philip Martin said. "We are focused on making sure that we are on the absolute cutting edge of security."

But the company's customers have had problems with hackers in the past.

A third party was able to access around 6,000 Coinbase accounts in 2021, and transfer funds to non-Coinbase crypto wallets. Coinbase covered the customer losses.

"While we are not able to determine conclusively how these third parties gained access to this information, this type of campaign typically involves phishing attacks or other social engineering techniques to trick a victim into unknowingly disclosing login credentials to a bad actor," Coinbase wrote to affected customers.

Coinbase spends heavily on security, and about 5 percent of its employees work in this area, Martin said, a level much higher than that of the banking industry. It requires all its customers to use two-factor authentication, which can be a code received via text, a verification app on a cellphone, or even the use of a physical "key" inserted in a phone or computer.

Coinbase is working to educate customers on how to remain safe online, Martin said. Society teaches people not to walk down dark alleys, to lock doors and to keep their wallets out of plain view in cars, he continued. The same need for precaution exists in crypto trading as well, he said. The company stresses the importance of password managers, which make it easy to establish long passwords without the need to memorize or write them down.

In the struggle between hackers and their current target of choice, DeFi, the winner will be clear, according to Erin Plante, vice president of investigations at Chainalysis, which conducts research on the industry.

"The DeFi platforms will definitely win," she said.

Much of the DeFi industry runs on open source code, meaning it is available to the public. Open source has its benefits, since the industry,

and not just hackers, reviews code for weaknesses. But criminals have examined this code and found weaknesses, Plante said.

Plante prefers to call this activity an exploit, instead of a hack, since it works by exploiting computer code.

For example, bad actors have targeted the code to alter smart contracts, she said. These computerized contracts could trigger a payment in cryptocurrency if certain conditions are met.

However, the very nature of blockchain technology, which is the foundation for cryptocurrency, is making it harder for criminals to use any funds they are able to steal, according to Plante.

"The transparency on the blockchain makes it more possible to root out and stop the illicit activity," she said. "There is more ability to trace stolen funds now then ever."

Transparency helped the U.S. government recover the bulk of funds stolen by hackers of Bitfinex, a crypto exchange, years after the funds were stolen in 2016. The hackers stole over 120,000 bitcoins, and the federal government was able to retrieve over 94,000 as of earlier this year, Chainalysis reported.

"It is clear that the permanence of the blockchain contributed significantly to the recovery of assets," the company said in a report. "Law enforcement now has the technology and techniques to keep the industry safe."

Green, at Johns Hopkins, said he is optimistic about what he called an important trend in crypto: the rise in stablecoins. The events here offer both promise and warnings.

Stablecoins are crypto tokens backed by the U.S. dollar, a commodity or another asset. They differ from bitcoin and ether, which don't have such backing. Stablecoins are a key part of DeFi because they allow users to redeem funds in dollars, the currency they will most likely use to buy something.

Stablecoins that are backed by U.S. currency have a good record, Green said, though not all stablecoins are the same and some lack sufficient backing.

One of these, Tether, settled charges in 2021 brought by the Commodity Futures Trading Commission that it did not provide 100 percent backing in dollars or euros, despite claims.

With crypto in the news, especially after the bankruptcy of FTX, calls for action are growing in Congress.

Brian Klein, a lawyer with the Waymaker law firm, urges a methodical approach.

"Recent events have amplified the voices of those calling on Congress to quickly enact legislation," said Klein, who is chair of an American Bar Association annual blockchain and digital currency seminar. "But Congress really needs to understand the industry and the issues. This all needs to be handled in a thoughtful manner and there shouldn't be a rush to legislate."