Explainer: Why are crypto exchanges vulnerable to hacks?

January 29 2018, by Youkyung Lee

A huge advertisement of Bitcon is displayed near a train station in Tokyo Monday, Jan. 29, 2018. Blockchain is a decentralized technology that can make transactions safe and secure, but crypto-currency exchanges that trade bitcoins and other virtual currencies that are based on this technology have been hacked because they are not working on secure networks. (AP Photo/Koji Sasahara)

Blockchain technology can make transactions safe and secure, but crypto-

currency exchanges that trade bitcoins and other virtual currencies that are based on this technology have been hacked because they are not working on secure networks, experts say. Late last week, the Tokyo-based Coincheck exchange reported a 58 billion yen ($530 million) loss of crypto currency due to hacking. The Coincheck exchange has halted trading of the stolen currency, NEM and restricted dealings in most other crypto currencies. It was the second major hacking assault on a Japanese crypto exchange after the Mt. Gox debacle in 2014. Here's a look at the security concerns surrounding crypto currencies.

___

WHAT IS BLOCKCHAIN?

As its name implies, blockchain is a chain of digital "blocks" that contain records of transactions, says Curtis Miles at IBM Blockchain. Each such block is connected to those before and behind it, making it difficult to tamper with because a hacker would need to change the block containing that record and all those linked to it to avoid detection. The records on a blockchain are secured through cryptography and network participants have their own private keys that are assigned to the transactions they make and act as personal digital signatures. Any alteration will make those signatures invalid and alert others in the network to the changes. Blockchains are kept in so-called "peer-to-peer" networks that are continually updated and kept in synchronization. It would require huge amounts of computing power to access every instance of a certain blockchain and alter all its blocks at the same time.

___

POOR SECURITY

While a blockchain can be secure, the exchanges that play a crucial role

in increasing the amount of crypto trading, enabling bitcoin and other such currencies go mainstream, do not use the same technology, says Simon Choi, a director at anti-virus software company Hauri Inc. South Korean exchanges reportedly get poor reviews for cyber security, and officials have said those that fail to beef up such precautions will face fines. "If security on the exchanges' is not secure, their currencies can be stolen," Choi said. "If the exchanges are to play their intermediary role, they should be as safe as banks and strengthen their security."

In this Friday, Jan. 26, 2018, file photo, Coincheck President Koichiro Wada, foreground, bows in apology at the beginning of a news conference in Tokyo. The Tokyo-based Coincheck exchange reported a 58 billion yen ($530 million) loss of crypto currency due to hacking. Blockchain is a decentralized technology that can make transactions safe and secure, but crypto-currency exchanges that trade bitcoins and other virtual currencies that are based on this technology have been hacked because they are not working on secure networks. (Kyodo News via AP, File)

___

RISING HACKS

According to crypto currency research firm Chainalysis, losses of bitcoin, including stealing individuals' holdings through scams, malicious computer software known as ransom ware and hacks, increased at least 30 times to $95 million in 2016 from at least $3 million in 2013.

The attack on Coincheck, which did not affect its holdings of bitcoin, was the second major hacking assault on a Japanese crypto exchange after Mt. Gox, the world's largest bitcoin trading exchange before its collapse, lost hundreds of thousands of bitcoins likely stolen through hacking.

Coincheck has apologized and promised to reimburse customers for their NEM losses. It has pledged to comply with a Financial Services Agency's order to determine why the losses happened, and improve its security to prevent a recurrence.

Details of how the losses happened or who might be behind them are still unclear.

The Mt. Gox case put many Japanese investors off bitcoin, at least for a time, and prompted authorities to impose more regulations. Chainalysis estimates that the bitcoins lost at Mt. Gox were worth $7.5 million at the time the coins were stolen but now worth nearly $10 billion as of January.

In this Friday, Jan. 19, 2018, photo, a man walks past a poster of bitcoin displayed at a retail store in Tokyo. Blockchain is a decentralized technology that can make transactions safe and secure, but crypto-currency exchanges that trade bitcoins and other virtual currencies that are based on this technology have been hacked because they are not working on secure networks. (AP Photo/Koji Sasahara)

IDENTIFYING HACKERS

It's possible to trace blockchain transactions but not to identify the owners of the "wallets" where the crypto currencies are kept, says Choi.

"It's the biggest weakness," said Choi. "You can track the blocks based on the records in the blocks but you cannot tell whose wallet it is. They went to hackers' wallet but if we don't know who the hackers are we

cannot catch them."

The rising hacks have prompted the crypto community to seek ways to halt the bad guys.

South Korea's government is trying to make crypto transactions traceable by implementing a system that links crypto accounts to existing bank accounts that have been vetted by financial institutions. Such efforts however will not help identify hackers if they send crypto currencies to exchanges outside Korea that do not identify their users.