November 21, 2019

VinDAX Is the Seventh Cryptocurrency Exchange Hacked This Year: What Should Investors Be Considering?

On November 5, 2019, Vietnam-based cryptocurrency exchange VinDAX was hacked, losing half a million U.S. dollars' worth of funds spread across 23 different cryptocurrencies.[1] The VinDAX hack marks the latest in a series of cryptocurrency exchange hacks and data breaches that have taken place this year, and is part of a larger and growing trend of digital currency heists that have occurred since Bitcoin, the first cryptocurrency, was introduced in 2008.[2] In July of this year, Japan-based cryptocurrency exchange Bitpoint was also hacked, losing about $32 million in cryptocurrency,[3] and earlier this year, hackers stole $16 million worth of cryptocurrency from New Zealand-based Cryptopia.[4] Losses from cryptocurrency hacks this year alone are reported to have totaled around $1.39 billion worth of assets.[5]

Background

Cryptocurrencies are built on a technology called "blockchain"— a distributed ledger technology in which transactions are recorded across a network of peer-to-peer computers. Since the most well-known cryptocurrency, Bitcoin, together with the underlying blockchain technology, was developed by one or more developers using the pseudonym Satoshi Nakamoto and published in a white paper in 2008,[6] blockchain has been praised for its intrinsic security, as well as qualities that allow cryptocurrency holders to remain largely anonymous. But the same features that have made blockchain an innovative financial technology

[1] Yogita Khatri, *Little-known Asian crypto exchange VinDAX got hacked; lost 'half a million USD' worth of tokens*, The Block (Nov. 8, 2019), https://www.theblockcrypto.com/post/46408/little-known-asian-crypto-exchange-vindax-got-hacked-lost-half-a-million-usd-worth-of-tokens?utm_source=newsletter&utm_medium=email&utm_campaign=2019-11-08.

[2] One of the biggest hacks was of the cryptocurrency exchange Mt. Gox, which resulted in the loss of nearly 850,000 Bitcoins, which were worth around $473 million at the time. *See* Darryn Pollock, *The Mess That Was Mt. Gox: Four Years On*, CoinTelegraph (Mar. 9, 2018), https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on.

[3] Wolfie Zhao, *Bitpoint Exchange Hacked for $32 Million in Cryptocurrency*, CoinDesk (July 12, 2019), https://www.coindesk.com/japanese-exchange-bitpoint-hacked-by-32-million-worth-in-cryptocurrencies.

[4] Josh Saul, *New Zealand Crypto Firm Hacked to Death, Seeks U.S. Bankruptcy*, Bloomberg (May 24, 2019), https://www.bloomberg.com/news/articles/2019-05-24/new-zealand-crypto-firm-hacked-to-death-seeks-u-s-bankruptcy.

[5] By comparison, in 2018, six crypto exchanges were hacked, with losses of approximately $865 million. *See* Eric Larcheveque, *2018: A Record-Breaking Year for Crypto Exchange Hacks*, CoinDesk (Dec. 29, 2018), https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks. 2017 saw only three hacks of cryptocurrency exchanges. *See* Eric Larcheveque, *2018: A Record-Breaking Year for Crypto Exchange Hacks*, CoinDesk (Dec. 29, 2018), https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks.

[6] https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf

also make cryptocurrencies an attractive target for theft; once stolen, the nature of blockchain technology makes it extremely difficult to trace the culprits and track down the stolen assets.

Cryptocurrencies generally are based upon a system that uses a public digital key, which is used for identification (similar to a bank account number), and a private digital key (similar to a personal identification number to access that account), which is used for encryption and authentication. The other component of the system is the wallet, which stores cryptocurrencies. Each wallet has a unique address, which is used for sending and receiving funds. A user starts with an address, which in turn generates a private key and a public key using an algorithm; the private key grants the user ownership of the funds at a specified address. When sending funds, the system software identifies the transaction with the private key (without disclosing it), which validates for the benefit of all on the relevant network the authority of the user to transfer the funds from its address (which it does by generating a unique digital signature for every transaction a user undertakes). The public key, which is the public address for the wallet (in effect the address is a representation of the public key) and is intended to be shared, is derived from the private key (that is, the private key generates the public key). At the heart of the cryptography system is the one-way aspect of these components: the public key cannot be derived from the address, and the private key cannot be derived from the public key.

Experts say that one of the safest ways to "store" cryptocurrency is by using what is known as a "hardware wallet."[7] This is an off-line device like a thumb drive, in which a user's private keys are stored. These devices often require passwords, backed by sophisticated encryption systems, and multi-factor authentication procedures in order to gain access to the private keys stored on them. (These devices do not store cryptocurrency assets themselves, but rather the private keys associated with the cryptocurrency assets in the blockchain system.) The problem with this system is that it is cumbersome. Accessing funds requires having the hardware wallet on-hand, and then engaging in a lengthy process of opening up the hardware wallet and gaining access to the private keys stored in the wallet. This can make it hard to respond quickly to the highly volatile cryptocurrency marketplace.

The solution to which many resort is keeping their funds on the exchanges they use to buy and sell cryptocurrency (examples include Coinbase, Bittrex and CEX.io). However, since the cryptocurrencies themselves are not actually on the exchanges, what this technically means is that the users are storing their private keys on the exchange. The exchanges therefore act as warehouses of private keys associated with hundreds of millions, and often billions, of dollars in cryptocurrency assets. Not surprisingly given the concentration risk, these exchanges have increasingly become a favorite target for high-value hacks.

Cryptocurrency hacks not only result in significant loss of personal holdings; they also create wild fluctuations in cryptocurrency markets. After a $37 million hack of the Korean exchange Coinrail in 2018,

[7] Lily Hay Newman, *How to Keep Your Bitcoin Safe and Secure*, Wired (Nov. 5, 2017), https://www.wired.com/story/how-to-keep-bitcoin-safe-and-secure/.

Bitcoin (the first, and most popular cryptocurrency) lost approximately 11% of its market value.[8] A similar drop occurred after hackers stole 120,000 Bitcoins from Hong Kong-based exchange Bitfinex in 2016.[9]

In light of the increasing number of cryptocurrency exchange hacks in recent years, companies that invest in cryptocurrency projects or have significant holdings in cryptocurrencies should keep the following in mind:

What should companies with significant holdings in cryptocurrencies be considering?

Due diligence

Companies considering investing in cryptocurrencies may want to undertake a thorough due diligence analysis of the cybersecurity measures, response protocols, and access controls for their preferred method of storing their private keys, whether that method involves using an exchange, a hardware wallet, or some other method.

Companies may also want to engage outside counsel or retain in-house expertise to advise them as to their legal obligations for how they store their private keys. For example, companies may need to determine whether applicable SEC laws and regulations require the use of a qualified custodian for holding private keys, as well as their obligations for instituting specific controls and response procedures for protecting against the loss of clients' assets.

Use offline or hardware wallets

As discussed above, there are few safer ways to secure cryptocurrency assets than using a hardware wallet for maintaining private keys. While these hardware wallets are commercially available, large investors may consider instead engaging computer engineers that can build custom hardware wallets. Similarly, as discussed above, companies may want to consider engaging a reputable, insured, qualified cryptocurrency custodian service for storing private keys.

What should companies that are investing in cryptocurrency businesses be considering?

When investing in a cryptocurrency exchange project, invest heavily in cybersecurity.

Cryptocurrency users have many exchange options, and they tend to be fairly discriminating about which they choose to use based on the exchanges' reputations for cybersecurity and history of cyber penetrations.

[8] *Bitcoin tumbles as hackers hit South Korean exchange Cointrail*, Reuters (June 11, 2018), https://finance.yahoo.com/news/south-korean-exchange-coinrail-says-hit-hackers-bitcoin-035951568.html/.

[9] Stan Higgins, *The Bitfinex Bitcoin Hack: What We Know (And Don't Know)*, Coindesk (Aug. 3, 2016), https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know.

A new cryptocurrency exchange will need to earn a reputation for integrity and cybersecurity in order to attract users (unless, as is sometimes the case, the exchange offers certain desirable cryptocurrencies that are not available on other available exchanges). Nothing will cripple a new cryptocurrency exchange faster than a successful cyber penetration, and the short history of cryptocurrency is rife with now-defunct exchanges that either went bankrupt and/or lost all user confidence after a cyberattack.

If your company is contemplating investing in a cryptocurrency exchange project, robust cybersecurity should be considered. This includes not only technical cybersecurity measures, but also robust cybersecurity policies, compliance and reporting mechanisms, and audit controls. Capable in-house expertise or outside firms can help you develop these procedures, and your company may want to secure this expertise well before your project launches.

When investing in a cryptocurrency blockchain project, develop cyber penetration response policies in advance.

As discussed above, most cryptocurrency hacks do not compromise the blockchain itself, but the exchanges where the transactions occur and the private keys are stored. These hacks can devastate the cryptocurrency market. But a cryptocurrency blockchain or platform can itself be compromised, and when this happens, having the right response procedures in place is critical.

An example of this was seen with Ethereum—a blockchain-based smart contract[10] system that used the cryptocurrency "Ether" to compensate the operators of the computational engine that powers the blockchain system and as a medium for the exchange of value for the performance of smart contracts. In 2016, an organization called The DAO[11] developed a smart contract system built on the Ethereum platform designed to facilitate venture capital fund investment. Hackers exploited a flaw in that smart contract system, resulting in the theft of $50 million worth of Ether. A vote was held within the Ethereum community about how to respond to the hack, with a majority voting to do a "hard fork"[12] of the Ethereum blockchain. Since the blockchain represents a history of all transactions since its inception, a "hard fork" is effectively a way to reverse time by erasing the history of the transactions on the blockchain system since the occurrence of the compromising event (hard forks can also be planned events so the rules and protocols governing the blockchain can be updated). This hard fork was extremely controversial within the Ethereum

[10] A smart contract is a blockchain-based protocol designed to facilitate and enforce performance of a contract.

[11] The DAO was a venture capital fund founded by a group of developers trying to automate venture capital investment by facilitating crowd-sourced decision-making for the projects in which The DAO would invest. *See* Cade Metz, The Biggest Crowdfunding Project Ever—the DAO—Is Kind of a Mess, Wired (June 6, 2016), https://www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess/.

[12] When a hard fork occurs, the blockchain splits into two separate blockchains starting from a predetermined period in the history of the transactions recorded on the blockchain. Usually what happens is that both blockchains will include the historical transactions that occurred before that predetermined period, but the old blockchain will also include the subsequent transactions in the original blockchain while the new blockchain will only include transactions that occur after the forking event.

community because it resulted in the reversal of both legitimate and illegitimate transactions, and the value of Ether and confidence in the Ethereum platform temporarily suffered as a result.

One of the reasons The DAO hack was so disruptive to the Ethereum community was because of the debate that ensued within that community over how to respond to it. Thus, companies considering whether to invest in a cryptocurrency project should consider not only how to gird their projects against technical hacks, but also how to develop and disseminate response policies that would give users assurance that the cryptocurrency project would commit to a predictable, controlled course of action in response to various compromising events.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Roberto Finzi
+1-212-373-3311
rfinzi@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Manuel S. Frey
+1-212-373-3127
mfrey@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Jonathan Ashtor
+1-212-373-3823
jashtor@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Daniel J. Klein and Apeksha S. Vora contributed to this Client Alert.