PiperAlderman

Article Information

Author: Michael Bacina
Service: Blockchain

$1B lost: the 5 biggest cryptocurrency fails of 2017

2017 was a stellar year for cryptocurrency valuations in general and Bitcoin in particular. On 1 January 2017 the USD$ value of a Bitcoin passed USD$1,000 and one year later on 1 January 2018 the price was USD$13,700.

2017 was a stellar year for cryptocurrency valuations in general and Bitcoin in particular. On 1 January 2017 the USD$ value of a Bitcoin passed USD$1,000 and one year later on 1 January 2018 the price was USD$13,700.

On 17 December 2017, Bitcoin reached an all time high price of $19,783.

But it hasn't been plain sailing for the crypto ecosystem with a number of security breaches and exploits in 2017 showing how vulnerable operations can be to malicious actors.

The total value these hacks and fails on 1 January 2018 prices is just shy of **USD$1 billion**, an eye-watering USD$978M.

Amid all the excitement of prices soaring, the opportunity cost of cryptocurrency theft is significant and it is worth looking back over the following multimillion dollar hacks and failures as we go into the new year.

No. 5: Coindash

In July 2017, I wrote about Coindash, an Israeli based company, which ran an ICO to fund the development of a social cryptocurrency portfolio platform.

Unfortunately, the Coinspot website was compromised, likely well before the ICO, and those responsible made code alterations which randomly changed the Ether address where ICO participants were contributing funds (switching between a legitimate address and a fraudulent one).

As a result of this hack, more than half the funds being raised in the ICO were diverted to a rogue Ether address. The ICO was suspended while the rogue address was removed.

The total amount stolen was then USD$7.9M in Ether, worth approximately USD$31.5M on 1 January 2018.

Despite these troubles, the value of CDT, the token issued, was 4 times the issue price on 4 January 2018.

The lesson from the Coindash hack is that close attention to detail for all aspects of security are needed when running an ICO.

No. 4: Veritaseum

In May 2017 Veritaseum completed an ICO, aiming to build a peer-to-peer platform for trading without the need for brokerages, traditional exchanges or banks. It is not known how much was raised in the ICO.

But only one month later, in July 2017, the founder of Vertiaseum, Reggie Middleton, posted in the Veritaseum Slack group that hackers had stolen 36,000 VERI tokens at the time worth approximately USD$8.7M (USD$32.5M as at 1 January 2017).

Middleton claimed that the hackers defeated two factor authorisation on two different accounts and "fineggeled 3rd

parties security (sic)". The sale of the stolen VERI tokens for Ether caused a flash crash in the price of VERI and a substantial (USD$80 or so) drop in the price, which has only recovered in late 2017.

If Middleton's comments are true, then even with multiple security layers, the business was still exposed to a determined hack.

While there is no indication that the Vertiaseum hack was an inside job, it would be a very determined hacker to break through two factor authentication protocols.

No. 3: Parity Wallet Hack

On 19 July 2017, Parity Technologies, a provider of multi-signature cryptocurrency wallets, announced a critical security flaw and that 3 wallets had been drained of over 150,000 Ether, then valued at USD$32M, and worth almost USD$120M as at 1 January 2018.

Multi-sig wallets are a form of smart contract code. When a person wants to use a multi-sig wallet, they deploy the code on the Ethereum blockchain and set the owners for the wallet and deposit funds into the wallet. The benefit of the multi-sig wallet is that it requires the co-operation of multiple parties to unlock, giving additional security (in theory).

The incident was caused by a bug in Parity's wallet code, which had not been discovered by audits of the code. The issue was that the code referenced a common library of code which is used for every parity wallet. This is done for efficiency buy creates a centralised vulnerability in the code as smart contracts cannot be modified once deployed. As such, when the bug was discovered, it affected all parity wallets.

What was surprising to many, is that 596 wallets were affected by the same vulnerability, but the hackers only targeted 3 wallets. A White Hat Group moved in quickly, exploiting the same bug to move at-risk funds from the remaining 593 wallets. Those funds were all restored to their owners once the bug was fixed.

Parity has instituted a bug bounty program in addition to their code audits. The lesson from the Parity wallet hack is how vulnerable computer code, particularly using libraries of functions, can be to a malicious actor.

Parity also updated all of its wallets on 20 July, but that created a further vulnerability…

No. 2: Nicehash

Nicehash claims to be the largest crypto mining marketplace, allowing users to sell spare computing power to those wishing to apply that to create hashing power for cryptocurrency mining, earning cryptocurrencies in the process.

On 6 December 2017, Nicehash reported that their systems had been compromised and the contents of their Bitcoin wallet had been stolen. A wallet address was confirmed by Nicehash CEO, Marko Kobal, to show the stolen funds.

The total theft was worth about USD$67M at the time, and appears to have been cashed out for about USD$80M just prior to Bitcoin's pre-christmas price slump. The 1 January 2018 value of the stolen Bitcoin is USD$64M.

In an interesting twist, Nicehash has set up a Reddit community /r/NiceHashHack to provide updates on the hunt for the stolen funds.

The hackers used over 3 million transfers of the original stolen Bitcoins to seek to launder the money and Nicehash say they have contacted the major exchanges.

Limited information is available about the details Nicehash hack other than rumours of the hackers being possibly linked to North Korea and a Nicehash computer being compromised. The Nicehash hack shows once more the vulnerabilities inherent in storing cryptocurrencies in hot wallets which are controlled by others.

No. 1: Parity Wallet Frozen Funds

Following their embarrassing hack on 19 July 2017, on 20 July 2017, Parity updated their multi-sig wallets to address the vulnerability exploited. Unfortunately this left a further vulnerability in the wallets.

On 6 November 2017, a person first calling him or herself "devops199" and then later "ghost" on Github discovered that a common element of code in all of the Parity wallets, a library of functions (for the non-developers, think of this as a kind of glossary referred to by the wallet) could itself be initialised as a wallet itself and the ownership could then be transferred.

Part of the design of a smart contract includes "kill" code, which enables a contract to reach an end and cease functioning. devops199 initialised the library as a wallet to claim ownership of it and then ran the "kill" command. This had the immediate effect of freezing all Parity wallets, permanently.

Devops199 posted messages claiming "i'm not malicious" and "i'm an Eth learner". The Guardian provided this fantastic analogy:

> Effectively, a user accidentally stole hundreds of wallets simultaneously, and then set them on fire in a panic while trying to give them back.

However, some are not convinced this was an accident, saying that devops199 tried to transfer ownership of frozen wallets after running the "kill" command.

Parity have now confirmed that 584 wallets are effected. At the time of the freeze, approximately 947,000 Ether was frozen up, worth then USD$300M and with an approximate value of USD$732M as at 1 January 2018.

Amazingly, despite almost 1% of all Ether being frozen, the price of Ether did not fall, as it did when the DAO Hack of 2016 occurred. Rather the price of Ether has continued to climb.

Takeaways

The above represent just the biggest and high profile losses and fails suffered in the cryptocurrency ecosystem in 2017. The common thread between them is diligence, or more accurately and absence of diligence.

Unfortunately the popularity of agile software development and a culture of "move fast and break things" in the start-up community stands in contrast to the standards required of smart contracts and crypto security which demand levels of coding perfection more akin to airline or NASA missions. There can be not hotfixes at 30,000ft or in orbit, and once a smart contract is deployed, it cannot be changed.

Whether it is auditing and testing code, or locking down systems with tight security, in cryptocurrency the price of crypto wealth is eternal (security and code) vigilance.

DISCLOSURE: The author holds a range of cryptocurrencies and acts for and advises cryptocurrency clients on legal matters. None of the above should be construed as legal or investment advice.