the Availability Digest

www.availabilitydigest.com

$280 Million in Cryptocurrency Lost Due to Bug

November 2017

Almost $300 million of cryptocurrency has been lost. However, the money wasn't deliberately taken. It was destroyed by accident. A series of bugs in a popular digital wallet service led one developer to accidentally take control of and then lock up the funds.

Ethereum and the Ether Token

A 'cryptocurrency' is a form of a digital asset created through a combination of encryption and peer-to-peer networking. It's transactions are recorded in a blockchain. The cryptocurrency that was lost was Ether tokens. Ethereum, using the Ether token, is now the second largest cryptocurrency after Bitcoin. Ether is the tradeable currency that fuels the Ethereum distributed application platform.

The lost Ether tokens were kept in digital multi-signature wallets. These wallets require more than one user to enter their key before funds can be transferred from the wallet.

The Parity Wallets

The wallets had been created by a developer calling himself 'Parity.' In July, 2017, Parity lost $32 million in Ether due to a bug in its wallet code. The vulnerability allowed users to become the owners of wallets that did not belong to them. This bug allowed Ether to be drained by hackers from three of Parity's wallets to other accounts. However, the money was returned to Parity, and Parity was encouraged to do a security audit of the Ethereum code.

As Parity was fixing this bug in its wallet, it inadvertently left a second flaw that allowed one user to become the sole owner of every single multi-signature wallet created by Parity. A user, 'devops199', triggered the flaw by accident, giving him possession of $280 million in Ether tokens. When he realized what he had done, he attempted to undo the damage by deleting the code that had transferred the funds. However, this action simply locked all the funds permanently in the multi-signature wallets. $280 million were now frozen, and users were unable to move their funds from these wallets.

Experts predicted that this loss was roughly 20 percent of the entire Ethereum network.

In a blog post, Parity wrote "It would seem the issue was triggered accidentally on Nov. 6, 2017, and subsequently a user suicided the wallet, wiping out the library code, which in turn rendered all multi-signature contracts unusable." That meant that no funds could be moved out of the multi-signature wallets.

A Hard Fork?

The head of security for the Ethereum Foundation says that a 'hard fork' of the blockchain containing the the Ethereum transactions is the only way to rectify the situation. A hard fork means creating a separate version of the network. This would undo the damage by asking 51% of the currency's users to agree to pretend that the transfer never happened in the first place. But for this to happen, at least 5!% of Ethereum's users need to agree to the hard fork.

Some users in the Ethereum community are pushing for a hard fork. However, others in the same community are refusing to accept the change. This would result in a split of the community into two parallel groups, one with the recovered $280 million in Ether tokens and one with the tokens frozen and inaccessible.

Summary

This incident reflects a hidden problem with cryptocurrencies such as Bitcoins and Ethereum. If something goes wrong, it may be impossible to fix because there may not be a common consensus as to how to proceed. Different users in the community may have different interests. For instance, in this case, some users will feel that the value of their Ether tokens may substantially increase if $280 million of Ether tokens suddenly disappeared.

Acknowledgements

Information for this article was taken from the following sources:

'Accidental' bug may have frozen $280 million worth of digital coin ether in a cryptocurrency wallet, *CNBC*; November 8, 2017.
'$300m in cryptocurrency' accidentally lost forever due to a bug, *The Guardian*; November 8, 2017.
£200 million worth of digital cryptocurrency is wiped out as bungling developer locks investors out while trying to stop hackers, *Daily Mail*; November 8, 2017.
How Ethereum lost $300 Million Dollars, *Hacker Noon*; November 9, 2017.