Bitcoin users largely shrug off latest $69m Bitcoin exchange heist

5 August 2016, by David Glance

Bitcoin. Credit: https://freeformers.com/uncover-digital-bitcoin-blockchain-blog/

Hong Kong Bitcoin exchange Bitfinex announced that it had been hacked and 119,756 Bitcoins stolen which at current prices represents nearly US $69 million. Bitcoin prices dropped 20% after word of the hack became public but the price has since recovered.

It is not clear how the hackers were able to get hold of the cryptographic keys that protected the stolen Bitcoins. Bitfinex had instituted a new way of protecting its accounts that involved multiple signatures, one of which was held by BitGo, the creators of the system that was supposed to keep the Bitcoin accounts safe from exactly this type of hack.

The hack is the second largest in a long line of hacks that have targeted Bitcoin. The biggest hack was that of Mt Gox in which 744,408 Bitcoin were stolen over a 2 year period. All of the hacks have essentially targeted Bitcoin's main weakness which is how to store the details of the Bitcoin accounts safely.

A Bitcoin account is actually a cryptographic private key which links back to transactions on Bitcoin's blockchain. If the private key is lost, so are the Bitcoins that were associated with it. Likewise, if someone steals the private key, they have access to all of the Bitcoin that are associated with it.

Keeping the private key associated with Bitcoin safe has proved a challenge. The safest place for a private key is in "cold storage" somewhere that is not attached to the Internet. This means potentially on a USB drive or in specialised encrypted devices called hardware wallets. The simplest way is to simply write the number down on a piece of paper.

With all of these solutions, keeping them safe from being lost or damaged is still an issue. Devices and USB drives can also fail raising the possibility of losing the information stored on them. There is also the issue that at some point, they have to be connected to a network to access the Bitcoin and at that point, they could be compromised.

For exchanges, the issue with storing Bitcoin in cold wallets is that it limits their customers' access to funds and so exchanges always keep a certain quantity of Bitcoin in "hot wallets". Bitfinex and BitGo had trumpeted the security of their multi-signature protection of customers' wallets but according to other exchanges that are also using multi-signature mechanisms, it might have been the way Bitfinex had implemented their specific version of the system that was at fault.

What is remarkable is that despite the magnitude of the hack, the Bitcoin price has started recovering and everyone not directly involved in the loss of Bitcoins have carried on as if nothing had happened. It is possibly a testament to the completely decentralised nature of Bitcoin that problems like this are considered to be isolated issues and not systemic problems. Loss of Bitcoins is treated in the same way as the potential loss in value of the currency that occur on a daily basis through its ongoing volatility.

It also indicates that the demand for Bitcoin is still robust because not only has it shrugged off hacks of this type but it seemingly has not reacted negatively to the "halving" of the reward given to Bitcoin miners that occurred in July. There was an expectation (including my own), that the halving would have made the economics of mining even more unfavourable. In the past few months however, Bitcoin's price has rallied partially mitigating this effect.

It is worth stressing that the vulnerability exploited by the hackers was not associated with Bitcoin's underlying blockchain technology as some seem to have suggested. At the time of preparing this article, Bitfinex was still offline with no indication of what the problems were that led to the hack. Whether customers flee the site when they are allowed to access funds or not is yet to be seen. To everyone else though, this is just another day in the never dull world of cryptocurrencies.

This article was originally published on The Conversation*. Read the* original article*.*

Source: The Conversation

APA citation: Bitcoin users largely shrug off latest $69m Bitcoin exchange heist (2016, August 5) retrieved 30 November 2020 from https://phys.org/news/2016-08-bitcoin-users-largely-latest-69m.html