Bitcoin's popular design is being exploited for theft and fraud

May 17 2017

The very design features that make Bitcoin technology appealing to its users are also weaknesses being exploited for the theft of the cryptocurrency – new research reveals.

The blockchain technology on which Bitcoin is based is decentralised, pseudo-anonymous and unregulated and therefore attractive to many of its users. It offers alternatives to, what many users consider to be, key weaknesses of traditional models - where banks act as trusted third parties to mediate financial transactions.

Traditional bank transactions can incur high fees, can be slow, and transactions can also be approved or reversed by banks even if contrary to a contract between the trading parties. In comparison, due to its open ledger design, blockchain is transparent, fast, cost-effective, and also intentionally provides irreversible transactions.

These transparent design features are supposed to promote trust in Bitcoin. However, computer scientists at Lancaster University and Universiti Teknologi MARA (Malaysia) show that these features are presenting opportunities for fraud– undermining trust in the currency.

Problematic Bitcoin design features include:

The risk of losing a password – a lost or forgotten password cannot be recovered so all bitcoins from an electronic wallet could be rendered unrecoverable.

Insecure passwords can lead to bitcoins being stolen – for example through phishing scams.

The irreversible nature of transactions means that stolen bitcoins diverted to another wallet, due to hacking or dishonest trading partners, cannot be reversed and recovered.

The anonymous nature of bitcoin users, and their unknown reputations, opens up opportunities for dishonest traders to scam during transactions.

Dr Corina Sas, Senior Lecturer at Lancaster University's School of Computing and Communications, said: "The main trust challenge experienced by Bitcoin users is the risk of insecure transactions and in particular that of dealing with dishonest traders.

"The design features that make Bitcoin popular are also enabling dishonest trading. For example, irreversible transactions are an issue when a trader does not fulfil their side of a transaction – by paying an agreed price in conventional currencies, or goods, for bitcoins. If this happens, then honest traders are not able to recover their bitcoins.

"Our findings also uncover an interesting tension. Despite deregulation being a crucial characteristic of blockchain, its users actually desire regulation, mostly because of the challenge of dealing with dishonest traders which, they believe, could be addressed by de-anonymising trading parties. Bitcoin provides freedom over one's assets, but at the same time it no longer provides the security that traditional regulated financial institutions provide."

The researchers, who interviewed 20 Bitcoin users, have suggested design improvements to support trust:

New digital tools to record information on conventional currencies

exchanged for bitcoins on the blockchain. Currently only the transfer of Bitcoins is recorded, and the offline transfer of fiat currency or goods is not, opening up opportunities for fraud.

A reputation management system built on top of the blockchain would motivate traders to keep the same wallet to build their reputation, providing more stable, though still private, identities.

New tools to reveal the identities of the owners of one-use only Bitcoin wallets, to deter dishonesty

The use of third parties to arbitrate and sign-off transactions.

More information: Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems , DOI: 10.1145/3025453.3025886

Provided by Lancaster University