The blockchain could have better security than the banks

July 17 2017, by Timothy Mccallum And Luke Van Der Laan

There are ways to improve the online ledger blockchain by taking some

security notes from banks. If people could use both two-step verification and spending limits on the blockchain, this would reduce any economic loss from cyber attacks and in turn encourage more users.

The blockchain is a global network of computers that run the same blockchain software. Transactions on the blockchain are currently limitless and there is no one governing body. Introducing security measures could demonstrate a level of predictability in the blockchain that could build more trust.

At the moment there are third-party sites that perform transactions with the blockchain on your behalf. They are owned and managed separately from the blockchain itself, and this presents a single point of failure.

These sites, like Kraken, Changelly and Shapeshift, allow people to purchase, as well as exchange, blockchain assets. Activity on these sites includes purchasing Bitcoin with US dollars or exchanging Bitcoin for Ethereum assets.

Current flaws in the system

The blockchain ecosystem is by no means perfect. Many people shy away from using it due to its perceived volatility. There is no "code of conduct" protocol for the blockchain at the moment and it's likely there never will be.

In addition, creating and maintaining blockchain software is arduous and managed by only a few people globally. These software developers, who are the trailblazers of this technology, are being disadvantaged by constantly being forced to respond to malicious attacks.

There have been many malicious attacks on the blockchain including the very recent attack on a third-party online wallet. In this attack, an

unknown user was able to hijack the third-party site and redirect all transactions to their account.

These and other malicious attacks have made blockchain assets either temporarily unavailable or permanently unrecoverable. It's for these reasons that the solution to secure the blockchain can't be owned and managed by third-parties, and must be part of the blockchain itself.

Security measures like the ones we're proposing may reduce the severity and speed of any malicious attacks. Lowering the bounty for malicious attacks could also prove to be a disincentive for this behaviour.

Bank style security for blockchain

The mechanisms we use to build trust in the traditional financial institutions could be coded into the blockchain.

It's unlikely that a blockchain user will use the technology to spend 100% of the assets in their account, with no notice whatsoever. This is why hacks of these accounts are so obvious, just as they would be if your bank account was suddenly drained.

Adjustable spend and transaction limits currently protect mainstream bank account users from one malicious transaction. There is no reason the same kind of consumer protection cannot apply to cryptocurrency users.

In order for this to work, the blockchain needs to verify that you are the legitimate user of the account, who is wanting to raise and lower spending limits for the purpose of transferring funds.

We propose this could work via voice authentication. This is where a blockchain user performs a transaction on the blockchain and is

subsequently prompted to provide a single-use vocal passphrase – this is the second step in the two-step verification process.

This would be similar to the program Captcha, but with one unique twist. Captcha is designed to discern legitimate users of the internet from online robots. It works by generating a one-time image of letters and numbers that the user has to type correctly to proceed. Captcha can verify if you are human, but is unable to verify your individual identity.

Using the human voice with this type of technology could be more commonplace in the future. It's also less complex than other types of biometric verification, which require sophisticated infrastructure such as retina- and iris-scanning hardware.

More importantly, the human voice shares blockchain attributes. Your voice and your public blockchain key are both public and unique.

At present there is no guarantee of holding blockchain assets without disruption of some kind. Providing security in the blockchain would convert into a degree of predictability in the technology. If this was shown to work in the long term, it would also create trust.

Obviously, we trust traditional currencies. For example, laws provide a promise that a $20 note will result in a mutual exchange of goods and services to that value. So once a degree of predictability is established in a blockchain, there will also be new business opportunities from traditional markets, such as insurance in case of sudden undue economic loss.

It's in the interests of the majority stakeholders of blockchain to consistently look for responses and improvements that reduce the limitations of the technology. A malicious attack, intent on bringing down the architecture of blockchain technology, would unfairly relegate

the blockchain to a history as another ponzi scheme.

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

Provided by The Conversation

Citation: The blockchain could have better security than the banks (2017, July 17) retrieved 23 April 2024 from https://phys.org/news/2017-07-blockchain-banks.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.