The blockchain does not eliminate the need for trust

November 16 2017, by Dirk Baur And Niels Van Quaquebeke

Credit: AI-generated image (disclaimer)

A common idea about the blockchain, the technology that powers Bitcoin and other cryptocurrencies, is that it can "create trust", or allow two parties to make a transaction "without relying on trust".

If true, this means we could create a world without a trusted "man in the

middle". We could have financial services without a bank verifying transactions and we could transfer ownership (of a house, for instance) without a lawyer. But this idea is wrong.

The blockchain does not create or eliminate trust. It merely converts trust from one form to another. While we previously had to trust financial institutions to verify transactions, with the blockchain we have to trust the technology itself.

It is also not clear that a blockchain-powered currency (such as Bitcoin) can go mainstream without the backing of a trusted authority. In fact there are hardly any examples of money (including gold) that have ever worked without the backing of a central authority or a sovereign.

When you make a traditional money transfer the bank will first verify that you have sufficient cash, and then debit your account and credit the recipient. Think of the blockchain as a decentralised version of this process. Rather than all of this information being held and verified by the bank, it is done on an "open public ledger".

When someone transfers a Bitcoin, it is verified by "miners" (really powerful computers), then encrypted, and a "block" is added to the ledger.

Because all of the verification is done by the system itself, the idea is that users do not need a trusted central authority. Instead, trust is transferred from one central authority (such as a bank) to many decentralised, anonymous participants (the miners).

But here lies the problem – users must trust the technology and the governance of the system.

What is trust?

In economic exchanges there are three kinds of trust: institutions-based, characteristic-based, and process-based.

Institutions-based trust comes from the involvement of a central authority. Think of a commercial bank (and a government insuring deposits in that bank), as in the previous example.

Characteristic-based trust is the trust we have in people mostly because they represent some sort of similarity to us, or show admirable features or values that warrant trust. For example, you are more likely to trust someone from the area where you grew up than someone from elsewhere; you might also trust someone with a similar taste in music, or who simply embodies what you value in life.

Process-based trust arises when previous experiences suggest that the inputs by one party will be predictably reciprocated. This trust often evolves into social micro-rules or norms. For example, most people would generally trust that if they do not harm a person, that person will also not harm them. Likewise, one would trust that others will answer when asked a question.

It follows that trust can be destroyed and lost if the central authority fails, the person you trusted fails, or the process you trusted fails.

When it comes to the blockchain specifically, we can see that there are at least two forms of this trust at play. Because of its complexity many people may find it difficult to trust the process.

But some may choose to trust it when like-minded people use it (characteristic-based trust). Indeed, friends of or nerds in the same sphere as Vitalik Buterin, the founder of the Ethereum cryptocurrency, likely became early adopters of the technology.

Yet, a different kind of trust may also be at play. For instance, when the Ethereum-powered decentralised autonomous organisation (DAO) was hacked, users asked Buterin to respond. This shows that people still need a central authority or will appeal to one if the system fails. Likewise, the fake news that Vitalik had died led to US$4 billion dollars being wiped off the market value of Ethereum. With the assumed loss of the central authority, many also lost their trust in the underlying system.

This may not be ideal but a truly open public blockchain (that is, one without any central authority behind it) is unlikely to work.

Analysis of the evolution of money shows that almost all currencies throughout history have had the backing of an authority. This is easy to understand. Think of a raw gold nugget. To be sure about its value you would need to trust a jeweller - a valuation authority. Because this process of identifying the quality of gold takes time, raw gold is not the ideal medium of exchange.

This problem with gold was largely resolved by the creation of the mint. In other words, the minting and standardisation of gold coins reduced the identification costs and thus the need to trust decentralised third parties such as the jeweller. Instead, there was now a need to trust a central authority – the mint.

You also need to trust that the government will accept tax payments in the minted gold coins, and that other people will take the coins as payment for goods and services. More generally, if people lose trust in the authority and the value of a currency, they will try to sell the currency, leading to inflation or even hyperinflation.

All of this shows that gold and any other form of money – including cryptocurrencies – are not "trustless".

The importance of the trusted central authority can also be understood in the case that a currency is destroyed. For example, when the Roman empire fell, the central authority collapsed and so did the currency it backed. Process-based trust collapsed as well, which shows that the process only worked because of the institution.

If history is any guide, privately created money such as Bitcoin or any other blockchain-based currency is unlikely to become globally accepted without a trusted central authority. This means that an "open" blockchain will not succeed.Although a "closed" blockchain, with the backing of a central authority, might work, it would be very different to the core feature of Bitcoin and the blockchain—decentralization.

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

Provided by The Conversation

Citation: The blockchain does not eliminate the need for trust (2017, November 16) retrieved 18 April 2024 from https://phys.org/news/2017-11-blockchain.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.