Bitcoin's central appeal could also be its biggest weakness

July 7 2017, by Corina Sas

Credit: AI-generated image (disclaimer)

Bitcoin reached a huge new peak in value in June 2017, when one unit of the virtual currency was worth US$2,851 (£2,208), up from around US$600 just a year earlier. More than 10m people worldwide are now thought to own bitcoin and more than 100,000 merchants accept it for goods (not counting all those using it to sell drugs and other illegal items

on the black market).

Part of bitcoin's appeal for many of its users is the lack of centralised control or regulation by any government or bank. Instead it relies on a technology known as blockchain to underpin and secure transactions. But research my colleagues and I have conducted suggests that the lack of any social trust in the way blockchain operates poses a challenge for bitcoin's further spread.

Blockchain is a public database that records digital transactions. These are validated by computers working within a worldwide network that solve complex coded problems. Whereas traditional bank transactions are authorised by financial institutions and controlled by governments through taxation and contracts between parties with known identities, blockchain is decentralised, unregulated and anonymous.

In our studies of blockchain's users we found that these features appeal to bitcoin users because of increasing distrust of financial institutions and governments. The technology empowers people to regain control over their money, with no restrictions over where and when they can send it.

But our findings also indicate that two core aspects of blockchain's design – the fact that transactions are anonymous and irreversible – pose significant challenges to the social trust among its users. Anonymity has an obvious appeal for people looking to avoid government control. And irreversible transactions were built into blockchain's original design as a positive feature to address banks' privilege of reversing transactions, even when the contract states that they were final.

But in practice, these features are a problem for many people. Most people are used to relying on the reputation of a seller to decide whether or not to buy from them – and the ability of the financial and legal

system to help them if something goes wrong. But neither of these things are possible through blockchain.

Paper trails have their advantages

Most transactions don't just involve moving bitcoin from one electronic wallet to another. In practice, they are often part of a larger, two-way transactions where both parties send and receive assets such as bitcoins, real world currency or physical goods.

The issue is that the blockchain only records the movement of bitcoin, not the movement of other currencies or goods. Because there is no authority to complain to, this raises a major risk that users could fall prey to dishonest traders who fail to deliver their side of the deal.

In our latest study, we interviewed 20 bitcoin users recruited from five online groups from Malaysia, most of them with more than two years experience of using bitcoins. Our research indicates that more than 50% of participants would prefer blockchain's transactions to be regulated and identifiable, so that transactions can be either reversed or the dishonest trader legally sanctioned.

This shows there is a tension between the freedom and empowerment of blockchain's unregulated nature, and the lack of security that most people are accustomed to receiving from traditional financial institutions. If this is not addressed, such tension may limit the spread of bitcoin beyond its current base. It could even reduce the number of bitcoin users involved in such two-way transactions, as more people become aware of the risks of dishonest traders. In contrast, the use of blockchain for one-way transactions such as remittance payments will continue to grow, as they are less affected by dishonest traders.

What can be done?

Even bitcoin's current users still operate largely under the traditional mindset of centralised and regulated currencies. Bitcoin advocates may need to find ways to encourage users to develop a new mental approach to unregulated blockchain technology.

But developers could also build tools to address some of bitcoin users' concerns. For example, there may be a way to record whether the real-world elements of bitcoin transactions are also verified, authorised and stored on the public ledger. Electronic wallets could be linked to a reputation file that users could view before agreeing to a deal, much like sites such as eBay allow consumers to rate sellers. And new mechanisms built on top of the irreversible blockchain protocol could enable individual two-way transactions to be reversed.

Without doing something to tackle these challenges, the very thing that caught people's attention about bitcoin in the first place could end up stifling its growth and eventually consigning it to history.

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

Provided by The Conversation

Citation: Bitcoin's central appeal could also be its biggest weakness (2017, July 7) retrieved 24 April 2024 from https://phys.org/news/2017-07-bitcoin-central-appeal-biggest-weakness.html