Bitcoin might not change the world, but the blockchain that makes it work, might

December 18 2015, by David Glance

Credit: AI-generated image (disclaimer)

Digital cryptocurrencies like Bitcoin may have failed to unseat their more traditional rivals, but the technology that underpins Bitcoin may yet bring about a revolution in finance and other industries. This technology is called the "blockhain".

The blockchain acts as a public database or ledger, and is the technology that stores the details of every exchange of bitcoins. What makes it particularly clever is that it is designed to stop the same bitcoin being spent twice, without the need for a third party (like a bank).

The promise of the blockchain

Even from the early days of Bitcoin, it was believed that the blockchain could be used for much more than recording Bitcoin transactions. What the blockchain does is record a set of details that include a time, a cryptographic signature linking back to the sender and some data that can represent almost anything. In the case of Bitcoin, it is the number of bitcoins being sent but it could be a digital cryptographic signature, called a "hash", of any electronic document.

One of the earliest demonstrations of the potential of using the blockchain in this way was "proof of existence", a website that allows a user to upload any document and have its signature recorded for ever on the Bitcoin blockchain.

What this does is prove that the person who uploaded the document had that specific document in their possession at a specific time. It can also be used to prove that the document had not been altered in any way from that time.

The blockchain realised

Proof of existence was intended as a demonstration of the potential of the blockchain technology. Startup Stampery has turned this service into a business that allows other companies to "digitally stamp" any of their electronic documents or emails in order to prove ownership and integrity.

This week the US Securities and Exchange Commission (SEC) approved the use of the blockchain as a share ownership register for online retailer Overstock.com.

Overstock plans to use alternative trading system technology provided by T0.com, to enable people to buy and sell these shares. The attraction of this system is that it provides instant settlement as opposed to the traditional three day settlement for traditional company stock.

T0's implementation of its share register uses an extension of the Bitcoin blockchain called "Colored Coin" that was originally seen as adding a "smart contract" functionality to Bitcoin. One scenario where this could be used would be where someone was sending Bitcoins for the purchase of a house for example, and the currency would only be released if the contracts for the sale went through.

The risks and challenges of the blockchain

Whilst Overstock's SEC filing does highlight the advantages of having a public ledger that is theoretically secure, it also stresses the risks. One of those is the fact that Overstock has chosen to make the information stored on the the blockchain ledger accessible by anyone, so investors may have concerns about the privacy of their holdings.

However, the main risk is one that is a general issue with all blockchain applications, including Bitcoin. This is the fact it is still not known exactly how secure the system is and whether it has any flaws that could be exploited by hackers.

One potential issue around the use of the blockchain is the fact that there are now a large number of different implementations, all based on different technological approaches. IBM, JP Morgan, Intel and a group of other companies have just launced the "Open Ledger Project". Open

Ledger does not use the Bitcoin blockchain but implements a different scheme that is more suited to companies wanting to restrict access to the blockchain ledger.

There is no doubt that the ideas behind the blockchain are clever ones and were critical to enabling a digital currency like Bitcoin to operate with many of the same properties as cash does in the physical world. When the technology is used for other applications, though, it is not absolutely clear that it actually does anything that can't be achieved with other, more conventional technology.

The social issues are harder than the technological ones

It is not the technology that is stopping shares from being settled instantly. It is regulators and the issues they are dealing with in terms of this type of settlement are social and legal ones, not technical.

In the hype that surrounds companies that are working on blockchain products, the real challenges facing the actual use of these products are often glossed over, with the main objective being to get rid of third parties but without necessarily replacing all of the positive things those third parties may actually have been doing.

It is inevitable that blockchain technology will become a mainstream technology. The level of interest being shown in this technology demonstrates its potential for enabling the development of applications that will bring new approaches to old business problems. It is the social, legal and financial challenges that these changes will surface that may prove a much harder problem to solve.

Commons-Attribution/No derivatives).

Source: The Conversation