11-2014

Bitcoins, block chains, and mining pools

Singapore Management University

Citation

Singapore Management University. Bitcoins, block chains, and mining pools. (2014).
Available at: https://ink.library.smu.edu.sg/pers/255

BITCOINS, BLOCK CHAINS, AND MINING POOLS

Published:
26 Nov 2014

Bitcoins can help facilitate online commerce, but investors – and speculators – should understand how the cryptocurrency works

In July 2014, technology giant Dell announced it will accept bitcoins as payment, becoming the biggest company by revenue to accept the cryptocurrency in business transactions. Two months later, digital payment platform PayPal – owned by the world's largest online shopping site, EBay – joined the fray. "Over the coming months we'll allow our merchants to accept Bitcoin," said Bill Ready, CEO of EBay's online payment arm, Braintree.

For something that started in obscurity in 2008 as a concept paper, Bitcoin has become the leading cryptocurrency. In it, the person (or group) who wrote that paper, Satoshi Nakamoto, expressed concern that commerce on the internet was dependent on financial institutions acting as intermediaries to process electronics payment, which carries with it a cost. "What is needed," Nakamoto wrote, "is an electronic payment system based on cryptographic proof…allowing any two willing parties to transact directly with each other without the need for a trusted third party (i.e. financial institutions)."

MONEY MATTERS

For Bitcoin to become more widely accepted, it has to function more like conventional currency. To do so, it must fulfill the three functions of money as:

1. A medium of exchange;
2. A unit of accounting; and
3. A Store of value.

The moves by Dell and PayPal suggest an increasing acceptance of bitcoins as a medium of exchange, but bitcoins fall some way short of the other two requirements.

"Would you post prices in bitcoins?" asks **Ernie Teo**, Research Fellow at the Singapore Management University's Sim Kee Boon Institute (SKBI) of Financial Economics. "Most merchants would not do that yet because bitcoins are still quite volatile. Is it a store of value? Not quite."

A quick check on coindesk.com is all one needs to do to see the wild price fluctuations of bitcoins. From July 2010 to the start of 2013, one bitcoin went from basically zero to about US$13.00. It peaked at US$979.45 at the end of November that year before dropping to just US$638 three weeks later. It has since lurched and surged, going for about US$380 as of November 2014. Why would anyone want to hold on to such a volatile medium as a form of money?

“Transferring money through a credit union can take as long as three days,” says Teo at the recent Chartered Alternative Investment Analyst Association(**CAIA**)-SKBI Cryptocurrency Conference 2014, “and it can cost as much as eight percent of the amount transferred. With Bitcoin, it can cost as little as 0.01 percent of a bitcoin per transaction and the transaction is done in hours.” Based on November 2014 Bitcoin prices, that translates to about four cents.

HOW ARE BITCOINS CREATED?

The price volatility of bitcoins is the simple result of demand and supply, explains bitcoin.org. But how exactly is a bitcoin created? Bitcoin.org explains it thus:

> “New bitcoins are generated by a competitive and decentralised process called "mining". This process involves individuals who are rewarded by the network for their services (solving mathematical puzzles called SHA – Secure Hash Algorithm). Bitcoin miners process transactions i.e. every exchange of Bitcoin that has taken place between a buyer and a seller and secure the network using specialised hardware and collect new bitcoins in exchange.
>
> Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.”

“Bitcoin was designed to be a decentralised system with no central authority, in the sense that no one has a major influence over the way mining functions,” Teo explains. “If no one wins consistently, then the ledger is updated by different miners for each critical cycle, which is six blocks.”

“Would you post prices in bitcoins? Most merchants would not do that yet because bitcoins are still quite volatile. Is it a store of value? Not quite.”

The “block” in question is a collection of files that makes up the Bitcoin network, which together make up the “block chain” which records every transaction that involves bitcoins. “The Bitcoin protocol is written is such a way that a block has to be created every 10 minutes,” Teo elaborates. “To do that with all the advanced machines, the (SHA) puzzle becomes more difficult. To win the contest to win these blocks, more and more advanced machines join the fray. It becomes very difficult to compete as an individual, and as a result, mining pools are formed.”

According to **Robert Deng**, Professor of Information Systems at SMU, the six biggest mining pools control 75 percent of the Bitcoin mining network. In June 2014, the GHash.io mining pool breached the 51 percent threshold of cryptographic hashing output – solving of the SHA puzzles – and could in theory pull off a “51 percent attack”. In practice, that means being able to trick sellers into believing bitcoins have been paid in order to release the products, only for the bitcoins to be withdrawn after getting the merchandise. This phenomenon is referred to as “double spending”.

In a statement, the CIO of GHash.io, Jeffrey Smith, said, “We never have and never will participate in any 51 [percent] attack or double spend against Bitcoin. Still, we are against temporary solutions, which could repel a 51 [percent] threat.”

BITCOINS: ANONYMITY ASSURED?

Despite the risks of holding bitcoins, demand is growing steadily. According to blockchain.info, there are now about 220,000 unique Bitcoin addresses that work similarly to an account; at the start of 2011, there were less than 1,000. Part of Bitcoin's appeal lay in its anonymity, as buyers and sellers of bitcoins do so with pseudonyms.

"Bitcoin is only pseudo-anonymous," Teo clarifies. "All transactions that have taken place can be seen by anyone on the network. Users are identified by pseudonyms. Satoshi recommends changing pseudonyms each time you transact in order to be truly anonymous."

Teo adds, "A group of researchers (see here) found that almost 40 percent of user identities can be recovered even if they were using the recommended privacy protection techniques such as using pseudonyms."

That is bad news for those who intend to use bitcoins to run illegal operations such as drug markets, as was the case of the now-closed Silk Road website. But for those who intend to invest or even speculate in bitcoins, security should not be an afterthought.

"Just like you can lose your money, you can lose your bitcoins," Teo warns. "If you don't backup your mobile wallet, for example, you will lose your bitcoins when you lose your phone. If you store your encrypted coins on your computer, and hackers get into your computer just like burglars get into your house, you'll lose your bitcoins.

"Some users turn to cold storage to protect their bitcoins. Cold storage means storing your bitcoins offline. You could print out your Bitcoin code on a piece of paper and lock it in a safe. You could also store it in a USB or hard disk, disconnect it from a computer and put it away. However, if you lose the paper or the disk drive, you'll also lose your bitcoins."