

The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution

Chris Rose, Capella University, USA

ABSTRACT

Bitcoin was not the first attempt at a digital currency, but it has been the most successful and it is now being accepted by a number of major retailers. Bitcoin is a cryptocurrency and operates as a peer-to-peer network. Its security is guaranteed by cryptographic algorithms instead of governments and has the potential to become a major means of payment for e-commerce and may even materialize as a viable challenge to traditional money-transfer providers. Instead of serving one country or some countries, Bitcoin serves the entire world.

Keywords: Bitcoin; Digital Currency; Cryptographic Currencies; Cryptocurrency; Cryptographic Algorithm; Blockchain

BACKGROUND

If you compare two pieces of American money dating to the 19th century, you could find a dollar coin made of silver and a paper dollar that in those days could also be exchanged for the same silver coin. More than a 100 years ago paper dollar bills were backed by silver, a precious metal that theoretically should always have value. However, today that has changed, a modern dollar bill is backed by nothing but the word of the U.S. government.

Therefore the government can do whatever they wish, they can print more paper money, devalue the dollar any time they want, in fact, and although unlikely, the dollar could even disappear completely (Metz, 2013).

There are subtle differences between a virtual currency, a digital currency and a cryptocurrency, although the terms are often used interchangeably.

- **Virtual Currency** – in 2012 the European Central Bank defined a virtual currency as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." The US Department of Treasury states that although a digital currency operates just like a traditional currency, it does not have the same attributes.
- **Digital Currency** – is a form of virtual currency that is electronically created and stored. Some, but not all digital currencies are cryptocurrencies.
- **Cryptocurrency** – is a subset of digital currencies, however, it uses cryptography for security so this makes it extremely difficult to counterfeit (Gilpin, 2014).

One important fact about all these is that they are not issued by any central authority and are independent of traditional banks. Many people do not even consider them to be money although they could eventually create extremely strong competition to traditional money. Many people do not believe in dollars, ruble, yen or any other government currency, they only believe in gold and silver but many people are also starting to believe in cryptocurrencies. "Bitcoin was created to take power out of the hands of the government and central bankers, and put it back into the hands of the people"(Gilpin, 2014).

DEVELOPMENT

In 2008, a programmer (or perhaps a group of programmers) using the name Satoshi Nakamoto published a paper describing digital currencies and the following year launched the Bitcoin network (Metz, 2013).

Unlike government currencies, there is no central bank backing Bitcoin and anyone with a computer or an Application-Specific Integrated Circuit (ASIC), which is a dedicated machine specifically created for the purpose, can create a Bitcoin by a process called mining. It is relatively fast, cheap and easy to do since in Bitcoin, each participant theoretically has equal power. There are no banks, therefore no bankers, so everyone stores their own Bitcoin in a virtual account called a wallet. The user controls their own money and users can even send micropayments as small as what is called one Satoshi or 0.00000001BTC, (a Bitcoin to eight decimal places) or about \$0.000005 today. The value of a Bitcoin, like any other currency, is dependent on what the buyer is willing to pay. If nobody used Bitcoin it would have no value but Bitcoin can have any price, and volatility is common, making and losing fortunes for many people in the process (Kelion, 2013).

The banking system today is stagnant and runs on an obsolete infrastructure which takes days or weeks to send money around the world. Same day payments only happened after banks “were dragged into the 19th century by the Office of Fair Trading. When Metro Bank opened in 2010, it received the first new UK banking license issued in 150 years” (Kelion, 2013).

Bitcoin is a new financial system, designed by the people, for the people and theoretically everyone has equal power. People control their own money and the rules of the Bitcoin system are enforced on everyone by each other through mutual distrust (Kelion, 2013). Nobody can tamper with or influence the system except in one unlikely scenario of controlling 51% of the entire network.

Value

Originally, Bitcoin was not of interest to the general public, since mainly cryptographers, hackers, and mathematicians understood its purpose and use. It is generated by an algorithm, it is impossible to counterfeit, it is more or less anonymous, and since it is a peer-to-peer network there are no additional fees from middlemen such as banks. In fact, these are the virtues of a currency uniquely suited to our modern digital economy. However, although the value of Bitcoin lies in a combination of speculation on future value and genuine, undeniable usefulness, the wild swings in price Bitcoin has been experiencing are a natural reaction to the massive global interest in a pool of money that is relatively tiny compared to its government-backed peers.

But all these wild swings are preventing Bitcoin from achieving its real purpose as an innovative new form of currency. Although many businesses from PayPal, to Dell to Newegg to Lamborghini dealers to Virgin Galactic have declared that they are accepting Bitcoin, it is difficult to accept a payment that could lose half its value overnight or might double by next week, and although it has the potential to become the basic value of exchange on the Internet “its high volatility, a result of speculative activities, is hindering its general acceptance as a means of payments for online commerce” (Popper, 2013).

Virtual currencies exhibit network externalities, the more people use them, the more valuable they are. Because Bitcoin was the first digital currency to market gives it a tremendous advantage. Bitcoin gets the most publicity and has more people and merchants supporting it, and also has the most users invested in it. As long as Bitcoin continues serving the needs of users, it has the potential of remaining the most important digital currency indefinitely. And although there are many proposed improvements to Bitcoin that are theoretically interesting, none appear to be able to induce users to switch in large numbers (Lee, 2013). “Bitcoin could become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers. As a medium of exchange, Bitcoin has clear potential for growth, in our view” (Popper, 2013).

How It Works

Bitcoin is a peer-to-peer network. In a conventional payment system such as a credit card, for example Visa, MasterCard or even PayPal, there is a company in the middle, a for-profit company that centralizes payments, operates the network, and makes sure it is secure and reliable. However, Bitcoin has a completely different model, its security is guaranteed by a cryptographic algorithm, a Secure Hash Algorithm (SHA) which is 256 bits (SHA-256) instead of being guaranteed by a government or governments. For example, if you deposit one dollar into PayPal, the PayPal network will guarantee that you will be able to retrieve a dollar whenever you wish.

However, no person, institution or government guarantees Bitcoin, since nobody owns the network. This means that there is no guarantee that a Bitcoin will have a stable relationship to any conventional currency. The Bitcoin floats against conventional currencies and has been less than a dollar in 2011 to more than \$1,200 in 2013 to presently about \$500. In addition, Bitcoin is open source therefore anyone can take the source code, make minor modifications and then create a similar network to Bitcoin thereby creating their own currency. However, the core Bitcoin protocol is extremely difficult to change because of the decentralization of the network, therefore if someone believes they have an idea for a better virtual currency, it is much easier to start their own currency than to convince Bitcoin users to change (Lee, 2013).

In Bitcoin mining, thousands of competitors race to solve a mathematically complex repetitive problem. If a person solves the problem then they are rewarded with the ability to add a block to the Bitcoin global transaction register and get 25 Bitcoins as a reward. However, because it takes so much computing power the more popular way is to join a mining pool of thousands of users each contributing their computing power to solving this problem and being rewarded with a share of the profits from the solving of the problem.

Originally it was thought that Bitcoin would be the “people’s currency” and that computing power would be decentralized and everyone would have an equal chance of solving the Bitcoin problem called a hash function. However, it has evolved that this hash function can be solved more efficiently by dedicated equipment built specifically for this purpose. What has happened is that instead of the average computer user trying to mine Bitcoin with their PC, it has now become the realm of people or groups of people investing hundreds of thousands of dollars into dedicated machinery which only has one function and that is to solve the hash function (Lee, 2013). Since every transaction in Bitcoin is available to be viewed, it is easy to find many people or groups of people making more than \$3,000 per day or more than \$1 million per year mining Bitcoin.

It is so much more efficient to use these ASICs that it is no longer cost-efficient to use an ordinary PC to mine Bitcoin, since the electricity used would be more than the value of the Bitcoin mined. Instead large pools of users have been formed and these pools control the majority of the network computing power. The major alternative to Bitcoin is called Litecoin, (sometimes called the silver to Bitcoin gold), and this uses an algorithm called Scrypt that was supposedly more difficult to automate. However, after a short time, considering the amount of money that could be made, it was inevitable that dedicated machinery would be produced for the Scrypt algorithm and since 2014 there are numerous Scrypt ASIC devices available on the market.

Legality

“The Department of Justice recognizes that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce,” (Ribeiro, 2013). You can purchase anything from “beer in Berlin, order pizza in Amsterdam, hire a taxi in Edinburgh, schedule a dental check-up in Ljubljana, do a degree in Nicosia, purchase Alpaca socks from Massachusetts - or even blast off into space with Virgin Galactic”(Kelion, 2013).

In May 2010 the first commercial transaction using Bitcoin was recorded where Laszlo Hanyecz, a Florida programmer, used 10,000 Bitcoin to purchase two pepperoni pizzas from Papa John's. Roughly valued at \$60 at the time, Hanyecz figured that was enough Bitcoin for two pizzas and compensation for somebody’s time but today that amount of Bitcoin would be worth about \$5 million (Griswold, 2014).

Bitcoin is a huge evolution in the history of money that is expected to thrive since the number of businesses and people who accept Bitcoin as payment is increasing. To move Bitcoin into the marketplace also means everyone has to be convinced that Bitcoin is legitimate, safe and has a value. "It's like being on the ground floor of the Internet 20 years ago,"... "Bitcoin is going to be transformative" (Leinwand, 2013) but unfortunately, since it is virtually untraceable it has been used for a host of nefarious purposes. "We have also seen, however, that certain aspects of virtual currencies appeal to criminals and present a host of new challenges to law enforcement," (Ribeiro, 2013).

CONCLUSION

At a university, if you see someone praising Bitcoin, that person is from the computer science department but if you see someone criticizing Bitcoin, that person is likely from the economics department. The reason is that the odds are objectively against Bitcoin's long-term success. It is extremely difficult to start an entirely new concept that depends on a lot of people accepting and using it, and it is even more difficult when the new concept is an entirely new payment and monetary system. There are countless possible ways that Bitcoin could fail. "The technology fails. Over speculation causes an irrecoverable crash. The price never settles down. Deflationary pressure annihilates liquidity. A government shuts it down. A new currency makes it obsolete. Users abandon it for some other reason" (Jeffries, 2013).

Economists have never had to consider a system such as Bitcoin until it was developed and now they are just beginning to imagine the ramifications. Some economist believe that Bitcoin will fail because the price of producing a Bitcoin clone is zero but it is also possible that Bitcoin will disrupt the entire monetary system. Money should serve as both a reliable medium of exchange and a stable storage of value. It is this storage of value that causes most economists problems since money that is a reliable store of value is usually backed by a government or some central authority or it has inherent value, such as gold or silver. If there is no backing and no intrinsic value people will not trust it over time (Jeffries, 2013).

However, Bitcoin is limited in supply, once 21 million Bitcoins are created there will be no more issued. This means the supply of Bitcoin is even more inelastic than gold and the supply is also much more transparent than gold. Just like gold, Bitcoin does not decay and it is perfectly divisible, it has no issuing authority or country of origin therefore it is a truly global currency, so it could become the medium of exchange between any two parties anywhere in the world. It is also the ultimate disintermediator since there is no central authority or bank. It requires no storage and is both a monetary raw material and payment system in one. It is either that Bitcoin fails and become worthless or it takes off and each Bitcoin is worth hundreds of thousands of paper dollars, maybe even more. Those who invest in Bitcoin should therefore consider it a speculative option on the future success of cryptocurrencies (Schlichter, 2013).

AUTHOR INFORMATION

Dr. Chris Rose earned his Masters and Doctorate degrees from Nova Southeastern University from both the Graduate School of Computer and Information Sciences and the H. Wayne Huizenga School of Business and Entrepreneurship and teaches in both disciplines. His current areas of interest are the Internet of Things and Digital Currencies.

REFERENCES

- Gilpin, L. (2014) 10 things you should know about Bitcoin and digital currencies. TechRepublic. Retrieved 6/28/2014 from <http://www.techrepublic.com/article/10-things-you-should-know-about-bitcoin-and-digital-currencies/>
- Griswold, A. (2014) The First-Ever Bitcoin Purchase Was Remarkably Inglorious. Slate.com. Retrieved 8/23/2014 from http://www.slate.com/blogs/moneybox/2014/05/23/first_bitcoin_purchase_two_pepperoni_pizzas_from_papa_john_s.html
- Jeffries, A. (2013) The Verge. Why don't economists like Bitcoin? Retrieved 1/4/2014 from <http://www.theverge.com/2013/12/31/5260534/krugman-bitcoin-evil-economists>
- Lee, T. (2013) The Washington Post. Dogecoins and Litecoins and Peercoins oh my: What you need to know about

- Bitcoin alternatives. Retrieved 12/28/2013 from <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/26/dogecoins-and-litecoins-and-peercoins-oh-my-what-you-need-to-know-about-bitcoin-alternatives/>
- Leinwand, D. USAtoday. Bitcoin: Super currency or super fad? Retrieved 12.22/2013 from <http://www.usatoday.com/story/news/nation/2013/12/10/bitcoin-entrepreneurs-seek-mainstream-acceptance/3971121/>
- Metz, C. (2013) For Bitcoin's Biggest Believers, Digital Currency Is Better Than Gold. Wired. Retrieved 7/14/2014 from <http://www.wired.com/2013/10/bitcoin-in-japan/>
- Popper, b. (2013) The Verge. Bitcoin is too cheap for its own good. Retrieved 1/3/2014 from <http://www.theverge.com/2013/12/9/5192054/bitcoin-boom-bust-bubble-currency-technology>
- Ribeiro, J. (2013) US agencies see some benefits in virtual currencies. PCWorld. Retrieved 12. 28/2013 from <http://www.pcworld.com/article/2064800/us-agencies-coming-around-cautiously-to-seeing-benefits-in-virtual-currencies.html>
- Schlichter, D. (2013) Could Bitcoin be the money of the future? Retrieved 8/26/2014 from <http://detlevschlichter.com/2013/04/could-bitcoin-be-the-money-of-the-future/>

NOTES