Bitcoin Currency

Abdulelah Almazrua

Abstract— This paper defines and explains the decentralized digital currency "Bitcoin", and highlights the most important features that Bitcoin has over other currencies. It is an attempt to explain with details how the transaction in Bitcoin occurs. In addition, the paper highlights the pros and cons of Bitcoin nowadays, and what the future might be for the digital currency.

1 Introduction

CREATING a new currency in the new world is not an easy job. There are almost 180 active currencies in the world, and most of them have a long history of exchanging goods and services, which gave them strength and made them accepted and trusted by people. For example, the United State Dollar (USD), the most used currency in the world, was established as the US currency in 1792 before 220 years ago, and some currencies were established before that.

Nowadays, people use different ways to buy and exchange things. One way that has been increasing over the recent years is buying things online. Millions of transactions have been made every day online, and all of these transactions were made through a third party such as a financial institution. In late 2008 an anonymous person established a paper and came up with an idea to create a new currency that does not require a third party such as a bank or payment processor to complete the transaction. He called the paper that he released an electronic cash system that was based on peer to peer (P2P) system. In 2009 the first open source Bitcoin client was released. This new currency could open a new chapter in the way of exchanging goods and services.

2 Bitcoin Creater

Satoshi Nakamoto is the pseudonymous individual who is attributed to the innovation of the Bitcoin whose identity has been found to be unique across the globe. This was launched in late 2008; however, he has not been involved in further development of the Bitcoin since 2010. Nonetheless, Nakamoto is noted to have played a critical role in the technical development of the Bitcoin that mainly involved the development of the Bitcoin protocol. As Davis (2011) notes that Nakamoto stopped being involved in the Bitcoin upon claiming that he got involved in other things that he considered important. To date, the true identity of Nakamoto has not successfully been confirmed, however, the initial intention was to develop a system that entirely controlled (Wolman, 2012).

3 Bitcoin definition

Bitcoin is an experimental, decentralized digital currency that enables instant payments to anyone, anywhere in the world. Every Bitcoin is divided into about 100 satoshis defined by eight decimal places. Bitcoin uses peer-to-peer (P2P) system to operate with no central authority. Managing transactions and issuing money are carried out collectively by the network. In addition, the process of the transaction uses Bitcoin miners' servers that involve internet based network linkage between communicating servers to confirm the transactions. Moreover, Bitcoin is an open source project so everyone can see the code of the program that runs the transactions. Digital signatures are used in bitcoin transactions to proof the transactions instead of financial institution, and the transaction is done through the use of smartphone or a computer, and does not involve a financial institution.

The implementation of the Bitcoin revolves around the introduction of the crypto currency concept that requires the use of the cryptography in transacting and creating a new category of money that does not involve the reliance of the central authorities. Since its inception, various developments have been made in the implementation of the Bitcoin. The latest developments occurred in 2013 that was notable with the development of the payment processor, internet archive, block chain, and financial crimes enforcement network. In the process of implementing the Bitcoin, various challenges have occurred and methods to overcome the challenges have been developed with critical resources being put on the efficiencies of the technological development. Some of the recent challenges that have occurred to the Bitcoin include the recent April 2013 processing delays that are attributed to Mt. Gox and Bitlnstant processors that are responsible for 80% of Bitcoin payments.

According to Ron & Shamiur (2012), among the most critical value of the Bitcoin is that it does not involve a centralized authority as in the case of the Fiat Currency. The Bitcoin software uses a geometric series to raise the money supply up to a level of 21 million Bitcoins. The Bitcoins are then issued via a transaction records transmitted through computer technology power nodes. The nodes earn Bitcoins that are traded. Presently, in every 10 minutes, there is a generation of 25 Bitcoins. More so, the production of the Bitcoins will continue to reduce in every four years (Wallace, 2011). The money supply is known by the clients subdividing the Bitcoin in 8 decimal places. The value of the Bitcoin is known after selling or buying them against other currencies. It is worthy noting that, relative to other global currencies like British Pound, Euro, and the United States Dollar, the Bitcoin has greatly appreciated.

According to Altshuler (2013), the Bitcoin offers a solution to the problem of double spending (p.221). The solution offers a peer-to-peer network in the management of the financial transactions. This is through hashing of the network timestamps through a proof of work chains that cannot be

redone. The long chains of the proof of work are referred to as blocks that employ computer technology. There is sufficient control of computer power through the nodes that provides security. Hackers within the system or outsiders cannot easily attack the nodes. The network used in the uses a minimum structure with the messages and nodes leaving and joining the network randomly. That plays a critical role in ensuring security in the Bitcoin network through the creation of long chains of proof of work of happenings in the network.

4 Digital Signatures

Identification of the Bitcoin is done through chain of ECDSA digital signatures. "Elliptic Curve Digital Signature Algorithm (ECDSA), the ECDSA algorithm has its use in digital signatures" (Kogent Learning Solutions, Inc., 2009, p.1648). Hashes are attached digitally to every coin being traded, and the ownership can be determined through the use of signatures attached to the coins that have been traded. SHA-256 is a combination of cryptographic hash functions that verifies the transaction. In addition, the RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) is a form of digital signature that is normally placed above the SHA-256. Trading of the Bitcoin begins with a timestamp whose use is to prove existence of Bitcoin data at a specific point of time before development of the harsh. The timestamps play an important role in development of the chains through the hashes. Another factor worth evaluating is the Bitcoin mining.

5 Bitcoin Mining

Bitcoin mining is a process that involves the use of the proof of work after the implementation of the timestamp that is distributed on peer-to-peer server. It is through Bitcoin mining that the value of a coin after hashing. The value of a coin is known after the use of the longest chain that is a presentation of the most valuable proof of work. That requires the long chain to play a critical role of the long chain in determination of the value of Bitcoin that must use honest nodes, and great computing power. The great computing power of the computer hardware that must be supported by nodes that run over time; however, a problem may arise if the nodes are produced so fast. That calls for the nodes to be produced on hourly basis.

6 Implementation

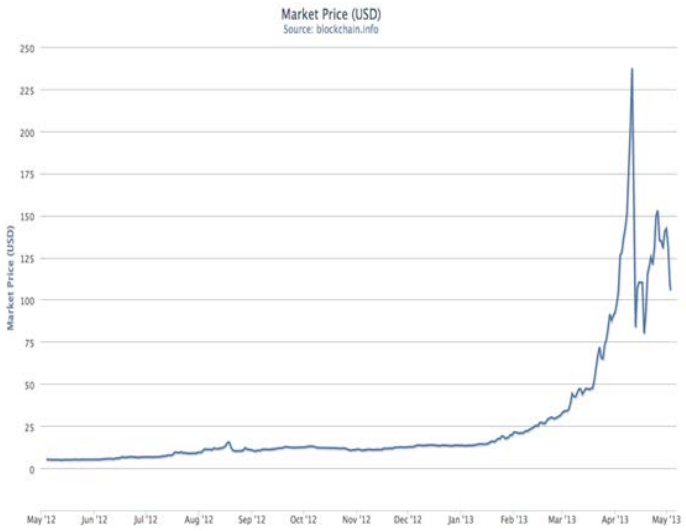
To start making transaction by Bitcoin what the user needs to do is installing a wallet, which is an application that needs to be run on a computer or smartphone, or using a third party service online. The wallet generates an address to the user, which is what the user needs to receive a Bitocin. Simply, using a Bitcoin address is similar to the use of e-mail address to send and receive e-mails. The Bitcoin address has numbers and letters around 33 characters in length, and always begins with the digit 1 or 3. Moreover, the user can have more than one address on his/her wallet, which is recommended to increase security and anonymity. Once the user had a wallet and address, and got the first Bitcoin, he/she can exchange things or invest the Bitcoin.

7 Advantages

There are several pros and cons attributed to the Bitcoin because it uses several technologies, and possess several economic features. Bitcoin works globally, and that makes it accepted everywhere and anytime across the world. In addition, since Bitcion doesn't involve a third party, the transactions can be made to anyone on earth with small amount of fees, unlike transactions that made through financial institutions such as a bank, which require a high amount of fees. Moreover, Sending Bitcoin by its application is simple, easy and doesn't require a lot of information such as expiration date, names, account number or CVV number. The recipient's address is enough to make the transaction. The transactions in case of Bitcoin are highly secure because of the use of digital signatures and the required conformations to identify the transaction. In addition, Bitcion is not controlled by any government or financial institution, therefore, inflation in Bitcion is unlikely to happen. Owning a Bitcoin account doesn't require any amount of deposit, which gives it another advantage compared to traditional bank accounts. However, despite of its pros, Bitcoin has several cons that some experts have been arguing about.

8 Disadvantages

Since Bitcoin is a new born currency, that eventually makes its value high in volatility. As an example, on April 10, 2013, the value for Bitcoin dropped to $105 from $266; however, within six hours of trading, the price rose to $160. The chart shows the volatility in Bitcoin compared to USD.

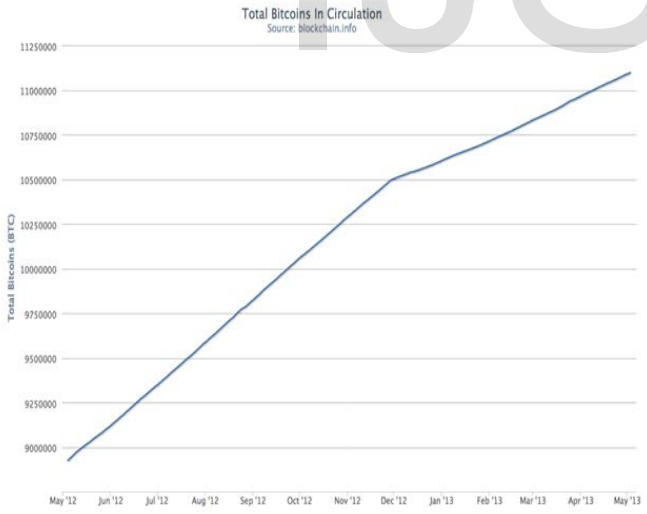


Economists refer to this situation as a kind of an economic bubble facing the Bitcoin (Farivar, 2013). Moreover, Bitcoin is still not widely accepted because it is a new currency that would be hardly to get trusted and accepted quickly and eve-

rywhere. However, the use of Bitcoin has been increasing over the recent years. On the other hand, some scholars have argued that the high use of the Bitcoin in some countries such as Spain may have attributed to the financial crises that have faced Spain between 2012 and 2013. That is through the high levies charged on deposits. Another disadvantage of Bitcoin is that Bitcoin can't be replaced if lost or stolen. Experts highly recommend making a wallet backup due to this issue. In addition, the use of Bitcoin as a currency has been opposed because it is not controlled by any sovereign country, and consequently, that makes it to be used in the black market. An example of the use of Bitcoin in the black market is evidenced by some Iranians who try to use it in efforts to avoid foreign currency sanctions. Another example is the heavily use of Bitcoin in some black market websites. Moreover, it is believed that Bitcoin could be replaced with similar currency. Since it is a new born currency and not controlled by any government, developers could develop a new version of Bitcoin protocol. Despite the fact that Bitcoin has many pros and cons, Bitcoin will be a big argumentative topic down the road.

9 Bitcoin Future

The future of Bitcoin is unpredictable. However, without any doubt the increased number of Bitcoins circulation is a good sign for Bitcoin. The chart shows the increased number of Bitcoins in circulation since May, 2012 until May, 2013. The number of Bitcoins has been increasing for more than 2 million Bitcoin in one year.



Moreover, First Bitcoin ATM in the world was launched in San Diego, CA in May 2, 2013, which shows another positive development in Bitcoin market. If Bitcoin complete growing up, its price would be stable and would become a small part of the world economy. However, Bitcoin has some powerful opponents, such as banks, payments processors and governments that might play a great role in controlling or ending Bitcoin era.

10 Conclusion

The Bitcoin uses cryptography in transacting and creating a new form of currency has greatly improved the use of digital currency across the globe. Despite having cons such as fluctuations in the prices, it has greatly scored. Of critical importance is the failure of making those holding money rich rather than facilitating the financial transactions and thereby contributing to the overall economy growth. In addition, the value of the Bitcoin having depends on speculation that other people will accept it during financial transactions. The Bitcoin protocol employee variety features of modern technology that offer solution to the problem of double spending; however, despite making efforts to maintain high security through the long chains of proof of work. Bitcoin is a great technological innovation that is yet to be accepted globally as a crypto form of currency.

References

Altshuler, Y. (2013). Security and privacy in social networks. New York, NY: Springer.

Davis, J. (October 10, 2011). The Crypto-Currency. The New Yorker. Retrieved 30 April 2013, from http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis.

Farivar, C. (Apr 10 2013). Bitcoin crashes, losing nearly half of its value in six hours. Technica. Re-trieved 29 April, 2013 from http://arstechnica.com/business/2013/04/bitcoin-crashes-losing-nearly-half-of-its-value-in-six-hours/

Kogent Learning Solutions, Inc. (2009). C# 2008 programming: Covers .NET 3.5: black book. New Delhi, India: Dreamtech Press.

Ron, D. & Shamir, A. (18 October 2012). Quantative Analysis of the Full Bitcoin Transaction Graph. Retrieved 29 April 2013 from http://eprint.iacr.org/2012/584.pdf.

Total bitcoins in circulation. (May 2013).

Retrieved 4 May 2013 from http://blockchain.info/charts/total-bitcoins

Wallace, B. (Nov 23, 2011). The Rise and Fall of Bitcoin. The Story of a Revolution. Retrieved 29 April 2013 from http://www.wired.com/magazine/2011/11/mf_bitcoin/.

Market price (USD). (May 2013).

Retrieved 4 May 2013 from http://blockchain.info/charts/market-price

Wolman, D. (2012). The end of money: Counterfeiters, preachers, techies, dreamers-and the coming cashless society. Boston, MA: Da Capo Press