International Journal of Hybrid Information Technology
Vol.8, No.9 (2015), pp.63-70
http://dx.doi.org/10.14257/ijhit.2015.8.9.07

The Study of New Virtual Currency-Bitcoin

Kai Chain and Yao-Ren Wen

Department of Computer and Information Science, R.O.C. Military Academy
chainkai@mail2000.com.tw

Abstract

It doesn't matter whether its coin, banknotes or even gold the usual currency in circulation in our communities. But have we ever thought of using virtual currency in the real world, with a higher value to that of gold. Bitcoin have caused waves across the globe, it is believed to be the most valuable currency in the future. This article describes the sensation caused by the global virtual currency Bitcoin, the rise resulting in principle and practical instruction on how to get Bitcoin currently in use.

Keywords: *Bitcoin, Virtual Currency, P2P, Electronic Commerce*

1. Introduction

What is Bitcoin (show in Figure 1)? The global sensation caused by the virtual currency (Bitcoin) its news to many [1, 2]. Bitcoin is different from the traditional currency. It's a set of complex algorithms with coded passwords. Bitcoin operating mechanism doesn't rely on central banks, government or cooperate business, but surly on peer seed file in the network to reach the network protocol, a perfect monetary system [3]. Theoretically speaking it is to ensure that the system is free from the control of government, organizations or individuals [4].

Each piece of Bitcoin generation and consumption will be distributed through the P2P network to record and inform the whole network. It helps avoid forgeries. It's not bound on any individual to monitor the virtual currency, resulting to it getting very popular [5].

Figure 1. Bitcoin

2. Brief history of Bitcoin

In this chapter, let us introduce the history of Bitcoin in the order of presence [6-8].

1982 David Chaum came up with "Untraceable Payment System" based on cryptograph.

1982 David Chaum in cryptography-based, first proposed "untraceable payment system."

ISSN: 1738-9968 IJHIT

1998 Nick Szabo invents “Bit gold”; Users through competition solve “the problem of workload proof”, then use password algorithm to broadcast the answer.

2008 Satoshi Nakamoto in a cryptography website email group published a paper describing Bitcoin electronic cash systems.

2009.1.3 Satoshi Nakamoto announced the code of program for Bitcoin and published the earliest Bitcoin

2010 The earliest trade agreement: bought a 25 U.S dollars pizza with 10000 Bitcoin.

2012.10 The Bitpay Company states: over 1000 stores traded using Bitcoin.

2013.8.8 The federal judge in Texas rule on Bitcoin as a legal currency, and supervised under *“Federal Securities Laws”*.

2013.8.19 German Government validates the position in law and taxation of Bitcoin. It was also the first country to validate Bitcoin as a legal currency globally.

2013.10.29 the first ATM for Bitcoin was set in Vancouver, Canada.

2013.11.20 the chairman of U.S. Federal Reserve, Ben Bemanke mentioned that “As all the other payment systems, Bitcoin have the same high potential” and it might foster a safer, faster and more effective system in the coming future.

2013.11.21 The President of Central Bank, Mr. Perng regards Bitcoin as a type of precious metal.

2013.12.5 People’s Bank of China issued statements that acquiring every financial institution and payment institution are not allowed to use product pricing. It is forbidden to provide any service to customer directly or indirectly.

2014.3.8 the first Bitcoin ATM appeared in a coffee shop in Seoul, South Korea.

2014.4.15 the first Bitcoin ATM appeared in a coffee shop in Shanghai, China.

3. How Bitcoin Works

3.1. The Theory of Producing

This chapter emphasizes on the principle of how Bitcoin is generated and mined. Bitcoin (or BTC,฿) are global wise P2P coded virtual currency The technological principle of Bitcoin depends on peer network and P2P node, it has to be calculated and solve some mathematical problem [9, 10]. Initially, it needs to be operated via CPU, and then it became more complicated. A professor found out that the speed of operation of GPU is ten times faster than which is operated by CPU. Therefore, CPU was replaced by GPU. The operating difficulty of Bitcoin is its ability to adjust automatically.

The first four years, the system produced 10,500,000 Bitcoin, which means started right after it published. (Jan 3rd, 2009) The value decreased into half every four-year. In the 4–8years there will be 5,250,000 Bitcoin produced. So, the limit sum of the Bitcoin will unlimited close to 21,000,000 but not more. Based on the current info structure, every unit of Bitcoin can be separated into 8decimal. In another word, 0.00000001BTC is the smallest unit of Bitcoin [11].

To make the Bitcoin from calculation, we need the built-in program from block. The population of the same block may also increase the difficulty to mine the new Bitcoin. This is the integrate analysis of the distributed network of Bitcoin. Therefore, the complexities are related to the average input computing capacity. To mine the Bitcoin, one’s computing capacity need to above the average miner’s computing capacity [12]. In another way, in the *minsanity*, the normal miner may barely mine the Bitcoin from this high computing competition. In the first 210,000 blocks, every block has exactly 50BTC. Due to the

algorithms, the next 210,000 blocks can only makes 25BTC. This depends on the rule, the last Bitcoin will be produce in 2040, and at the same time, the sum of the BTC will be twenty-one million.

3.2. The Explanation of Operation

Recently, the main way to make Bitcoin is still the mining system. First of all, every miner needs to create an electric wallet. Miners can apply it from the official website of Bitcoin or the online wallet account web such as Blockchain. Then make the Bitcoin through mining. There is very few ways to mine. For example, here I mention 6 different ways that I had experienced (Figure 2 and 3 shows how to create an electric wallet for Bitcoin), such as slush, pay-per-share, luke-jr, triplemining, p2pool, puddinpop .*etc*. The most common way so far is pay-per-share. The theory is they make a high computing capacity computer being the host, and let the share mine for the host. The benefit for this is the share can immediately get the Bitcoin they make rather than wait for the entire block being calculated. Usually, the miner should wait for the entire blocks get calculated so they can get their pay. Therefore, there exists a risk is that the miner may get nothing once if they leave before the entire block was solved. So in the pay-per-share case, the miner can avoid the situation and transfer the risk to the host. Also, the host can charge the commission to cover the possible risk for if the cost did not make up the expenses.

Figure 2. Create Bitcoin Wallet

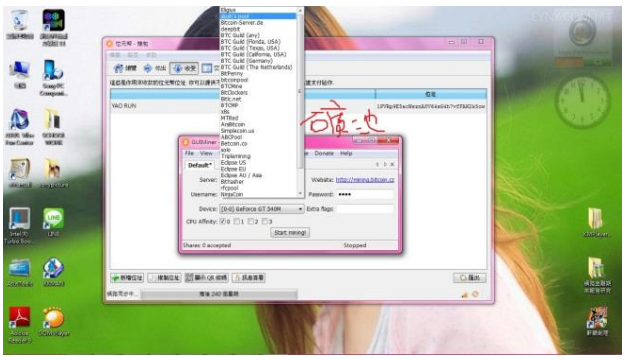

Figure 3. Search for Mining Pool and Start Mining

The safest method is p2pool, which is manipulated by centralized concept (the content is no longer produced by specific experts, instead is participated by internet users and class equality) to block the attack by DoS. The value of Bitcoin reached 1000 U.S. dollars in November, 2013. Compared to its value in 2009, it

grew two hundred thousand times than before. The limited sum of Bitcoin causes high exchange rate. Its security is undoubted and seen as the safest currency in the modern world. It combines the principle of p2p peer network and cryptograph. In the peer network, every user is seen as a node, and every node has the function of server. For each node, it is not able to find any other node directly. Instead, the problem can be solved by joining a group.

It incorporates peer network, nodes and other sites in the sent messages, and nodes can be found by anonymous users directly. Nodes are distributed all over the internet with P2P skills and the principle of cryptograph to make sure Bitcoin distributed system will not be undermined by government, organization, hacker and quarantine. DDos and other cyber-attack are against to Bitcoin trading center. In theory, the cyber-attack or shut down the network of traditional currency trading center will not influence the distribution and usage of currency [13]. Figure 4 shows the operation of Bitcoin.

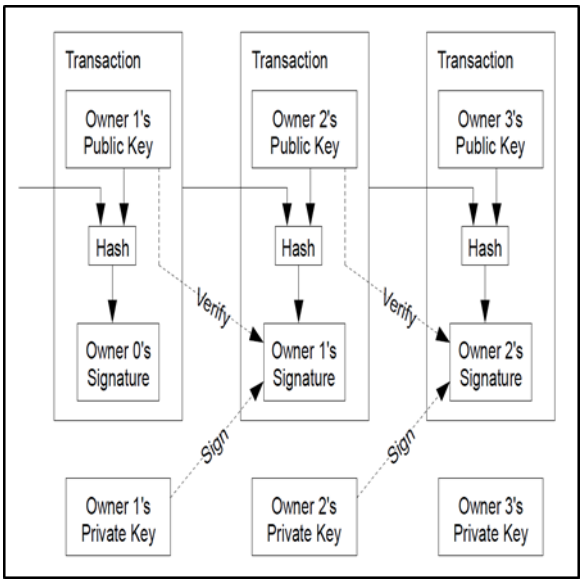

Figure 4. Operation of Bitcoin

4. The Status Analysis of Bitcoin

The method to earn money via network is the main reason causing *minsanity*, just boost the computer and hanging computer. Furthermore, according to physical test, mining with GPU is faster ten times than CPU. It proves that the speed of Bitcoin *minsanity* is based on the level of Graphic Cards.

The following list is how to gain Bitcoin:

1. Bitcoin mining: This is the easiest method and adapt to common users. The users needless to be professional and the standard is the lowest. The more people join in the activity, the harder to make Bitcoin. Figure 5 shows the mining machine.
2. The ticket to participate in the party of mining is to having an effective technological gear which has powerful graphical processing unit to afford complicated calculation and decode.
3. There is a problem that cannot be ignored. The values of Bitcoin will collapse if bugged, which can be used as money laundering, being created.
4. Bitcoin is a virtual currency that will not be monitored by any government or financial institutions. There is a chance that the values of

Bitcoin can be drop to zero. However, the Bitcoin cannot be hacked and the chance of forgery in its security system is nil, this is the motive behind increasing the value of Bitcoin. A Bitcoin could exchange one thousand U.S. dollar during the peak.

5. The cyber-security and trading circulation is not clear, but extremely unrestrained. The creation of mining depends on calculation and cryptograph to sustain its stability. So, financial institution and government are not able to supervise it.

The difference between Bitcoin and traditional currency: Regardless of the not mining and the probability of collapse for vital currency, Bitcoin is creating a brand new vital currency. Despite the currency is not guaranteed and the possibility of collapse, its advantage is tradable.

It needs to be registered and validated to avail of vital currency on online trading post (Mt Gox). However, Bitcoin is not limited, and the software needs to be installed. It will give user a scrambled code to receive and distribute BTC (like 14NgUhgnTByY3YYxAzoFLchLL8yjAhj y09d). Initially, traditional currency requires deposit and withdraws. But Bitcoin does not need to do such thing like that; the amount of account is from mining.

Bitcoin is a kind of vital currency, which cannot be prosperous by distributing uniformly. Thus, the professors invented mining, by means of GPU and CPU to gain more BTC. Figure 5 shows Bitcoin mining machine.

Figure 5. Bitcoin Mining Machine

Few people gain Bitcoin gradually by over running GPU or CPU. The market can be manipulated freely, once users appear. There still have people willing to try and accept this kind of coin even if there is no total control, insurance and collapsing in anytime. Therefore, the trading market for Bitcoin became prosperous until the copied bug shows up.

The life expectancy of Bitcoin still needs time to be proved. Recently, the government and corporation business will not allowed the currency be replaced, because this will risk their profit. When it comes to currency trading and circulation, it needs to be supervised and controlled by government and bank. Thus, it can make profit through currency flow.

Right now the government decided to fight against these Bitcoin by defaming them (for example, the government saying that those Bitcoin are come from gambling, drug deal and other illegal activity). And therefore forbid those Bitcoin. However, time will prove whether the global sensation “Bitcoin” will

keep on developing or collapsing under the defense from government. Furthermore, the security of Bitcoin is still unknown, so does its terminal.

5. Using Status of Bitcoin

Let's list the news about Bitcoin to show that it is a new trend about the global market.

Example 1: Four-years earlier, Kristoffer Koch, a Norwegian who had buy Bitcoin is now reaching to thirty-thousand time than original, valued 880000. Four years before, Koch spend 26 U.S. on a virtual currency which is still unknown at that time. At the end, the sum in April 2013, that 26 U.S. is already have a big curve and reach to 885,520 U.S. Koch didn't expect that at first.

In 2009, when Koch is working on an on-code technology report, he finds a virtual currency that was not on market yet. He buys it without thinking too deeply, then, he forgot it until April 2013. In a very short time in 2013, all the media starts focus on a new term called Bitcoin, and report it as a currency that it's valued is unlimited growing. So, Koch recalls the trade he makes before. When he opened the account that he almost forgot the code, guess what he saw? The value of the 500 Bitcoin that he bought before is already unexpectedly. The most important is that when he opened the Bitcoin account, the value was over than five million krone or ninety thousand U.S. dollars. It is hard to describe the feeling when your money multiplies many times. Afterward, Koch made some achievement to buy the most expensive house in Norway. After he got the accident money, the memory of virtual money shows up. Koch said that his friend criticized him as an idiot to buy virtual money with fake one. However, it is a giant wealth better than before.

Example 2: The value of Bitcoin mark up over one thousand U.S. dollars within ten days. In November, 2013, the value of Bitcoin rose eight hundred dollars, and then kept up and down around one thousand dollars. It was stable during that time. An IT manufacturer got seventy five thousand Bicoin, and he threw the hard ware away which means he lost two hundred million New Taiwan dollars. Recently, the other virtual currency begin to appreciate, maybe the real currency will be replaced by virtual currency someday.

An anchor from CNN said: "The value of Bitcoin rose seventy six hundred percent." The word "Bitcoin" was compiled to Oxford Dictionary. The anchor from CCTV said "Bitcoin influenced U.S. dollars significantly." In November 2013, the financial function of Bitcoin was recognized. Fed Chairman Ben Bernanke affirms it is prospective. The CNN anchor recorded that Bitcoin made the record again and again to reach over than one thousand dollars. It rose to four hundred percent in November 2013. In the London Exhibition, lots of relative businessmen analyzed the future of Bitcoin, and they congratulated each other about the good result.

However, An Britain IT manufacturer, Howle felt regretful a day after another day when he spoiled his beverage on his laptop. He discarded his hard ware and forgot that he got seventy hundred Bitcoin. He lost seventy five million U.S. dollars. He found out how stupid he was, and tried to hire somebody to find his hard ware from landfill. He also said:" The first time he touched Bitcoin, he predicted it would be a good invest. However, I still feel regretful when I did the stupid thing." It is good to recognize the value and benefit of virtual currency. The second famous virtual currency, Litecoin does lots of achievement like Bitcoin. Litecoin could exchange forty nine U.S. dollars, also the market gross price in rise to eleven billion in twenty four hours. The third famous virtual currency, Peer coin, gross twenty two percents. The fourth famous virtual

currency, Nmecoina, also gross seventy percents. Bloomberg reporter said" the biggest issue is that why does Bitcoin gross so much? Is this necessary?" Europe faced debt crisis, Greek and Spanish do not trust the financial strategy.

Without the control and management from government, some businessmen trade with virtual currency and make less risk. The circulation of Bitcoin is visible, and its limited amount can reach to twenty one million units; Litecoin can reach to eighty four million units. CNN anchor said: "Do you think Bitcoin will last longer than ten years in a long term?" Bitcoin Payment Company CEO, Gailey said:" Of course, we think this an extremely important technological creation. It also might be the most significant invention in 21st century". Professors agree with that and take email for example. Virtual currency is suitable in Digital Age, and it might replace the traditional financial organization. CNN reporter Monica said:" Lots of people predict Chinese have more ability to avail of of Bitcoin. Furthermore, it might be legal in Africa, because they have worse financial situation". Bitcoin has some advantages like anonymity, shorter transaction time and less regulation.

Some people worried about Bitcoin currency will foam, because it is also an illegal trading media. America New York editor states that "On the other hand, more people concentrate on regarding Bitcoin as an investment, the less Bitcoin flow in the market. The result will cause devalue the Bitcoin, and this is immature and confusing". The pros and cons brought by new currency still need time to prove.

6. Conclusions

Bitcoin sweep across the world and brought global sensation, no one knows it would cause sensation in 2013. No matter the economic benefit, freedom and reliability will challenge so called traditional financial and governmental institution. Some people worry about not relying on governmental supervision but strong calculation and cryptograph. However, Bitcoin keeps evolution, so the amount of Block chain, speed of transaction, irreversibility, the probability of being hacked will be solved by the third service and protocol.

Therefore, Bitcoin maybe become a revolutionary currency in the Digital Age. The most important of all, governmental institution will not allow it grows as infinite as possible. The prelude of war is begins gradually, let us wait and see now.

Acknoledgment

This work was supported by MOST 104-2623-E-145-001-D.

References

[1] The Bitcoin wiki. Available online at https://bitcoin.it.
[2] The DARPA network challenge. Available online at http://archive.darpa.mil/network challenge/.
[3] Joshua Davis. The crypto-currency: Bitcoin and its mysterious inventor. **(2011)** October 10; The New Yorker.
[4] Kirill Dyagilev, Shie Mannor, and Elad Yom-Tov. Generative models for rapid information propagation. Proceedings of the First Workshop on Social Media Analytics, SOMA '10, **(2010)** ACM pages 35–43, New York, USA.
[5] Yuval Emek, Ron Karidi, Moshe Tennenholtz, and Aviv Zohar. Mechanisms for multi-level marketing. Proceedings of the 12th ACM conference on Electronic commerce, EC '11, **(2011)** ACM pages 209–218, New York, USA.

[6] Jon Kleinberg and Prabhakar Raghavan. Query incentive networks. Proceedings of the 46th IEEE Symposium on Foundations of Computer Science, **(2005)** pages 132–141.
[7] Paul Krugman. Golden cyberfetters. Available online at http://krugman.blogs. nytimes.com/2011/09/07/golden-cyberfetters/.
[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available online at http://bitcoin.org/bitcoin.pdf, **(2008)**.
[9] Galen Pickard, Iyad Rahwan, Wei Pan, Manuel Cebri´an, Riley Crane, Anmol Madan, and Alex Pentland. Time critical social mobilization: The darpa network challenge winning strategy. CoRR, abs/1008.3172, **(2010)**.
[10] Fergal Reid and Martin Harrigan. An analysis of anonymity in the Bitcoin system. CoRR, arXiv/1107.4524, **(2011)**.
[11] S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to Better - How to Make Bitcoin a Better Currency. Proceedings of Financial Cryptography and Data Security, **(2012)**.
[12] J. Clark and A. Essex. (Short Paper) CommitCoin: Carbon Dating Commitments with Bitcoin. Proceedings of Financial Cryptography and Data Security, **(2012)**.
[13] G. Karame, E. Androulaki, and S. Capkun. Double-Spending Fast Payments in Bitcoin. Proceedings of ACM CCS, **(2012)**.

Authors

Kai Chain, he received the M.S. degree in Electrical Engineering from National Taiwan University in 2001-2003. He is an assistant professor in the Department of Computer and Information Science at the Republic of China Military Academy. He is currently pursuing his Ph.D. degree in Cryptography from the Institute of Computer Science and Communication Engineering at National Cheng Kung University under Profs. Chi-Sung Laih and Jar-Ferr Yang. His research interests include Network and Information Security, with a concentration on applied Cryptography.

Yao-Ren Wen, he received the B.S. degree in Computer and Information Science from the Republic of China Military Academy in 2014. His research interest is information security.

