A Study on the Comparative Analysis of Bitcoin Miner

Jong-Bae Kim, Hyungwoo Park

Abstract*: *Many of the cryptocurrency, such as bitcoin, have introduced a job proof scheme for the normal operation of the block chain network. This is entirely dependent on the computing power of the participating computer, and Satoshi Nakamoto has described it as "one-CPU-one-vote" in his paper on bitcoin. In order to maintain the block-chain network, a series of operations carried out by the node is called mining. In the early days of the bitcoin, Bitcoin Client (now Bitcoin-Core) was itself a mining software, and the mining hardware was a plain PC CPU. At that time, Satoshi Nakamoto advocated mining using only the CPU, saying, "Anyone can compete fairly equally (CPU mining) is good", and postpone the GPU arms race. However, the SHA-256 hash algorithm used in the bitcoin was, by its nature, overwhelmingly faster than GPU-based computation over CPU, which meant that it would be money. This led to the GPU mining boom, which continued until around 2014. However, this plot collapsed sharply as mining equipment using ASIC appeared. ASIC refers to an application-specific semiconductor, in this case an integrated circuit designed to perform only mining operations from the hardware stage. The ASIC mining equipment, led by Bitmain's Antminer, was nothing but a useless piece of silicon except that the mining performance was so fast that it could not be compared to CPU or GPU, so we replaced the GPU mining equipment at a rapid pace. As the ASIC digger manufacturer and the holder of the digger are positioned as a force and begin to threaten the identity of the bitcoin called "one-CPU-one-vote" and "decentralization", passwords such as the latecomer Etherium are difficult to manufacture ASIC and has begun adopting a proprietary hash algorithm. This has sparked demand for GPU mining again, and by 2017 it has resulted in a massive shortage of graphics card supplies. This paper analyses the problems of various mining methods and compares the performance. This will expand the range of mining methods that users can choose from, and suggest ways that various users can easily participate.

Index Terms*: *bitcoin, cryptocurrency, Miner, ASIC, GPU

I. INTRODUCTION

Block chains, beat coins, virtual currency, and many others are words you might have heard once or twice. Theoretically, it is almost impossible to manipulate and the stored records can re-main "almost" permanently, which is a topic of discussion among many academics and industry including security academics. As a result, block chains are being used in various industries as well as virtual money. Government agencies, startups, and large corporations, and have been actively researched and utilized in the field of security. In particular, IBM and Microsoft are attempting to integrate cloud services or block of chains with Internet of Things (IoT).

Block Chain can be defined as a decentralization technique by recording and managing the transaction record and management authority through a P2P network composed of peers, as a block. That is, it is also called a public transaction book, and it is also a technique to prevent hacking damage when it is intended to deal with encrypted currency. Recently, it is the digital book that the transaction is sequentially and publicly recorded such as bit coin and Etherium based on the encryption money system.

Bitcoin is a virtual currency developed in 2009 by a person named Nakamoto Satoshi. It is characterized by the transaction without central control through a decentralized public transaction book called a block chain. In 2014, the FBI auctioned out 50,000 Bitcoins from cyber-black market Silk Road [1]. The Japanese government also revised the law on virtual money in May 2016 to foster virtual money-related industries and changed the establishment of a bit coin exchange to a registration fee and added an audit obligation [2]. Bitcoin has already been recognized globally as electronic money.

The bit coin is issued through an act called mining. Currently, a dedicated mining machine called ASIC (Application Specific Integrated Circuit) mined most bit coins. If a small number of miners with high mining capacity monopolize the mining, the possibility of threatening the decentralization of the block chain, that is, the base of the bit coin, is increased. With the advent of this exclusive mining machine, a few miners have the ability to mined a large number of bit coins.

Therefore, this paper analyzes the problems of ASIC mining method in terms of block chain decentralization and propose a GPU mining method to solve the problem based on the development of the current GPU performance rather than the past GPU. In this paper, we compare the mining performance of ASIC and GPU mining methods to show that the general mining ability of home computer is sufficient. This suggests a direction for many miners to participate in mining. We expect that the block chain will be decentralized and the bit coin stability will increase as a result.

Revised Manuscript Received on December 22, 2018.

Jong-Bae Kim, Startup Support Foundation, Soongsil University, 369, Sangdo-Ro, Dongjak-Gu, Seoul, 06978, Korea (e-mail : kjb123@ssu.ac.kr)

Hyungwoo Park, School of Electonic Engineering, Soongsil University, 369, Sangdo-Ro, Dongjak-Gu, Seoul, 06978, Korea
(e-mail : pphw@ssu.ac.kr)

II. RELATED WORKS

A. Blockchain

A block is a record in a block chain that holds and acknowledges a number of waiting transactions. A blockchain is a public statement of chronologically listed bit coin transactions. The block-chain is shared among all users and is used for verifying the persistence of bit coin transactions and for preventing duplication [7]. The blockchain is a structure that is open to all trading participants, not to keep transaction records on a central server. Block-chain is designed to be difficult for an arbitrary operation because network participants are storing and verifying data in a form similar to a distributed database.

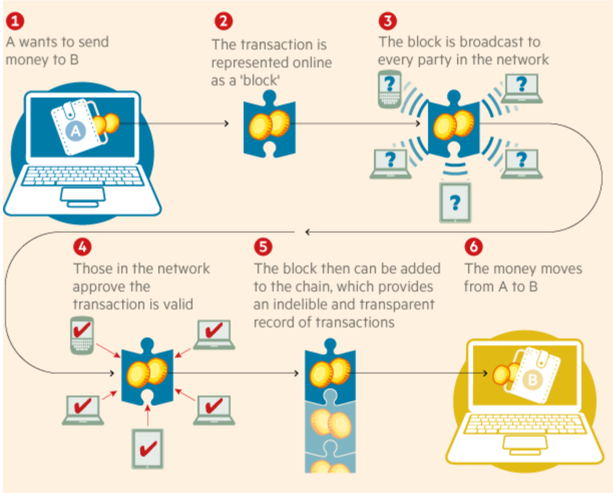
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
A
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

Fig. 1: Concept of the Blockchain

The blockchain creates a 'block' that records all transaction information that occurred during 10 minutes and transmits it to all the members and connects to the existing blockchain only when the validity is confirmed [8].

The block chain consists of four basic technologies: P2P network, encryption, distributed book, and distribution agreement. Because of this feature, block chain technology has recently been adopted where security and reliability are required, such as encryption, shared economy application, copyright payment system. The distributed consensus is a protocol that draws consensus on specific data values between processes or agents to achieve over-all system reliability. In the case of bit coin, it uses a protocol called Proof of Work. In addition, it is possible to store variables and functions in the block chain as well as variables and functions, so that Smart Contract, which can avoid excessive CPU consumption, and the application possibility of a new block chain service is suggested. In addition, Smart Grid and SD-IoT (Software Defined IoT) are presented in various fields in the IOT field. The Smart Grid is a smart grid that utilizes electricity and information and communication technologies to intelligently and advanced the use of renewable energy. By applying the block chain to the power grid, it is possible to construct a stable management system while reducing costs. SD-IoT is an application of SDN to IoT, which exposes virtual resources to facilitate privilege management and customization of IoT components [15].

With the expansion of the application range for the block chain, industrial and government interest is growing. In addition, each country is highly likely to use block-chain technology to secure the communication environment between devices in the core industry of the fourth industrial revolution era, IoT industry. In addition, it is possible to monitor and authenticate between trading partners, so that the fintech industry has brightened the prospects of a new business model by building new security and cost reduction system [16].

For example, Kodak and photo publisher WENN Digital announced KodakOne image rights management platform and KodakCoin through a licensing partnership. KodakCoin is a photo-centric block-chain-based encryption technology that allows photographers and agencies to more effectively control image rights management. When the original artist registers a photo, a block in which the copyright information is input is formed. When a consumer who wants to purchase the photo downloads a photo, the royalty is paid to the original artist by KodakCoin immediately according to the Smart Contract, it is a way to automatically distribute transaction information when another customer purchases additional photographs. Consumers are trying to create copyright management revenue through KodakCoin, which uses block-chain technology, such as Getty Images, which does not have to pay excessive commissions as in existing photo sharing platforms, and the original writer is also able to get higher royalty fees. The KodakOne platform provides ongoing web crawling to monitor and protect the intellectual property (IP) of images registered with the KodakOne system. If unlicensed image usage is detected, the KodakOne platform can efficiently manage the post-licensing process to compensate photographers [17].

On the other hand, the block chain technology is expected to be actively applied in the health care field. For example, there are 'Luna DNA Coin Project', 'Mord Project', 'BlockRx Flower', and 'Medi token (MED)' of the MediBlock platform. The purpose of the Luna DNA business model is to contribute directly to improving human health and quality of life. It is a business structure that allows people who receive DNA tests to provide their encrypted information to pharmaceutical companies for use in drug development and to receive compensation. On the other hand, the pharmaceutical industry takes the form of coin and information. This genetic information is used to drive drug development in the pharmaceutical and biotechnology industries. Pharmaceutical companies and biotechnology companies need a Luna DNA coin to access a database of Luna DNA. Luna DNA's block chain technology allows the community that provided the data to own a database created by Luna DNA. As more value is added to the database, members are rewarded with coins and ownership. New drug development success and other commercial accomplishments will be shared with data providers.

The remaining surplus will also be used to purchase tokens and distribute them to the community. Later, Luna DNA will work with the Luna community to collect health, medical, environmental and biometric data. These are likely to develop precision drugs and be valuable for important gene markers [16].

B. *Virtual Currency*

Bitcoin is a virtual currency developed by a person named Nakamoto Satoshi in January 2009 [3]. BitCoin does not have a central control authority that issues bit coins with P2P distributed digital encryption. And because it is issued only through the process of mining, the amount is fixed and is not influenced by inflation. The person or group who mined the bit coin is called a miner. They unlock complex mathematical ciphers and receive bit coins as much as they cost. The bit coin guarantees the anonymity of the user, so the personal information protection function is excellent. This approach can be useful in underdeveloped countries where access to the financial system is inadequate or high commissions have to be paid because central control agencies are not needed [4].

And as shown in Figure 2, bit coin is a bidirectional virtual currency unlike other electronic money. An example of a closed virtual currency is game money, and an example of a unidirectional virtual currency is Cyworld acorn [5]. However, unlike the electronic money, the bit coin can buy real money, purchase goods, or provide services [5].

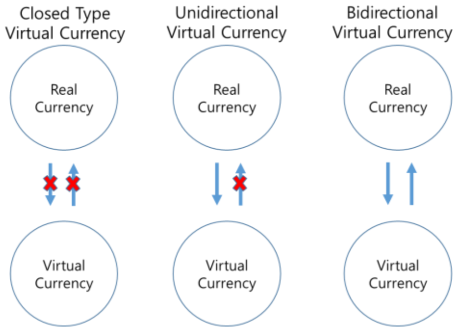
Closed Type Virtual Currency
Unidirectional Virtual Currency
Bidirectional Virtual Currency
Real Currency
Real Currency
Real Currency
Virtual Currency
Virtual Currency
Virtual Currency

Fig. 2: Comparison of Real vs. Virtual Currency

Bitcoin can be directly paid online using electronic cash that is traded in the P2P without going through financial institutions [3]. We solved the problem of the existing electronic money by solving the double payment problem not only through digital signature but also through the P2P network. Bitcoin has already been used for remittance and as of 2014, the amount of remittances is 222 million per month, which is more than the total transaction value of the existing money order and western union, which is over 216 million won [18]. But bit coin is limited due to high price volatility, low price predictability, and risk management limitations for currency in everyday life. Because it takes at least 10 minutes before the final approval due to the long transaction approval time, there is a technical limitation of the bit coin itself in using the micro payment system such as the traffic card. In addition, bit coin lowers the transaction cost of individual use, but it actually costs more than cash or debit cards because it uses much electricity during mining [19].

Nonetheless, many central governments, including Britain, Canada, and China, are considering currency issuance using encrypted currency technologies such as Bitcoin. There is also positive analysis that if we make digital money that can be accessed by all countries and give interest, we can increase GDP by 3%, stabilize the business cycle, and reduce the shock caused by the failure to control the call volume. Bitcoin, in particular, is free from the risk of cost savings and brokerage bankruptcy and is an alternative to the legal currency issued by the central bank [20].

Figure 3 shows the cumulative amount of bit coins mined to date(https://www.blockchain.com/ko/charts/total-bitcoins?timespan=all&showDataPoints=true). We can see that the amount of bit coin mined decreases over time. This is because the bit coin is set so that the total amount of bit coin mined at the time of first development is reduced, and the amount of mined at a time decreases [6].

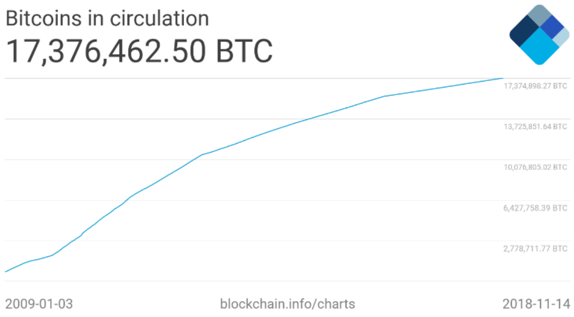

Fig. 3: Cumulative amount of bit coins mined

III. PROBLEMS OF MINING METHOD

At first, bitcoin was mined using CPU. But the CPU has only two or four processors, so the mining speed is slow. After that, we began to mining bit coins using GPUs with hundreds of processors to speed up the mining. Subsequently, in 2013, an application-specific integrated circuit (ASIC), which is a dedicated mining machine for mining only, was developed, and most of the miners are mined using ASIC.

Figure 4 shows the estimated number of bit coin diggers. It can be seen that the number of diggers has increased rapidly since 2013 when ASIC appeared [9].

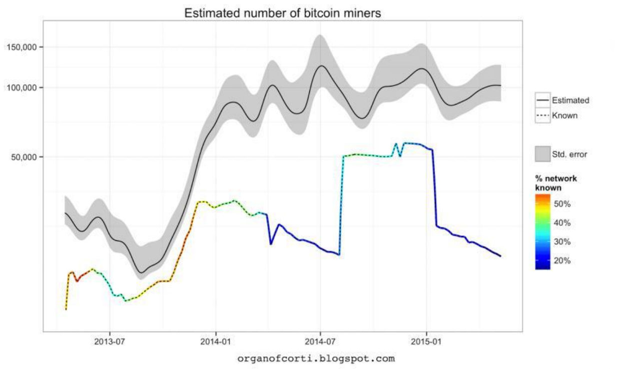

Fig. 4: Estimated number of bitcoin miners

When mining ability is concentrated on miners who have excellent mining ability by using the exclusive mining machine, the block chain which is the basic concept of bit coin is not dispersed and the possibility of modulation of the block chain is increased. In other words, selfish miners can unite and self-destruct mining that dominates the distributed network and dam-ages good-quality miners. To prevent selfish mining, the number of honest miners in the size of the whole pool should be at least two-thirds [10]. Considering that the GPU's mining ability cannot be a self-exploiting miner, the influx of miners using the GPU is an honest miner. Therefore, it is possible to reduce the possibility of modulating the block chain through the penetration of diggers using GPU.

IV. RESULTS AND DISCUSSIONS COMPARISON OF ASIC AND GPU MINING CAPACITY

The reason for the change from the method of using the existing GPU to the method of mining with the exclusive excavator is because the miner's electricity consumption cost is not higher than the bit coin received by mining compensation. However, as can be seen in Figure 5, as the graphics card technology developed, the mining ability of the current graphics card developed more rapidly than the graphics card of 2010 [12]. Therefore, even if the mining efficiency is lower than that of the dedicated mining machine, it is expected that the mining reward will be profitable in the future. These benefits will motivate new miners to participate in mining. The recently released high-end graphics FPS game over watched more than 15 million players [11]. This means that about 15 million high-end graphics cards are being used. In addition, there are a lot of potential miners who have high-end graphics cards because of recent high-end games. By engaging these potential miners in the mining process, the size of the pool can be increased and the bit coin stability enhanced.

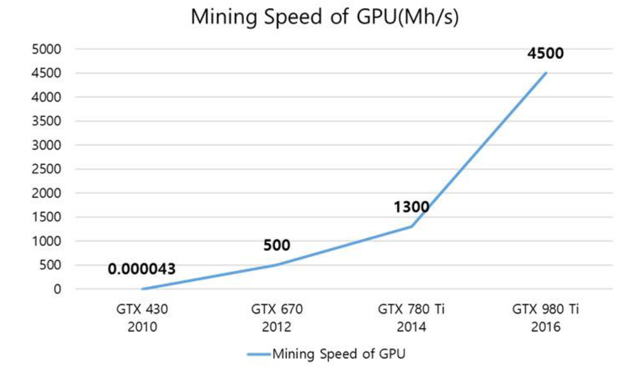

Fig. 5: Mining Speed of Gpu(Mh/s)

The following table is the ASIC and graphics card hash rate tables for 2013 [12, 13]. The hash rate is a measure of the processing capability of the bit coin network, which means that 1Mhash / s can perform 1 million calculations per second [14]. Comparing the two tables shows that there is a big difference in the bit-coin network processing capability of ASICs and graphics cards in 2013.

Table 1: Graphic Cards‘ and ASICs‘ Mhash/s retrieved in 2013

Graphic Card Model	Mhash /s	ASIC Product	Mhash/s
GTX 660 Ti	23	Avalon ASIC	66,300
GTX 680	15	ModMiner Quad	800
GTX 670	13	X6500 FPGA Min	400
GTX 760	9	BitForce SHA256 Single	832
GTX 770	12	Butterflylabs Mini Rig	25,200
GTX 780	20	-	-

The following table shows the hash rate comparison chart between ASIC and graphic cards in 2016[12, 13].

Table 2: Graphic Cards‘ and ASICs‘ Mhash/s retrieved in 2016

Graphic Card Model	Mhash /s	ASIC Product	Mhash/s
Titan X	1,980	AntMiner S7	4,730,000
GTX 980 Ti	4,500	Avalon 6	3,500,000
GTX 960 Gaming 2GOC	1,173	SP20 Jackson	1,500,000
GTX 1080	2,048	-	-
GTX 1060	1,800	-	-

In 2013, ASICs with the largest mining capacity in the table was 2882 times better than those with the largest mining capacity in the table. In 2016, ASICs with the largest mining capacity in the table were about 1051 times better than those with the largest mining capacity in the table. That is, the difference in mining ability between the ASIC and the graphics card is reduced by about two times.

In addition, the 2016 graphics card 's mining ability caught up with the mining capabilities of the 2013 ASIC. This shows that the current graphics card is capable of mining.

V. Conclusion

In this paper, we analyze the problems caused by the use of ASIC mining and show that we have developed past and present GPU performance. And we proposed a mining method using GPU as a solution to the problem. In addition, comparing the performance of the ASIC-based mining method with that of the GPU-based mining method, it has been shown that general home computers have sufficient mining capacity.

This comparison is meaningful as it suggests that the users of the general home computer, not ASIC, can participate in the new mining.

As a result of this study, it is expected that the size of the pool of the miner will be bigger and the possibility of self - mining, that is, the modulation of the block chain, will be lowered.

REFERENCES

1. http://www.yonhapnews.co.kr/bulletin/2014/11/18/0200000000AKR20141118036800091.HTML?input=1195m,Nov 18 (2014).
2. http://news.joins.com/article/20716182, Oct 13 (2016).
3. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2009).
4. Kyung-Mi Lee, Eun-Hee Koh, So-Hyun Joo. A Review of Bitcoin use in Korea, U.S., and Germany and its Implications for Creating Shared Value. Financial Planning Review. (2016), Vol.9, No.3, pp.85-111.
5. Hee Sung Yang, Yeong Mi Gwong, Internet Money – Trends of Bitcoin. Korea Multimedia Society Conference. (2015), Vol.19, No.1, pp.28-36.
6. https://blockchain.info/ko/charts/total-bitcoins?showDataPoints=true&timespan=all&daysAverageString=7 (2016)
7. https://bitcoin.org/ko/vocabulary#block-chain
8. Park Su-min, Kang Hee Jung, Jung Yun Jeong, Hong Seng-phil. A Suggestion for Secure Fintech Services based on Blockchain. Korean Soceity For Internet Information Conference. (2016), Vol.17, No.1, pp.117-118.
9. http://bravenewcoin.com/news/number-of-bitcoin-miners-far-higher-than-popular-estimates/ (2015).
10. Suryanto, T., Haseeb, M., & Hartani, N. H. (2018). The Correlates of Developing Green Supply Chain Management Practices: Firms Level Analysis in Malaysia. *Int. J Sup. Chain. Mgt Vol, 7*(5), 316.
11. JiYeon Yang, SoHee Kim, YoonJeong Kim. Bitcoin Vulnerability and Limitation Analysis of Current Countermeasure. Korean Institue of Information Scientists and Engineers Conference. (2015), pp.1013-1015.
12. https://www.engadget.com/2016/08/05/overwatch-15-million-players/
13. http://www.mininghwcomparison.com/list/index.php?brand=nvidia
14. https://en.bitcoin.it/wiki/Mining_hardware_comparison
15. https://bitcoin.org/ko/vocabulary#hash-rate
16. Jung-Sook Kim. "Service Status and Problem Analysis Based on Blockchain." The Society of Convergence Knowledge Transactions, 6.1 (2018.1): 135-140.
17. Lee, Jong - Ki. "An Exploratory Case Study of Distributed Ledger Processing Using IBM Bluemix Blockchain." Korean Computers and Accounting Review, 15.1 (2017.6): 25-38.
18. www.kodakcoin.com
19. Asghar, Eram, Aamer Ahmad Baqai, Ramshah Ahmad Toor, and Sara Ayub. "Co-Development of Process Planning and Structural Configurations Considering Machine's Accessibility in a Reconfigurable Setup." Review of Computer Engineering Research 3. 2 (2016): 41-46.
20. Yermack, D., "Is Bitcoin a real currency?," An economic appraisal (No. w19747). National Bureau of Economic Research, 2013.
21. Barrdear, John, and Michael Kumhof., "The macroeconomics of central bank issued digital currencies," 2016.

AUTHORS PROFILE

Jong-Bae Kim received his bachelor's degree of Business Administration in University of Seoul, Seoul (1995) and master's degree (2002), doctor‟s degree of Computer Science in Soongsil University, Seoul (2006). Now, he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.

Hyungwoo Park received a Ph.D., an M.S., and a B.S. in Electrical Engineering from Soongsil University. He is an assistant professor at the Information and Technology Department at Soongsil University, Seoul, Korea. His current research interest includes sound signal processing, big data analysis, voice analysis, noise reduction system, wave field synthesis, railway noise, and Internet of Things.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*