Understanding Blockchain technology and applications : A review

2019

KIM Seokju

Thesis for Bachelor's Degree

Understanding Blockchain technology and applications : A review

KIM Seokju

BS / EC

Gwangju Institute of Science and Technology

2019

Understanding Blockchain technology and applications : A review

블록체인 기술의 이해와 응용사례연구 : 리뷰 논문

Understanding Blockchain technology and applications : A review

Advisor : Professor Lee Heung-No

by

KIM Seokju

School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology

A dissertation(thesis) submitted to the faculty of the Gwangju Institute of Science and Technology in partial fulfillment of the requirements for the degree of Bachelor of Science in the School Of Electrical Engineering and Computer Science.

Gwangju, Republic of Korea
2019. 6. .
Approved by

_____
Professor Lee Heung-No
Committee Chair

Understanding Blockchain technology and applications : A review

KIM Seokju

Accepted in partial fulfillment of the requirements for the degree of degree of Bachelor of Science

June 2019

Committee Chair _____

Prof. Lee Heung-No

Committee Member _____

Prof. Ha Dae-Cheong

BS/EC

20115013

KIM Seokju(김석주). Understanding Blockchain technology and applications : A review(블록체인 기술의 이해와 응용사례 연구 : 리뷰논문). School of Electrical Engineering and Computer Science. 2019. 20p. Prof. Lee Heung-No

Abstract

Blockchain opened a new chapter with Bitcoin as a crypto currency. Blockchain technology provides data storage with resistance to modify. Crypto currencies are the new rising assets in global economy. In this paper, we aim in the reviewing blockchain technology. Understanding blockchain technology and researching case study of crypto currencies can show us the potentials of them. Smart contract can be the substitution for existing legal contract. Now the currency is in the area of engineering. Designing well engineered currency could be the great support to future society.

Keywords— Blockchain, Bitcoin, QE, DS, DS Attack, Ethereum, Crypto currency, Smart contract, PDSA.

Contents

I. INTRODUCTION

1. 1. Backgound

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks[1]. This message is contained in genesis block of Bitcoin. In 2008 there was a global financial crisis[2]. The start was from housing bubble burst in 2007. Many investment banks filed for bankruptcy in serial. When giant banks such as AIG and lehman brothers were about to go bankrupt, to prevent chain bankruptcies, US government bailed them out by enacting a new law. The treatment was Quantitative easing(QE). A monetary base of U.S. dollar was about $3 trillion after a series of QEs. But the impact of QE could be only directly to the tax-payers. From this point, financial authorities lost their faith. Among these situations, Bitcoin was born in 2009 January. Bitcoin is basically a digital ledger that shared by all participants in Bitcoin network. Bitcoin is actively traded worldwide and the market capitalization of Bitcoin is about $95,501,110,091(USD) on May 1, 2019[3]. There could be a question that 'how digital data can be a money?' Long time ago, doughnut-shaped giant stones were used as a money in Yap islands of western Micronesia[4]. These stones are called *Rai*(Yapese language) or stone money. The stones functioned as a banking system. The most important characteristic of money is the consensus among users. So with social agreement, a digital currency like Bitcoin can function as a money. If everyone has the same copy of a digital ledger and there has been no changes, everyone can trust the content of the ledger. In Bitcoin network a trustworthy ledger is added block by block. In every 10 minutes, a block that contains transaction informations is added. An electronic currency fundamentally has double spending problem. Because digital files can be easily copied.

Bitcoin solved this problem with proof of work algorithm. Understanding technological characteristic of Crypto currencies can give us a clue for future society.

1. 2. Nomenclature

ASIC	Application Specific Integrated Circuit
BTC	Bitcoin
DApp	Decetralized Applications
DPoS	Delegated Proof of Stake
DS	Double Spending
ETF	Exchange Traded Funds
FED	Federal Reserve Board
PoS	Proof of Stake
PoW	Proof of Work
P2P	Peer To Peer
QE	Quantitative easing
SEC	Securities and Exchange Commission
SHA	Secure Hash Algorithm
TPS	Transaction Per Seconds
UTXO	Unspent Transaction Output

II. SUBJECT

2. 1. Global financial crisis

In 2008 there was a global financial crisis[5]. The main cause was the housing bubble burst. Mortgage loan is a financial product that the bank lends money for guaranteed house. If the payer fails to pay loan money, the bank seizes the house and sells it. So mortgage loan doesn't damage the bank when the market price of house goes up. Subprime mortgage seemed safe for financial institutions. So many mortgage products sold in early 2000s. But in case of housing bubble pops, financial institutions are not able to withdraw original money. In 2007 April, the second biggest mortgage loan company applied for bankruptcy. This bankruptcy affected lots of financial companies. A lot of financial companies bankrupted globally. Finally giant financial companies like AIG, lehman brothers were about to bankrupt. If these giant financial companies bankrupt, it gives unrecoverable damage to U.S. economy. This is too-big-to-fail problem, if the size of failing company is too big, it would be disaster to U.S. economy. To prevent this problem, U.S. Government bailed them out based on law enforcement. The treatment was also a problem. The federal reserve bank of U.S. bought bad depts, to do that, they have minted a lot of U.S. dollars. What they actually did was increasing the valance of account electronically. In these situations, financial institutions lost their faith. People wanted a new financial system which is not dependent on trusted third financial institutions. With public needs, Bitcoin was born as a new crypto currency using blockchain technology.

2. 2. Bitcoin technology

Bitcoin is a electronic cash system in p2p network[6]. 2009 January 3, Bitcoin genesis block was created. Before Bitcoin code is published online, a person named Satoshi Nakamoto published white paper online. Bitcoin is so called 1th generation crypto currency. Because Bitcoin solved decentralization problem and double spending problem at the same time using proof of work algorithm. Bitcoin is basically a ledger. In Bitcoin network using proof of work algorithm, the amount of verified ledger is increasing. The basic unit of Bitcoin is a block. Blocks are chained in chronological order.

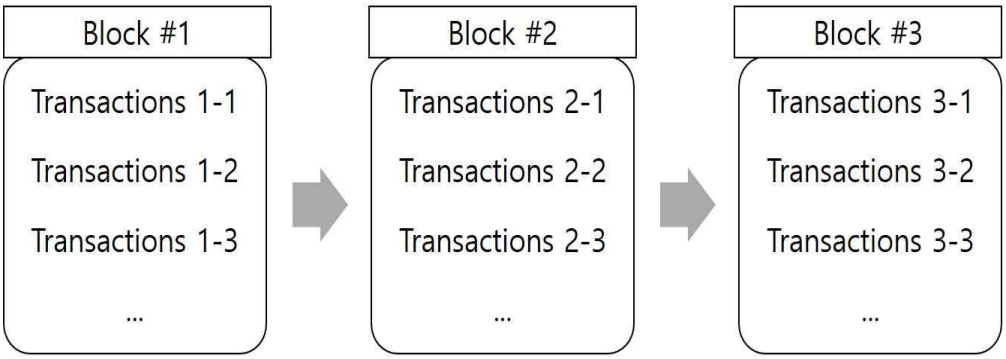

Figure 2.1

This data system is called ‘Linked list’. The most important thing in linked list is the connection. The previous block has the address of next block. Each block contains a pointer to the next block. In blockchain technology, each block has a value named hash. Hash value is the summary of present block.

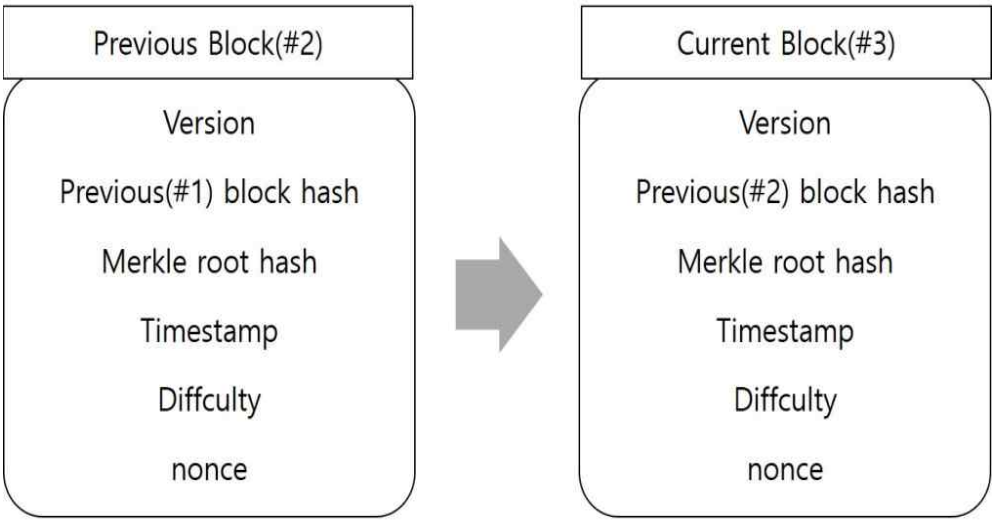

Figure 2.2

The informations contained in a block header are shown in Figure 2.2. The version is updated as the program code update. Each block has a block hash of the previous block. In figure shows block#2 has the block hash of block#1. In blockchain, each block hash transaction information s. They are stored in a binary tree. A merkle root hash is the root has h value of transaction tree. Timestamp is when the time block is genera ted obviously. To know what the difficulty is, we should know the block formation period of Bitcoin. Every 10 minutes, a new block is generated in Bitcoin network. When the participants in Bitcoin network become big ger, Bitcoin program increases difficulty level, it is programmed code. S o the average block formation period is kept around 10 minutes. Bitcoin mining is somewhat similar with winning the lottery. In mining process, miners tries to find the good hash value as the nonce value increasing. To understand about good hash value, we have know what SHA256 func tion is. SHA256 is a hash algorithm that takes random sized input and gives fixed sized output. The size of input field is $2^{8,000,000}$ in SHA256 alg orithm and the size of output field is 2^{256}.

Figure 2.3

Figure 2.3 shows the characteristic of the SHA256 function. A single addition of a dot gives totally different result in SHA256 function. Another characteristic of SHA256 function is Pre-image resistance. Making the output with the given input is fast but deriving the input value from output value is impossible in SHA256 function. In Bitcoin network, miner differs nonce value and find good hash value like hash values with multiple leading zeros. Miners voluntarily participate in mining process because if a miner succeeds to mine a block, he earns BTC as the block formation rewards. In early history of Bitcoin the block formation rewards was 50 BTC to encourage participating in the network. In every 4 years, the block formation rewards become half. Eventually after all mining process is done, the total amount of Bitcoin become 21 millions. In ordinary banking system an account has a valance, in Bitcoin a valance is represented by unspent transaction output(UTXO). Because Bitcoin is a digital ledger, the valance of an account is derived from the sum of unspent transaction output.

A Bitcoin trader only can broadcast his transaction with his UTXOs. In Bitcoin network, there are different types of nodes depending on its purpose. A full node keeps entire blocks in Bitcoin network, usually miners choose this type of node. A Light node only keeps informations in each block headers. These users usually trade Bitcoin using wallet program.

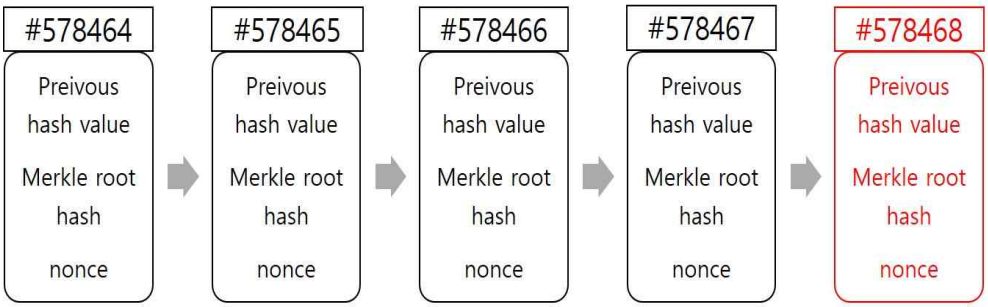

Figure 2.4

When a new block is created in Bitcoin network, each nodes in network verifies the new block. If the SHA256 output of the new block summary matches with broadcasted block hash value, the new block is accepted in the blockchain. If the hash value doesn't match in the verifying process, the new block is abandoned. Figure 2.4 shows a block failed in verifying process. Because the mining process is somewhat similar to winning a lottery, two different new blocks can be mined almost at the same time. In that case, blockchain always follows the longest chain. The characteristic that proofing is hard and verifying is easy is the most elegance part in the Bitcoin consensus algorithm. If a certain group has the more than 51% computing power of the total network, they can selectively adopt the new block in the blockchain. But the total number of nodes in Bitcoin network is more than 10,000, so it is really difficult to have more than half computing power of the total network.

Even if they have the half computing power of the total network, they only can take back the Bitcoin they spent in previous transaction. In peer-to-peer network, considering propagation time, a transaction is considered as a confirmed transaction after 6 new blocks are mined. The possibility modifying blockchain after 6 blocks is given with the calculations in the Bitcoin white paper[6]. Suppose there are honest node and attack node.

p = probability of an honest node mines the next block

q = probability of the attacker node mines the next block

q_z = probability of the attacker will ever overtake from z blocks behind

$$qz = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

$$\lambda = z\frac{q}{p}$$

$$\sum_{k=0}^{\infty} \frac{\lambda^e e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

From the result of this equation, the possibility that the attacker ever catches up converges to zero as the mining process proceeds. And waiting 6 blocks is safe for prevent attack.

2. 3. Re-centralization of Bitcoin and DS attack

Ordinary banking system is centralized in giant banks and financial institutions. The original purpose of Bitcoin was decentralization from the authorized third party. If a single individual node participates in mining process, the expected time the node mines new block is decades. So these individuals participate in mining pool and share their block formation rewards. There are many mining pool groups in Bitcoin network and they are geometrically located in the china. Another reason node gather around mining pool is the ASIC chips[7]. ASIC chip is Application specific integrated circuit. They are made for special purpose like mining chip for Bitcoin. A single mining chip has more than 10TH/s as a computing power. They are very powerful than normal computing machine.

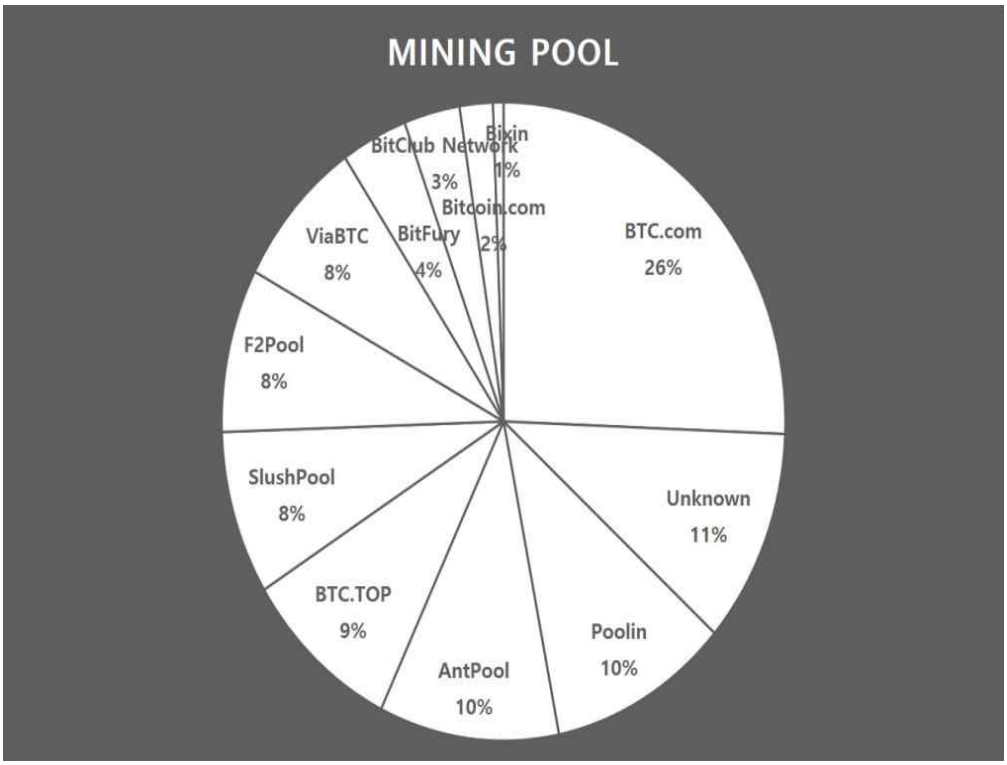

Figure 2.5

Figure 2.5 shows the mining pools in the Bitcoin network[8]. SlushPool is czech mining pool and the rest of top mining pools are chinese pools. So if the chinese pools unite, they can easily make a double spending attack. Double spending attack(DS attack) is canceling the latest spent BTC using large computing power. Double spending attack also consumes computing power, so honestly participating in minning process could more profitable. Still successful double spending attack makes possible taking back his recently used BTC, so there should be mathematical analysis of proper amount of BTC in a transaction. A pessimistic fact about double spending attack is the attack is possible under 50% computing power of the total network. According to an analysis[9], if the amount of BTC in a transaction is big enough, the attack is still profitable even with sub-50% computing power.

Provided temporary management of DS attack with sub-50% hash power is to wait enough number of blocks after the transaction is included in a block. Block confirmation number should be proportional to the amount BTC spent in the transaction. But the fundamental solution for mining pools and DS attack is neutralizing ASIC chips. Or an advent of new blockchain crypto currency with new network policy could be the another solution. Hardforking blockchain by foundation could be another option for resisting ASIC chips. But this treatment is only temporary measures, it cannot be the final solution for crypto currency economy. A try of neutralizing ASIC chips is Monero's CryptoNight algorithm. They modified the mining algorithm to resist with ASIC chips. This treatment makes ASIC chips for cryptonight algorithm not compatible with other crypto currency network. Also, an analysis shows that the cryptonight algorithm is not fully ASIC resistance[10]. Another research attempting for having ASIC resistance is ECC-POW algorithm. It adopted a modified hashing algorithm called ECC-POW. ECC-POW uses error correcting codes in communication engineering. It is actively researched in GIST. Proof of Stake(PoS) or Delegated proof of stake(DPoS) are another algorithms substituting Proof of work(Pow) algorithm. In PoS algorithm, nodes can mine a new block by chance proportional to his staked valance. PoS consumes much less energy in mining than Pow algorithm. In PoS algorithm 51% attack is more expensive than Pow algorithm does. Ethereum foundation has a plan for migrating to adopt PoS algorithm. In Delegated Proof of Stake, small entity participate in mining process. The entity is selected with voting by all network participants. Good thing about DPoS algorithm is capability of providing fast transaction speed. But PoS and DPoS both are not free with criticisms because of their centralization issues.

2. 4. Ethereum

Ethereum is decentralized application platform providing Smart Contract[11]. Vitalik Buterin founded Ethereum platform and it started in 2015 July 30. The main difference in Ethereum is providing platform for applications like contracts, SNS service, electronic vote. Ethereum is not only a crypto currency but also the decentralized platform of DApps. Ethereum provides many types of tokens. The representative type of token is ERC-20 tokens. On Ethereum platform users can buy tokens using ETH. Token economy operates on Ethereum platform is the powerful characteristic of Ethereum. Smart contract has unlimited application possibilities. Turing completeness of the smart contract makes possible of all programs that human can imagine. Smart contract on Ethereum platform can be very powerful substitutable option for ordinary contracts.

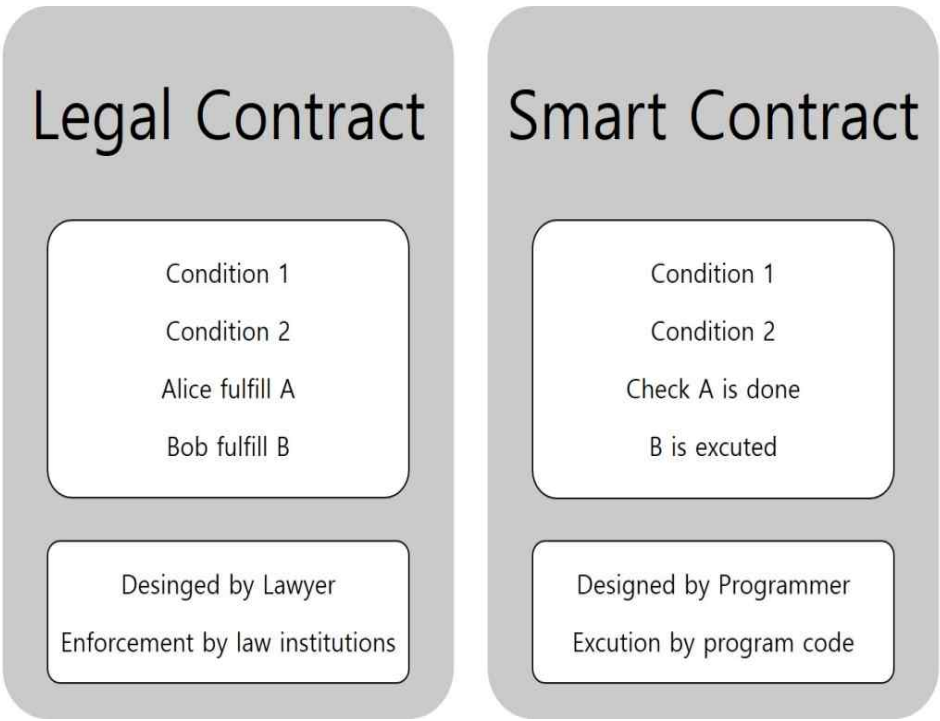

Figure 2.6

Figure 2.6 shows the differences between a legal contract and the smart contract. All legal contracts are programmable as the codes. A legal contract is designed by the lawyer on the other hand a smart contract is designed by a programmer. The powerful characteristic of Smart contract is auto-fulfilling of the contracted agreement. In a legal contract, enforcement of the contracted agreement forced by law institutions. But the legal contract doesn't always guarantee the enforcement of contracted agreement. On Ethereum platform all kinds of codes can be programmed. It could be harmful because an infinity loop can suspend the entire network. To prevent that situation Ethereum platform introduced a concept called 'Gas'. Gas is the resource for executing codes. Every code is executed after pre decided amount of gas is consumed. In this way, Ethereum prevent risk for whole system down by infinite code while providing turing completeness. But providing turing completeness is not always safe. In 2016 June 17, 3.6 million of ETH was stolen from DAO contract[12]. The hacker found the weaknesss of DAO contract and transferred ETH to his account. The solution Ethereum foundation proposed was the Hardforking Ethereum blockchain to go back to the state before the attack. This treatment also reminds decentralization issue because Ethereum foundation intervened in the network. From this case, we should be aware that turing completeness is not always good in a blockchain crypto currency. The reason Bitcoin only provide script language is not by lack of talent but the decisions for the safe and sound network.

2. 5. Blockchain technology itself

Blockchain itself is a good technology except crypto currency. Estonia introduced the e-government and accomplished remarkable success[13]. They switch all government institutions and infra services to online.

In this paper blockchain technology in estonian e-government will be focused. Since 2012 Estonia introduced blockchain in managing medical data, public document, all kinds of registering informations. Introducing blockchain technology to these areas can give the faith that informations cannot be modified or hacked. Thanks to blockchain technology, informations widely open and transparency is secured. The trait for accessing data is remained in the blockchain, so unreasonably access is prevented. As shown in this case, blockchain technology also can be applied in the field of database system. In the Ethereum network, 'Panmunjom Declaration' is stored[14]. This is a good example for preserving historical information in the blockchain. Busan harbor in South Korea introduced transporting system based on blockchain technology[15]. The status of shipping container can be provided, so the transportation company can make the best efficient plans in system. This example shows that the easy verification of information can improve all kinds of system. In Nowon district introduced local crypto currency using blochchain[16]. District crypto currency is a new trend in local governments. It contributes in activating local economy. Trending of local crypto currency is also an optimistic sign for crypto economy. This could be a potential to the currency design for future society.

2. 6. Crypto currency in Korean society

In Korean crypto economy, trades centered in coin exchanges are developed. The price of Bitcoin in Korean exchanges was much expensive than the price of global exchanges. This phenomenon is known as 'kimchi premium[17]. The trades in Korean crypto currency economy was very active in between 2017 and 2018.

The gambling investments like in certain types of trading stocks are observed in Korean crypto currency economy. Many crypto exchanges reserves tiny amount of crypto currencies than the volume of total trades. But this is not only issue for Korean exchanges, global exchanges shows the same aspects in reserving crypto currencies. Short sale in crypto exchanges also an issue. These tendencies affects on crypto economy is still not completely identified. ICO is the another trend in global crypto economy. Initial coin offering(ICO) is a funding system using crypto currencies. If a certain group offers coins for special purpose, donors fund and take coins as rewards. The first ICO was held by Mastercoin in July 2013[18]. The purpose of Mastercoin was making free-market system not leading by government. They made a system using blockchain technology without help of banks or financial institutions and it was very successful. Because ICO has the form of donation, it evades securities law but it is still controversial. Regulations on crypto currencies and ICOs are very hot and controversial topics in global market. SEC delayed the judgment on ETF product applied by Bitwise[19]. So the regulations on crypto currencies are not determined. In Korean society, crypto currencies are regulated without distinct laws or policies. But the regulations could not be permanent and Korean society would and should follows the global tendencies.

III. Discussion

In a main text, we covered the technical aspects of blockchain and it's current situation. In the ordinary computing, data can be easily copied and modified. One single approval of digital information takes many steps of complicated process. In that part, blockchain bears relative efficiency. Now we do many things using blockchain technology. Blockchain can give a true democracy with electronic voting system. Storaging data which needs to be verified is another strong part of blockchain. Crypto currency is the best active field adopting blockchain technology. Running a government is an assembling of personal opinion. Which is obvious, I think. Until now, we elected representatives and the government run by those representatives. Because it was the only way under technical and realistic issues. With blockchain, we can directly affect national policies. To do or not to do is another problem. The important thing is we can do now. The society is enthusiastic about 5G internet. But we can't use simple electronic voting system, which is irony. I always thought tax should be used in the way they support. Tax money is the essence of public people and which is sacred. In the future I hope tax payers gain tokens as a rewards and using the tokens, they increase the budget of national policy which they support.

Let's say about the necessities of crypto currency. It's definitely apocalypse world. The internet and network is connected partially but no safe and sound government. In that situation, we should depend on crypto currencies. The most probable scenario is the nuclear war. Surely the possibility of nuclear war converges to 0. By the way US and China are in the middle of trade war. They don't mind announce that they are prepared to take a military posture.

To consider in a realistic way, the significance of blockchain comes from Trust-based computing. It can provide us the efficiency. The nation is born to be stable. To keep stable, it grows bigger and bigger. The meaning of big government is having a complex hierarchy. It is directly connected to bringing inefficiency. Diet in inefficiency hierarchy is the most important assignment for good government. In 2008 Bitcoin was born because people didn't trust government and financial institutions. Now they recovered, I think the Diet should start from making crypto currency by government. Once they make, they only support by law and the currency is run by public nodes. I think this is the best way in global economy. Ripple(XRP) is a p2p based crypto currency that multiple banks developed in cooperation[20]. The advantage of Ripple is in transaction speed between countries. The market capitalization of Ripple is 3rd after Ethereum and their vision is also promising depending on the global tendency. Samsung electronic included crypto wallet service in Galaxy S10 smartphone. As the total amount of users for Samsung pay is more then 1.4 million[21], the accessibility for crypto currencies is greatly improved. The participation of public mass on crypto market is promising therefore Korean crypto economy has the chance for huge expansion.

Currency has the long history, It is almost the same with history of human being. But it never been researched and developed than these days. Now the currency step into the field of engineering. New coins are created and disappear everyday. In the meantime major currencies like Bitcoin and Ethereum hold their position stably. The total capital of crypto market is increasing every year. The scams and frauds would increase accordingly. To prepared that, Korean government should be open-minded and move in the right direction. Adjusting related laws and regulations are in a hurry.

IV. Conclusion

Understanding blockchain technology is important in current society. Considering crypto currencies as an asset and investment target, well understanding on technology could bear more efficient investment. Prof. Lee Heung-No said 'Now designing a currency is in the engineering part' and he emphasized the necessity of researching on crypto currency. The environment for co-developing crypto currencies should be prepared. Research and development on crypto currencies can be good contribution to future economy.

SUMMARY

Understanding Blockchain technology and applications : A review

블록체인은 암호화폐인 비트코인과 더불어 새로운 장을 열었다. 블록체인 기술은 위조 불가능한 데이터 저장방법을 제공한다. 암호화폐는 세계 경제에서 새롭게 떠오르는 자산이다. 이 논문에서 우리는 블록체인 기술을 이해하고 응용사례연구를 통해 미래사회의 단면을 엿보고자 한다. 블록체인 기술을 이해하고 암호화폐 응용사례를 연구에서 각각의 잠재력을 확인할 수 있다. 스마트 컨트랙트는 기존의 법리계약을 대체할 수 있다. 이흥노 교수님은 '이제 화폐도 공학의 범주에 들어오게 되었다' 말하며 암호화폐 연구의 필요성을 강조하셨다. 공학적인 화폐를 설계하는 것은 미래사회에서의 큰 토대가 될 수 있다.

Reference

[1] Francis Elliott, “Chancellor Alistair Darling on brink of second bailou t for banks”, TheTimes, 03-Jan-2009. [Online]. Available: ht tps://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

[2] Andrew K. Rose, Mark M. Spiegel, “Cross-Country Causes And Conse quences Of The 2008 Crisis: International Linkages And American Expos ure”, National Bureau Of Economic Research, Sep. 2009.

[3] CoinmarketCap, Bitcoin market capitalization, 01-May-2019. [Online] Available: https://coinmarketcap.com/currencies/bitcoin/historical-data/

[4] SCOTT M. FITZPATRICK, “A Radiocarbon Chronology of Yapese Ston e Money Quarries in Palau”, Micronesica 34(2):227-242, 2002.

[5] Eric Helleiner, “Understanding the 2007-2008 Global Financial Crisis Lessons for Scholars of International Political Economy”, Annu. Rev. Pol it. Sci. 2011.14-67.

[6] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Bitcoin.org, 01.Nov.2008.

[7] Ikuo Magaki, Moein Khazraee, ASIC Clouds: Specializing the Datacent er, 2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture.

[8] Blockchain, Mining pool, 31-May-2019, [Online] Available : https://w ww.blockchain.com/ko/pools?

[9] Jehyuk Jang, Heung-No Lee, “Profitable Double-Spending Attacks”, IE EE, Oct. 2018.

[10] Daren Tuzi, Cryptonight GPU Mining Efficiency, Tampere University of technology, Jun.2018.

Reference

[11] Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum Foundation, 2013.

[12] Nicola Atzei, Massimo Bartoletti, A survey of attacks on Ethereum smart contracts, IACR Cryptology ePrint Archive, 2016.

[13] Tarmo Kalvet, Innovation: A factor explaining e-government success in Estonia, Electronic Government, an International Journal, 2012.

[14] Wolfie Zhao, "Historic Korean Peace Declaration Recorded on Ethereum Blockchain", Coindesk, 02-May-2018. [Online] Available : https://www.coindesk.com/historic-korean-peace-declaration-recorded-on-ethereum-blockchain

[15] Yogita Khatri, South Korean Government Trials Blockchain for Shipping Efficiency Boost, Coindesk, 18-Dec-2018. [Online] Available : https://www.coindesk.com/south-korean-government-trials-blockchain-for-shipping-efficiency-boost

[16] Hyunsu Yim, "NW: Nowon District's Local Cryptocurrency", The Korean Bitwire, 18-Jan-2018. [Online] Available : http://koreabizwire.com/nw-nowon-districts-local-cryptocurrency/108057

[17] KJ Choi, A Lehar, "Bitcoin Microstructure and the Kimchi premium", papers.ssrn.com, 2018.

[18] ICO, Initial coin offereing, Wikipedia, 31-May-2019, [Online] Available : https://en.wikipedia.org/wiki/Initial_coin_offering#History

[19] Nikhilesh De, "SEC Again Delays Decision on Bitwise Bitcoin ETF Approval", Coindesk, 14-May-2019. [Online] Available : https://www.coindesk.com/sec-again-delays-decision-on-bitwise-bitcoin-etf-approval

[20] F Armknecht, GO Karame, "Ripple: Overview and outlook", Conference on Trust , 2015.

[21] KIM Jihyo, "삼성전자 '삼성페이' 국내 가입자 1400만 명, 누적결제 40조 달성", Bussinesspost, 14-May-2019. [Online] Available : http://www.businesspost.co.kr/BP?command=naver&num=127164

감사의 글

처음 블록체인 연구실 인턴에 지원했을 때, 선입견 없이 저를 받아들여 주셨을 때 제가 받은 감동은 말로 이루어 표현할 수 없습니다. 따듯한 마음으로 저를 받아들여 주신 이흥노 교수님께 감사드립니다.

인포랩에서 블록체인을 공부할 기회를 가진 것은 저에게 영광이었습니다. 블록체인 경제특론에서 다양한 분야에 걸쳐 좋은 강의를 해주신 연사님들께도 감사드립니다. 이 논문을 작성하는 것에 많은 영감과 힘이 되었습니다.

저의 논문 지도교수님을 맡아주신 이흥노 교수님께는 다시 한번 감사의 말씀을 드립니다. 모자라고 부족한 저를 가르쳐 주셔서 감사합니다.

연구실에서 저를 따듯하게 챙겨줬던 형들께 감사의 말을 드립니다. 형들이 저를 따뜻하게 챙겨주셔서 연구실에 적응하고 블록체인 공부를 원활히 할 수 있었습니다.

저를 낳아주신 부모님, 드디어 졸업할 수 있을 것 같습니다. 항상 사랑합니다.

이 력 서

성 명 : 김 석 주

생년월일 : 1992년 08월 31일

출 생 지 : 대한민국 광주광역시

본 적 : 대한민국 광주광역시

학 력

2011 - 2019 ..... (B.S.)