Journal of Digital Convergence
Vol. 16. No. 8, pp. 201-210, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.8.201

A Study on Blockchain Networking for Internet of Things

Il-Gu Lee
Assistant Professor, Department of Convergence Security Engineering, Sungshin University

사물인터넷을 위한 블록체인 네트워킹에 대한 연구

이일구
성신여자대학교 융합보안공학과 조교수

Abstract High expectations are posed on the blockchain-based internet of things (IoT), in which IoT and blockchain technology is combined to obtain trust in the Internet, where trust appears impossible to obtain. However, applications of current blockchain-based IoT technology to real-world scenarios appears to be significantly more difficult owing to limitations regarding scalability and security. In this paper, the difficulties to implement blockchain networking technologies for IoT and digital businesses are investigated and practical solutions such as sharding, off-chain, de-idetification and P2P crypto-currency exchange are explored. In further work, a blockchain platform for IoTs which provides scalability and security will be implemented according to this research results, and compared with conventional blockchain platforms.

Key Words : Blockchain, Internet of Things, Networking, Security, Integrity

요 약 신뢰하기 어려운 인터넷 환경에서 신뢰를 확보하기 위해 블록체인 기술을 사물인터넷 (IoT · Internet of Things)에 적용한 '블록체인 기반 IoT'에 대한 기대감이 높다. 그러나 현재의 블록체인 기반의 IoT 기술은 확장성과 보안성 측면에서 실생활에 응용하기에 한계가 있는 것으로 보인다. 본 논문에서는 최근 각광받는 사물인터넷 디지털 비즈니스를 실현시키기 위한 블록체인 네트워킹 기술의 확장성과 보안성 난제를 고찰하고 정책과 샤딩, 오프체인, 비식별화, P2P 암호화폐 교환 등의 기술적 해결 방안 도입을 제안한다. 후속 연구에서는 본 연구 결과를 바탕으로 보안성과 확장성을 보장하는 사물인터넷 블록체인 플랫폼을 구현하고 기존의 블록체인 플랫폼과 비교할 계획이다.

주제어 : 블록체인, 사물인터넷, 네트워킹, 보안, 무결성

1. Introduction: Blockchain-based IoT

Internet of Things(IoT) is one of the essential infrastructures in the fourth industrial revolution where devices connect to each other, systematize, and establish smart networks creating a smart city. Nevertheless, if everything is connected to the central server, all types of side effects arise in addition to convenience. An enormous maintenance cost is incurred, security becomes fragile, and scalability and stability deteriorate. To tackle these problems, 'blockchain based IoT' is proposed [1-3].

Then how is 'IoT' and "blockchain-based IoT" different from each other? Firstly, IoT is initiated from the concept called "things connected to the Internet." Now, this evolved into 'swarm intelligence' where

*This work was supported by the Sungshin Women's University Research Grant of 2018-1-28-001/1
-본 연구는 성신여자대학교 연구과제 (2018-1-28-001/1) 지원으로 수행하였음.
*Corresponding Author : Il-Gu Lee (iglee@sungshin.ac.kr)
Received July 4, 2018 Revised July 20, 2018
Accepted August 20, 2018 Published August 28, 2018

devices with intelligence cooperate and 'social intelligence' where users' behaviors and states are analyzed to provide optimized services.

Intelligent IoTs known as FinTech, connected cars, drones, wearable devices, transplantable medical devices, and smart grid are predicted to enhance the quality of life of human beings to become better and richer. An era where smart devices perform tasks that require a lot of time, effort, and costs has started.

In reality, many industries have adopted and applied blockchain technologies [4].

Financial service industries and enterprises are fiercely and competitively adopting blockchain technologies. Credit card service industries established using blockchain-based individual authentication certificates, enabling integrated login service, and guaranteeing safe one-click use across services and applications [5, 6]. Korea Securities Depository has finished verifying the blockchain-based electronic voting system technology and is building an electronic security system to improve the participation rate of stockholders in general meetings[7]. Industries are applying blockchains in the manufacturers' electronic contract systems and in supply chain management, thereby expanding the use cases into industries in general [8].

In medical industries, access to patients' information is only allowed within hospital networks and medical data application is very limited due to the privacy policy. It is also difficult to view patients' data that is scattered in different hospitals. Hence, managing medical data can lead to enormous costs [9]. If blockchain technologies are incorporated into medical data, an integrated medical data management system can be realized and any patient can view his/her medical records, separate ledgers safely using their keys in the places connected to the Internet, and can manage them at a cheap cost.

Public infrastructure and energy industries expect that blockchain will put up a smart grid with a distributed electricity infrastructure in advance [10]. In a blockchain-based smart grid environment, using a blockchain-based energy distribution and transaction platform where energy production, consumption, and surplus are recorded and made transactable and efficient, the industries can provide visible and convenient electricity management. Electricity user will get energy prices based on their electricity consumption by time, and credits provided as virtual currency mining will be based on the use, environment, and contribution to energy saving.

There is only one obstacle for all of us to tackle. As intelligent IoTs trade important data regarding human life, property, and social safety, they should be 'accountable and safe.' However, the reality is far from that. A global security company, Symantec, indicated that "600% increase in attacks against IoT devices and IoTs are exposed to security fragilities," and warned that "they can turn into the main income sources for cybercrimes with financial and political purposes" [11]. If a hacker hacks a database and falsifies or modifies data, the whole IoT network will collapse.

Even when people engage in economic and social activities, trust among the stakeholders is essential. Similarly, in IoT where objects exchange information, trust towards the other party and data are essential. Therefore, IoT devices are built after a thorough contemplation on the security aspects and they optimize security environments by collaborating with each other. However, the computing power in normal IoT devices is low. The traditional security technologies applied to PCs or mobile devices cannot be applied to IoT devices. Since the product prices are low and security fragile, it is easier for hackers to attack these devices.

Then, how can blockchains solve these problems? A blockchain is a technology that distributes and saves a data unit called a block by connecting it to a chain in every given amount of time. A multiple number of network participants test the validity and approve the revealed data. This enables effective and safe data transactions among stakeholders without any third-party authority. A well-known industry that

applied the blockchain technology is the virtual currency sector where counterfeiting and falsifying of currencies are forbidden, and quick and safe validation and processing are feasible.

High hopes are put on the 'blockchain-based IoT' where blockchain technology was incorporated into IoT [12, 13]. Due to the distribution structure, it is possible to prevent a DDoS attack. This is because the system where each node has data and is tested makes it difficult to counterfeit or falsify data. Although devices are connected, the overall effect is minimal even when some of the devices have problems. Moreover, with the connection of nodes in the system, new nodes can be easily added increasing scalability. In addition to this, as the whole system is established by connecting the IoT devices compared to the traditional IoT system with center services, costs can be saved considerably.

Consequentially, blockchain technology can be applied to IoT data management, transactions, and authentication. Blockchains have the potential to extend beyond IoT. This is the reason why the technology is in the spotlight as a future growth driver.

In the paper, chapter 2 examines the trustworthiness of blockchain-based IoT and chapter 3 illustrates security and transparency. In the following chapter 4, analysis of technological limitations of blockchain-based IoT and solutions to them are provided followed by the conclusion in chapter 5.

2. Requirements for Blockchain-based IoT Networking

2.1 Trustworthiness of Blockchain-based IoT

In 1990, Tim Berners-Lee invented world wide web to link all information on the web, verifying facts, creating ideas, selling and buying of products, and networking with new people will be done at a speed and a scale which was unimaginable back in the analogue era[14]. The world has become the place he predicted.

Nakamoto Satoshi who proposed the bitcoin in 2008 in the paper 'Bitcoin: Peer to Peer Electronic Cash System,' addressed that "stakeholders can pay online without any financial institutions and through encoded verification, the central security institution is replaceable" [15]. Similar to Satoshi's proposal, the alpha and omega of blockchains is 'trust.' Blockchains completely scrapped the traditional meaning of 'trust' and redefined the term. Nakamoto Satoshi asserted that "trust is based on individual relationship, not on the central institutions, and can be verified."

Each country in the world uses a reliable third-party institution like the government and central banks to verify information and guarantee transactions so that wrong information is filtered and the social system is managed in a more stable manner. However, users must bear considerable costs on their part and suffer from any possible damages caused by wrong policies and decisions of external institutions. If stakeholders can willingly trust and exchange without any third-party institutions, i.e., if distributed computing is feasible, then they will have lower costs and be free from the risks caused by external agencies.

However, there is a hurdle to reach a state where stakeholders can trust and transact, i.e., to filter the 'hackers' who hide everywhere to create false information. The technology to prevent the 'overlapping use' where one spends twice the money, is especially a typical dilemma in distributed computing. Microsoft Inc., also contemplated on how network participants could reach an agreement without a central control system [16]. The solution to this was the 'Byzantine General's Problem.' The blockchain solved this so-called Byzantine general's problem to detect hackers producing dilemmas and false information in unreliable distributed networks by hashing and using proof-of-work.

'Proof-of-work' refers to creating new blocks through mining. The process of mining involves finds 'hash' values and connects the blocks. Mining for virtual currencies commonly refers to the process of

finding the input value that satisfies the hash conditions given the output value in a transaction record in a given amount of time. Moreover, the one who finds the hash value that satisfies the given conditions are rewarded with cryptocurrency. Therefore, a multiple number of stakeholders divide the domains and mine, and if they win, they divide the compensations as well. Therefore, in case they successfully proved the mining tasks by obtaining a hash value, the previous transaction data are linked to existing blocks.

Of course, this is not the first time that the hash and proof-of-work techniques were adopted in the blockchain technology. This technique is very similar to the hashcash technologies that send evidence of hash calculation through an e-mail [17]. Hashcash technology has been used for a long time to exploit spam filtering and defend service rejection attacks. However, a number of experts believe that blockchain technology is a momentum that goes beyond Internet technology, which will bring about a new change in the world [18]. Why is it so? A blockchain not only uses the hashcash technology to go through proof-of-work, but it also connects blocks with the hash and is a platform to safely transact data by inducing competitive verifications of participants in the networks to enhance trust in the blockchains.

By making the hash value of the recently created block as the condition for creating hash values to include the previous hash value with the part of the data in the block to be created next, a blockchain is created by linking the previous block and next block with the hash value. Although it is difficult to obtain a hash value, once the value is derived, it is very easy to verify whether it is the correct answer. Consequently, participants in the blockchain network can readily and quickly verify whether the recent blockchain is proper and the blockchain completed with verification is spread throughout the whole network in an instant. The participants connected in the blockchain network will put the data into blocks and transfer them to other participants. Then, the data is recorded in the blockchain and participants collect them and continue linking the previous blockchains to new blockchains.

Ultimately, a blockchain with more blocks mean more participants' verification distributed within the network implying a higher trustworthiness or reliability. Therefore, each participant repeats the process of choosing longer blockchains and discarding shorter blockchains. Eventually, as the blockchain that survives in the end becomes the winner, and only one blockchain will remain valid, the risks of overlapping transactions are gone. In addition, as the probability to get compensated increases depending on how fast one accepts a longer blockchain and builds another block upon it, the participants in the network behave in a way that strengthens trustworthiness.

In this way, blockchain has used an innovative idea suggested as a solution to the 'Byzantine General's problem,' a seemingly unsolvable dilemma in distributed computing and established trust among the participants and transact without any third-party institutions. The traditional centralized financial system is inefficient, costly, and a target for crimes and abuses as all transactions are conducted via the third-party institution. In contrary, the blockchain-based financial system is more efficient, safer and incurs a lower cost as distributed participants can transact without any centralized institutions. This is the ground to dub blockchain as 'the technology to change the world.'

2.2 Security and Transparency of Blockchain-based IoT

A modern society is progressing to a 'transparent society' from a 'trust society' with IT technologies developing at a rapid rate. While the trust society operates transactions based on trust and security which has accumulated over the years, the transparent society adopts a transaction method where it analyzes the integrity data and calculates the objective trustworthiness.

One example of a transparent society is 'digital

forensics.' When there is a crime breakout these days, it is often reported that the criminal's digital devices were seized to analyze data and acquired evidence to arrest him or her. The technology used in this case is the digital forensic. Digital forensic is a scientific investigation technique to find criminal clues and evidence by collecting and analyzing the data in PCs, smartphones, tablets, and black boxes.

Today, various industries such as general enterprises, accounting services, legal services, medical services, financial services, insurance services, the transportation industry, software industries, and content industries use this technique. The digital forensic technique is especially used to verify fact relationships or solve legal disputes.

The problem for digital forensics to operate properly in the IoT era is that obstacles should be resolved. Firstly, the scope of digital forensics has become too wide and the level of difficulties are heightened at the same time. Now wearable devices that internalized digital functionalities in watches, glasses, accessories, and clothes measure and save various body states like heartbeats, body temperature, blood pressure, and sleeping pattern. Moreover, electronic home appliances such as TVs, speakers, air conditioners, refrigerators, vacuum cleaners, and door locks collect, process, and analyze log information and leave it. Ironically, there is too much information to consider.

A bigger problem is the integrity of data. As the amount of data increases, the probability of data being exposed to counterfeiting or falsifying grows even higher. Digital forensics assumes 'integrity,' which indicates that digital evidence data are untampered. Therefore, inefficient tasks using expensive devices should be conducted to test data integrity. Under such a situation, the target of digital forensic is complicated and the scope widened with increasing cost and decreasing efficiency [19].

Digital forensics especially becomes nullified with intelligent anti-digital forensic technique [20]. Hackers know different ways to completely delete the access records or make it impossible to recover memory or physically destroy hardware devices. There are cheap tools and ways to open records for general users.

Then what will happen if the blockchain technology is applied to IoT? Scientists expect that when the intelligent IoT incorporated with blockchain technology, i.e., chain of things, is realized, people will be free of false information [21].

Chain of Things is a technology to strengthen the transparency of data by binding things under a blockchain and it has two advantages.

The first advantage is that it guarantees the 'integrity of data.' Whenever a block is accumulated, more trust is formed in each transaction. Once generated, the block is impossible to modify as it is retroactive. The transaction participants can choose, trust, and transact upon one of the distributed common ledgers which are saved, instead of tracking the ledgers that are saved separately. Therefore, the transparency derived from the unique integrity of data in block chains allows freedom to get more information, freedom from false information and more effectiveness.

Another advantage is that security increases tremendously. The data recorded in blockchains are shared with all devices and users who participated in the network. Therefore, to falsify data, more than 50% of all users should be hacked at the same time. This requires enormous effort and cost, and it is not feasible at the current technological growth state. Additionally, as data are distributed and saved within the whole network, even when some problems arise in part of the network, the whole system is secured.

The battle of 'hacking and security' is similar to the battle of 'a spear and a shield,' so it is difficult to arrive at a conclusion. In this world, 'a spear that can pierce any shield' or 'a shield that can combat any spear' never exists. Likewise, 'a hacking that can attack any system' or 'a security system that will block any attack' does not exist.

As offensive weapons and defensive technologies increase with the growth of cutting-edge technology

and continued wars, hacking and security technologies are developing even more due to cyberwars. In the midst of this, a blockchain is expected to be “a shield that can block all types of attacks”. However, like existing security technologies, a blockchain is close to perfection, but it is not perfect. Although there are weaknesses in blockchain technologies, there are more drawbacks found in the application software to apply blockchains and in the interfaces of blockchain users.

Despite this, blockchain has a high probability of becoming the ‘second Internet technology’ to be applied in all industries. Then, blockchain security is directly related to social security, life, and property. What we need to do is to complement blockchain security so that it is close to perfection and improve its weaknesses. Additionally, using blockchain technology, we must establish a system to validate information quickly and efficiently, and evaluate and verify the reliability of data.

The current blockchain is evaluated as a high-quality security technology with integrity, availability, and confidentiality.

First, ‘integrity’ is proved when falsifying of data can be efficiently detected in a network environment that cannot be trusted. Moreover, as important data are equally distributed and managed in all nodes participating in the blockchain network, the service does not come to a stop in case of DDoS attacks. In other words, the ‘availability’ of technology is high. In addition to this, as it adopts the hash-based proof-of-work and public key cryptography method, which have long been proven in the computer science field, security is superior in terms of ‘confidentiality.’

This type of evaluation is a result of the comparative analysis of the centralized system. This is not an absolute evaluation. At the end, ‘blockchains also do not guarantee the perfect security.’ However, it is evident that blockchain technology is a developed technology that can tackle the dilemma that is not solved by existing techniques.

3. Technological Limitations and Solutions of Blockchain-based IoT and Solutions

3.1 Scalability of the Blockchain-based IoT

It is of interest whether the blockchain technology can properly be integrated into networks of super speed and hyper-connectivity, as communication networks, which form the foundation for the fourth industrial revolution are developing at lightning speed. Although blockchains are called ‘the second Internet’ and praised for its innovativeness, unless inherent limitations such as scalability and speed are solved, they will end up being like one of the previous techniques, which could not overcome obstacles.

The basic moral of blockchains is that ‘all participants in the network record and manage transactions, and prevent falsification or counterfeit information without any third-party management’ i.e., it is a method where all nodes in the network save the whole transaction record and verify them. All nodes have the blockchain distributed ledgers connected with hashes and the distributed nodes test the data falsification. Based on this, integrity and security were increased significantly.

As a side effect to this, it results in binding the whole network′s processing capacity as a singular node’s processing capacity. When the number of users and blocks increase the speed abruptly goes down. For example, as the users of ‘Cryptokitties,’ a cat collecting game using the Ethereum blockchain increased to 200,000, the whole Ethereum network got slower and the transaction costs increased [22].

Moreover, bitcoins have a limited amount of transaction records in one block as the size of a block is bound to 1 MB. The transaction processing speed is also 7 pieces per second. When compared to credit cards that process tens of thousands of transactions per second, bitcoins are far below the standard. It is difficult to expand block sizes as well. When the size of a block grows larger, the computer performance should be enhanced to calculate the hash values. High

performing computing power and increased records of blockchains lead to more costs, i.e., it seems to be a white elephant in financial transactions where scalability and speed are all that matter.

In industries, the second layer protocol method using sharding and off-chains are considered as a solution to speed up the rate of blockchains [23]. In the computer science field, it is already a valid technology being used and adopted actively.

The second layer sharding is a method of dividing transaction records, allocating the distributed node groups and processing them in parallel [24]. It is a sort of role allocation model. By dividing nodes into groups and verifying them, this method can achieve speed and effectiveness at the same time. Telegram Open Network (TON), the third generation blockchain developed by Telegram is known to apply the dynamic sharding method. It is a method that automatically splits or binds the node groups to process transactions based on the number of network transactions.

On the other hand, off-chain is a layering protocol model that processes transaction records outside the chains and only records final transactions in the blockchains [23]. The principle 'global agreement is slow, but local agreement is fast' is applied. As the transaction records are processed outside the blockchains and only the results are recorded, when transactions occur frequently, the records can take place offline, outside of blockchains and when the transaction is finished, the records will be on chain. With the two-layering structure, the scalability is increased.

For Internet of Things applications, IOTA is proposed as a next generation distributed ledger[25]. IOTA can achieve high transaction throughput using parallelized validation of transactions. However, the hash function of IOTA was vulnerable to a well-known technique for breaking hash function called differential cryptanalysis, which generate practical collisions.

Blockchain is indeed an innovative technology. However, the system is not completely done with verification. Moreover, the perceived blockchain service by users is enabled through the software. There is no perfect software in the human world. Repeated efforts to investigate and fix bugs and weaknesses should be taken.

Regarding this issue, centralized methods solve the problem by updating the central server. In contrast, as blockchains are structured in a distributed manner, it is not easy to patch everyone in the network. Therefore, developing protocols to quickly and effectively patch (upgrade) in the distributed networks is crucial.

3.2 Security of the Blockchain-based IoT

For a perfect defense, research on offensive tactics mandatory. Likewise, the hacking skill is developing at a rapid speed. As hacking got more intelligent and serious, economic losses and damages have grown even larger. Counterfeiting and falsifying the data of governments, enterprises, and individuals lead to confusion in countries and societies. The scope of side effects completely goes beyond the cyber world and reflects in reality [26].

The security in the fourth industrial revolution is not sufficient just because integrity, availability, and confidentiality are outstanding. Trustworthiness that goes beyond security is crucial. If products and services are to be recognized for their trustworthiness, the security elements should be in place already from the planning and designing processes. With that information assurance, a managerial and technological system to verify security can be integrated into products and services. Additionally, during the process of designing products, the establishment of a system that developers, reviewers, and users can all measure security and trust is feasible by information assurances in all stages of service points.

Recently, as a new automatic hacking tool to generate new malicious codes spread out, anyone could easily use it. Additionally, life expectancy of malicious codes got shorter and the attack periods grew shorter. Instances of malicious codes taking advantage of the

weaknesses in the web, networks, systems, and applications which we use in our everyday lives have also considerably increased.

Hackers also adopted machine learning and artificial intelligence technologies. After automatically analyzing the detection patterns of security systems, they proceeded with evasion attacks. It is a method to first test whether their attacks are blocked using the commercial security system and then to attack again. Hacking has always evolved with the approach to take on the weaknesses of systems and networks and spread throughout the network in an instant. They have grown its destructive power by integrating different attacks to speed up processes.

Therefore, the technology of a shield that combats against the spear should be changed. To protect the blockchain-based products and services, adopting intelligent security technologies is mandatory. The technologies should be embedded into the system and network technologies. Advanced persistent threat (APT) attack became the cause of major security accidents recently. It starts the weak points of a target after a prolonged and detailed analysis. Hence, it is not easy to defend. As existing security solutions detect hacking behaviors and defend them based on the signatures and thresholds, the solutions will be impotent under continuous attacks for a long period of time.

Adopting AI is also urgent in security. When AIs learn data and gain expertise-level insights, we can reduce managerial costs and prevent security accidents from breaking out due to the mistakes of managers. It is also feasible to distribute strategies and action plans to each node and update security policy automatically by analyzing correlations of risk information in the distributed networks and detecting attacks. Based on all strategies and systems, one can be more responsive in coping with attacks in prevention, detection, response, and prediction stages.

As stated earlier, the security weaknesses in blockchains can be found in the blockchain technology itself, blockchain user interface, and application software to apply blockchains.

As the network size grows larger and distribution increases, a blockchain will be safer. Although it is technologically challenging to hack 51% of the blockchain networking nodes, it is not impossible. The hacking skills targeting inherent weaknesses of a system and using malicious codes that spread quickly through the network threaten the blockchain technology. To cope with blockchain hacking, after analyzing the correlation relationships of threat information collected from the distributed networks, automated process of distributing coping strategies to each distributed node and updating security policies should be carried forward.

Secret keys can be also leaked or lost in the user interface. As one would use the public key cryptography method, the person cannot claim ownership of the content once he gets the secret key stolen by a third entity or it is lost. To protect the blockchain user interface and cope with secret keys getting stolen or being lost, secret keys should be secured in a hardware wallet and multi-signature applications where a multiple number of participants should sign at the same time to approve transactions are mandatory.

Additionally, as blockchains are developed in an open-source format and operate in a distributed network method, a quick security patch and verification are difficult. When weaknesses are revealed, they could bring about serious damages. Therefore, when programming blockchain applications, one should do secure coding implementing the standard library functions and follow the verification process, establishing an automatic security program patch environment that assures integrity.

Large scale hacking accidents continue to break out in well-known national and global crypto-currency exchange markets. Although blockchain is acknowledged for its security based on cryptology distributed ledger technology, security accidents still

occur in the exchange markets.

Last February, the asset size of national crypto-currency exchange amounted to 17 trillion Korean won; however, level of security was found to be absurdly inferior. The exchange itself counteracts the 'decentralized' concept of blockchain philosophy and works as a centralized institution. When important data are concentrated in a database, said database becomes a target for hacking. As a system become increasingly complicated, more weaknesses are found.

Therefore, the crypto-currency exchanges should take initiatives to stop these vicious cycles. To achieve this, an exchange should proactively adopt security systems such as DDoS defense, firewalls, and attack prevention systems in addition to endpoint security solutions like network separation, encryption, and access control systems.

4. Conclusion

Owing to data transparency provided by chain of things in blockchain-based IoT, will privacy be invaded? Some people claim that invasion of privacy will take place more frequently as transparency will lead to easier controls and regulations, thereby resulting in more privacy invasions [27]. However, that is not the case. Rather a non-transparent structure has a higher probability of privacy invasion. In case of digital forensics, previously, it was difficult to investigate which data were true and important as evidence out of non-transparent data. Therefore, complete enumeration had to be conducted and in the case of IoT devices. All related devices had to be examined. In contrast, in the case of blockchains, as complete trust relationships exist between blocks, and they adopt an organized time series structure, an investigation in a part of the block in one device is sufficient. Moreover, by using various de-identification technologies, privacy will also become increasingly stronger after complementing the integrity and security of data.

Humanity has been developing technologies such that common value can be added to the public. Blockchain-based technologies will bring about greater freedom of information, freedom from false information. As further work, a blockchain platform for IoTs which provides scalability and security will be implemented according to this research results, and compared with conventional blockchain platforms.

REFERENCES

[1] Y. Yuan & F. Y. Wang. (2016). Towards blockchain-based intelligent transportation systems. *In Intelligent Transportation Systems (ITSC), 2016 IEEE19th International Conference on,* 2663-2668.

[2] J. Sun, J. Yan & K. Z. Zhang. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation, 2(1)*, 26.

[3] A. Dorri, S. S. Kangere, R. Jurdak & P. Gauravarm. (2017). Blockchain for IoT security and Privacy: The case study of a smart home. *In Pervasive Computing and Communications Workshop, 2017 IEEE International Conference on,* 618-623.

[4] S. Lee & D. Lee. (2016). Actual Cases for Smart Fusion Industry based on Internet of Things. *Journal of the Korea Convergence Society, 7(2),* 1-6.

[5] P. Treleaven, R. G. Brown & D. Yang. (2017). Blockchain Technology in Finance. *Computer, 50(9),* 14-17.

[6] H. Mun. (2018). Biometric information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology, 8(3),* 85-90.

[7] K. M. Khan, J. Arshad & M. M. Khan. (2018). Secure Digital Voting System Based on Blockchain Technology. *International Journal of Electronic Government Research (IJEGR), 14(1),* 53-62.

[8] H. M. Kim & M. Laskowski. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, *Finance and Management, 25(1),* 18-27.

[9] K. Fan, S. Wang, Y. Ren, H. Li & Y. Yang. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems, 42(8),* 136.

[10] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia & G. Dong. (2018). GridMonitoring: Secured

Sovereign Blockchain Based Monitoring on Smart Grid. *IEEE Access, 6,* 9917-9925.

[11] Symantec internet security threat report. Technical report, Symantec Corporation. url: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf (last access: 2018.06.30.)

[12] N. Kshetri. (2017). Can Blockchain Strengthen the Internet of Things?. *IT Professional, 19(4),* 68-72.

[13] S. Hong & S. Park. (2017). The Research on Blockchain-based Secure IoT Authentication. *Journal of the Korea Convergence Society, 8(11),* 57-62.

[14] T. B. Lee & M. Fischetti. (2001). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor,* DIANE Publishing Company.

[15] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, url: http://www.bitcoin.org (last access: 2018.06.30.)

[16] M. Castro & B. Liskov. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transaction on Computer Systems (TOCS), 20(4),* 398-461.

[17] A. Back. (2002). Hashcash - a denial of service counter-measure. url: http://hashcash.org/papers/hashcash.pdf (last access: 2018.06.30.).

[18] S. Underwood. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59(11),* 15-17.

[19] X. Feng & Y. Zhao. (2017). Digital forensics challenges to big data in the cloud. *2017 IEEE International Conference on Internet of Things,* 858-862.

[20] M. Wundram, F. C. Freiling & C. Moch. (2013). Anti-forensics: the next step in digital forensics tool testing. *2013 Seventh IEEE International Conference on IT Security Incident Management and IT Forensics (IMF),* 83-97.

[21] D. Miller. (2018). Blockchain and the Internet of Things in the Industrial Sector. *IT Professional, 20(3),* 15-18.

[22] BBC News, url: https://www.bbc.com/news/technology-42237162 (last access: 2018.06.30.).

[23] W. Li, A. Sforzin, S. Fedorov & G. O. Karame. (2017). Towards scalable and private industrial blockchains. *In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts,* 9-14.

[24] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert & P. Saxena. (2016). A secure sharding protocol for open blockchains. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* 17-30.

[25] M. Divya & N. B. Biradar. (2018). IOTA-Next Generation Block chain. *International Journal of Engineering And Computer Science, 7(4),* 23823-23826.

[26] S. Shin, G. Chae & T. Lee. (2015). An Investigation Study to Reduce Security Threat in the Internet of Things Environment, *Journal of Convergence for Information Technology, 5(4),* 31-36.

[27] G. Zyskind & O. Nathan. (2015). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE security and Privacy Workshop (SPW),* 180-184.

이 일 구(Lee, Il Gu) [정회원]

- 2003년 2월 : 서강대학교 전자공학과 (공학사)
- 2005년 2월 : 한국과학기술원 정보통신대학원 (공학석사)
- 2012년 2월 : 한국과학기술원 지식재산대학원 (경영학석사)
- 2016년 2월 : 한국과학기술원 정보보호대학원 (공학박사)
- 2017년 2월 ~ 현재 : 성신여자대학교 융합보안공학과 조교수
- 관심분야 : 정보통신, 정보보호, 지식재산
- E-Mail : iglee@sungshin.ac.kr