

New Function and Configuration of Future Network for Blockchain Platform Operation

Suyeon KIM*, Chang Su LEE**, Hyun K. KAHNG**

* Department of Industry Cooperation, Keimyung University, Korea

** Department of Electronics & Information Engineering, Korea University, Korea
sykim388@gmail.com, lcs3708@korea.ac.kr, kahng@korea.ac.kr

Abstract— In this paper, we discuss the subnetwork structure of the Blockchain system, which is expected to develop various application platforms in the future. Blockchain is an innovative trading system, and many studies have been conducted recently. It is expected to be used in various fields with stable security function of each node taking part in the system without central server control. However, due to its three functional limitations (excessive traffic generation, lack of distributed control, and unfairness of network resources) presented in this paper, it is difficult to provide complete service in the present network. In order to minimize such problems, a subnetwork structure providing a Blockchain service should provide an appropriate network configuration according to a Blockchain application or service type. In addition, based on the number of the node participated in Blockchain and the amount of data transmitted, it is necessary to provide appropriate QoS and the subnetwork should provide stable protocol function and efficient traffic operation. This subnetwork structure is proposed as a service function of the future network structure of ISO / IEC JTC1 SC6 which is being standardized.

Keywords— Future Network, Blockchain, Blockchain Subnetwork, P2P Networks, ISO/IEC JTC1 SC6

I. INTRODUCTION

Blockchain first proposed to implement electronic cryptography called Bitcoin is a system that can be traded without the control of a reliable central server in a P2P based network and is drawing attention as a core technology of the fourth industrial revolution. Recently, with the increase of O2O (Online to Offline) transactions using PC and smart phone, new business models applying Blockchain technology are increasing to overall industry area. Especially Blockchain Technology which cannot be hacked, tampered and counterfeited have been increasing in the Fintech industry. In addition, global financial institutions are pursuing Blockchain system development and standards development through partnership, and Blockchain Platforms are expected to be activated around the world.

However, since the first proposed Blockchain technique was developed as the implementation technique of cryptography like Bitcoin, the data structure or protocol method is not universal and is still evolving for deploy. Recently, various kinds of Blockchain platforms have been

made to be applicable to other fields. The Blockchain system is expanding into a variety of e-commerce companies including securities companies, banks, trading solution companies, and O2O. It is expected that start-up, virtual money developers, Fintech companies, information protection companies, copyrights, ownership and registration agencies will actively participate in the development and build an ecosystem of Blockchain.

Until now, Blockchain system is operated using an existing network like internet, however it is expected that various Blockchain platforms and application programs different from existing transaction methods will appear in a short period of time. The need for a subnetwork that fits to Blockchain platform and runs it smoothly is expected as shown in Figure 1. As shown in Figure. 1, the upper layer consists of various types of Blockchain platforms, and each node that operates the Blockchain platform will be connected by the infrastructure of the future network.

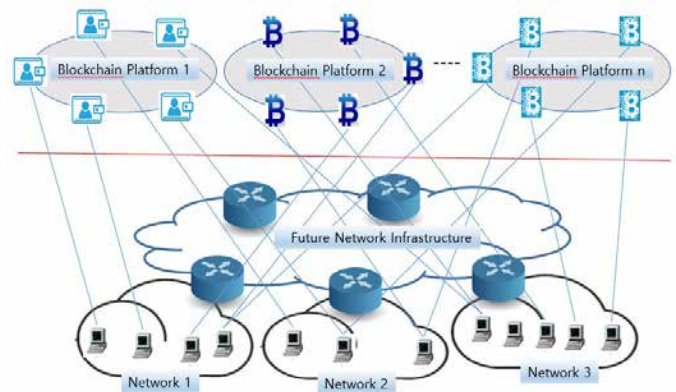


Figure 1. Subnetwork structure of Blockchain network

In this paper, we analysed the problems that can be caused by various Blockchain applications in the current network system. And if we apply these problems and solutions to future network requirements that are being standardized in ISO / IEC JTC1 SC6, the optimal future network running Blockchain will be constructed as a new platform. We think that such a future network will provide users with optimal trading system.

For this purpose, Section 2 of this paper briefly introduces the Blockchain system and introduces the problems that can occur in the current network environment. Section 3 presents

the requirements of the future network to solve these problems and suggests to apply these requirements to future network standardization in progress. Finally, Section 4 presents conclusions on the requirements for future networks and presents future research plans.

II. INTRODUCTION TO BLOCKCHAIN SYSTEM AND PROBLEM ANALYSIS FOR ITS SUBNETWORK^{[1][2][3]}

Unlike the conventional method of handling transactions by a centralized server, Blockchain system, core technology of Bitcoin, uses resources (processing power, disk capacity, network bandwidth, etc.) held by participants on a P2P network to which general nodes are connected. This Blockchain technology has emerged as an innovative technology. Bitcoin client based on Blockchain technology is possible for anyone to download the program and to remit or mine Bitcoin and to use it in certain places. Bitcoin system has the same flow chart as shown in Figure 2.

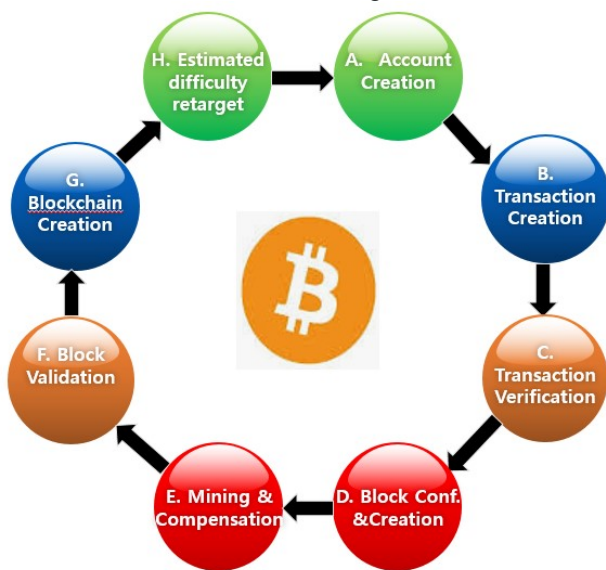


Figure 2. Overall flowchart of Bitcoin Transaction

In [Figure 2], the creation of an account in step A is action for creating an individual account in the same way as a bank account. At this time, a private key and a public key are generated. Transactions in step B can be transmitted or received in Bitcoin data using the public key as the receiving address (or account number). The data could represent money, contract, deeds, medical record, customer details, or any other asset that can be described in digital form. The transaction verification of step C is performed by transmitting the transaction generated in step B to the neighbouring nodes. If the transaction is judged to be appropriate through this verification process, it is propagated again, and if it is judged that the transaction is not appropriate, the transaction is deleted. The transaction is either verified instantly or transcribed into a secured record and placed in a queue of pending transactions.

The block configuration and creation of step D stores the transaction judged appropriate by each node in the memory

pool for block production. Each block is identified by a hash, a 256-bit number, created using an algorithm agreed upon by the network. The mining and compensation of step E is the process of solving the block by making incremental changes to one variable until the solution satisfies network-wide target. Block validation of step F confirms the appropriateness of the block from the neighboring node by transferring the generated block to the neighboring node. If more than half of all nodes agree with the appropriateness of the generated block, it is approved as a new block.

In the Blockchain generation of step G, the node that received the block generated in step F completes the verification of the convex and connects to the existing block chain. Because of the distributed data structure, the mined blocks can be created at the same time from other nodes, which can result in Blockchain branching (Forking) due to network delay. In fact, in the Bitcoin, only the longest block chain survives and the remaining chains disappear into short orphan blocks. The degree of difficulty of step H adjusts the probability of self-occurrence that difficulty in mining so that the block generation cycle can be adjusted every 10 minutes.

Since the block chain is a distributed data structure as shown in the previous block chain generation flow, the mined blocks can be simultaneously generated at different nodes at the same time. Such blocks may be transmitted to the nodes participating in the platform at the same time, resulting in a large number of branching phenomena. An example of an agreement algorithm for solving the branch phenomenon is 'The Byzantine Generals Problem'. BGP solution is to remove these orphaned blocks if less than one-third of the nodes present an orphan block.^[4]

As the branching phenomenon occurs more frequently, the number of orphan blocks not connected to the chain is increased, resulting in network congestion and a waste of bandwidth. In Blockchain system, since only the longest block chain survives, the slower the network processing speed, the more often the orphan block is generated.

How much blocks to process per second is very important for Blockchain performance. However, the Blockchain performance such as the finality of each transaction, the cycle in which blocks are generated, the amount of processing variation depending on the block size, the number of nodes showing decentralization, the efficiency of the algorithm, and parallel scalability, should be considered together.^[5]

As considering the fast processing speed that will be the basis of the 5G network or the future network, the generation of orphan blocks may be minimized according to the network configuration method. And if you have to charge a fee based on network usage, you can simplify the algorithm of the Blockchain or you can save the network usage fee and computing power by managing the network bandwidth.

In this way, it is expected that the Blockchain will be used in various fields by the stable security function of each node

without central server control. However the problems that may occur in the subnetwork due to the introduction of the Blockchain system cannot be overlooked. In this paper, we present the following three problems.

- 1) Possibility of excessive traffic on the subnetwork side: Mass traffic generated in the process of transmission and appropriateness checking of transactions caused by various Blockchain applications, and large amounts of traffic due to frequent data exchange for block validation process through block transmission and consensus process to all participants in the network.
- 2) Absence of decentralized control: Subscription and transaction of Blockchain can be done by anyone, and some nodes can generate large amount of data locally. Because of this problem, it is impossible to control the traffic of the Blockchain system considering the load of the network.
- 3) Fairness of network resources: In Blockchain system, a node with a lot of computing resources monopolizes block generation, resulting in unfairness in network bandwidth usage due to unbalanced computing resources.

III. NEW FUNCTIONS OF FUTURE NETWORK TO SUPPORT BLOCKCHAIN SYSTEM

In addition to the problems that the Blockchain system mentioned in Chapter 2 may cause in the subnetwork, there may be more problems. However, in this paper, we consider the requirements of the future network focusing on the above three problems.

In ISO / IEC JTC1 SC6, we are already studying the subnetwork structure to support various high level application programs including Blockchain, and its standardization is in progress taking into account the expected requirements. The details of the future network requirement are defined in the document TR 29181. Based on this document, standardization of ISO/IEC 21558: future network structure and ISO/IEC 21559: future network protocol and mechanism is currently underway. [7][8]

ISO / IEC 21558 Future network structure documents are subdivided into areas as shown in [Table 1].

TABLE 1. FUTURE NETWORK STANDARDIZATION AREA

Document Number	Topic
ISO/IEC 21558-1	Part 1: Overview and high level architecture
ISO/IEC 21558-2	Part 2: Naming and Addressing
ISO/IEC 21558-3	Part 3: Switching and Routing
ISO/IEC 21558-4	Part 4: Mobility
ISO/IEC 21558-5	Part 5: Security
ISO/IEC 21558-6	Part 6: Media Transport
ISO/IEC 21558-7	Part 7: Service Composition
ISO/IEC 21558-8	Part 8: Quality of Service
ISO/IEC 21558-9	Part 9: Networking of Everything

For smooth operation of the Blockchain system, the requirements of the future network belonging to the lower layer are analysed as follows.

- 1) Necessity of Traffic Control: It is necessary to control traffic by measuring the number of the blocks occurring in each node and to adjust it so that excessive traffic does not occur in the network. In order to adjust the traffic, we need to study and enhance the routing protocol of the future network considering the tree configuration for verifying the chain validity of the Blockchain. This work is related to the routing configuration of Document Part 3.
- 2) To construct an effective Blockchain system, various subnetwork configurations need to be constructed for each Blockchain platform, and subnetwork should support these diverse configurations. For this purpose, the network is configured to minimize the generation of orphaned blocks and the network can be reconfigured if a large number of orphaned blocks are created.
- 3) The subnetwork should grasp the usage of computing power and network resources in a legitimate way, controls nodes that use many resources, and equally distribute resources to maintain fairness of network traffic. If the particular node uses excessive traffic on the specific platform, the subnetwork has to adjust the value of QoS in Document Part 8 to control the traffic usage to be in proportion to the cost.
- 4) For the smooth operation of the Blockchain system, the subnetwork needs to provide stability and robustness. As the applications of the Blockchain become more diverse, the number of transactions occurring at the same time is expected to increase exponentially. Therefore, the subnetwork must be stable according to the amount of traffic changing in the Blockchain. A number of nodes participate in the Naming scheme of Part 2 and a lower network layer should be configured to facilitate traffic management by the switching scheme of Part 3.

Based on these requirements, the ISO / IEC 21558-9 document described to allow nodes belonging to the same social platform to form a thing-user social group through appropriate validation procedures. Each thing-user social group will provide security and intellectual capabilities through AI mechanisms and semantic inferences. In addition, the nodes of the thing-user social group will be able to infer new knowledge by exchanging information with each other. Unfortunately, the specific protocol for the thing-user social group is not yet standardized, so the specific algorithm is not yet available. [9]

IV. CONCLUSION

In the future, the Blockchain technology will be made in various Blockchain platforms to be applied in many areas. These Blockchain platforms are expanding into securities companies, banks, trading solution companies, and e-commerce companies including O2O. It is expected that various development agencies will participate in building a new ecosystem for Blockchain. In this paper, we study on the necessary functions and services of the future network as a

subnetwork structure to provide stable protocol function and efficient traffic operation of the Blockchain system that various platforms are expected to be developed.

And we analysed the problems that may arise from various Blockchain applications in the current network system, and introduced the requirements to solve these problems in the Future Network standardized by ISO / IEC JTC1 SC6. Based on the four requirements presented in this paper, we will define the services to be provided for the Blockchain platform on the Future Network. ^[10] I believe that standardizing the protocol mechanisms needed to provide such services is now a matter of preparation. If a suitable Future subnetwork is standardized, the Blockchain and the optimal Future subnetwork will be able to provide the optimal trading system to the users as a new Blockchain infra-structure.

ACKNOWLEDGMENT

This paper was prepared by the support of the 'National Standard Technology Improvement Project' of the Ministry of Commerce, Industry and Energy. (Project Number: 20002532)

REFERENCES

- [1] Kim Won, "Bitcoin Blockchain Operation Principle and Evolution", Weekly ICT Trends, Vol 1851, 2018. 6. 20, pp. 2-15.
- [2] Lim Myunghwan, "Analysis of Utilization Trend of Blockchain Technology", Weekly ICT Trends, Vol 1772, 2016. 11. 15, pp. 2-14.
- [3] Satoshi Nakamoto, "Bitcoin: A Peer-to Peer Electric Cash System", www.bitcoin.org, 2008. 10. 31.
- [4] Nagato Kasaki, Wataru Shinohara, "Blockchain application kaihatsu no kyokasho", ISBN 979-11-6224-083-0
- [5] <https://bitcoin.org/en/developer-reference#block-chain>
- [6] Shin-Gak Kang, Wook Hyun, Changkyu Lee, "Proposed updates to Study Rport of PWI-P2P, "Functional Architecture and Protocols for Managed P2P communications", ISO/IEC JTC1/SC6/WG7 N154.
- [7] ISO/IEC 21558 – Information Technology – Telecommunications and information exchange between systems – Future Network – Architecture
- [8] ISO/IEC 21559 – Information Technology – Telecommunications and information exchange between systems – Future Network – Protocols and mechanisms
- [9] ISO/IEC JTC1/SC6/WG7 N164, "Updated WD text of ISO/IEC 21558-9, Future Network Architecture – Part 9: Networking of Everything", which is produced SC6/WG7 Tokyo meeting, held in August 2018.
- [10] ISO/IEC JTC1/SC6 N16860, "Summary of voting on the establishment of a Ad-hoc Group on Networking for Blockchain and its ToR on 6N16841"
- [11] Suyeon Kim, Chang Su Lee, Hyun K. Kahng, "The Requirement Analysis for Future Network suitable for various Blockchain Platforms", KIPS_C2018B0039, 2018.11.3



Suyeon Kim is an Associate Professor of Industry-Academic Cooperation Group at Keimyung University, Taegu, Korea. He received Master degree in Computer Engineering from the Kyungpook National University, Korea, in 1991 and Ph.D. degree in Electronics and Information Engineering at Korea University. From 1991 to 1998, he was a Senior Research staff at ETRI, Korea. His research interests include Future Network, IoT, Telecommunication standardization, and Blockchain.



Chang-Su Lee is a Ph. D graduate student in Department of Electronics and Information Engineering Korea University. His major is ICT Convergence Technology. In 1999, He received a Master's degree in Information & Engineering Korea University. From 1995 to 1997, he worked for LG Information & Communications and from 1999 to 2002, he worked at POSDATA.



Dr. Hyun-Kook Kahng is a Professor of Department of Electronics and Information Engineering at Korea University Sejong campus, Sejong city, Korea. He received master's degree in Computer Engineering from University of Michigan, Ann Arbor in 1984, and Ph.D. in Computer Networking from Georgia Institute of Technology in 1990. From 1991 to 1994, he was a Senior Research Engineer at ETRI, Korea. Since 1994, he has been a professor in Korea University. He has been standardizing, as a Korean delegate, in various SDO's such as ITU-T, ISO/IEC JTC1 SC6 and IETF in the field of computer networking. His current research interest includes, future networking technologies, especially for IoT, Blockchain, wearable devices, and autonomous cooperative system.