International Journal of
Emerging Multidisciplinary Research

ISSN : 2546-1583
Volume 1, Number 2, December 2017
https:// doi.org./10.22662/IJEMR.2017.1.2.009

Development of a Secure and Intelligent IoT System based on a Consortium Blockchain

Sunghyuck Hong[1]
[1]Div. of Information Communication, Baekseok University, KOREA

Abstract

Background/Objectives: Blockchain technology is a decentralized digital book that discloses transactions to all trading participants, unlike traditional methods of keeping records on a centralized server when trading data, it is a security technology that is virtually impossible to hack because it must forge a block chain at the same time. However, the current block chain technology is a public block chain. Anyone can join a block-chain network, view all the details, and anyone can verify transaction history. On the other hand, a private block chain or a consensus block chain refers to a block chain in which a participant is restricted to participate in building an internal network with a restricted block chain or through a separate authentication method. **Methods/Statistical analysis:** In the case of the bit coin using the public block chain technique, the mining process is required in the network in order to prevent the Sybil attack (DDoS attack) which takes over the network by the number of nodes. If Blockchain is used in IoT environment, then IoT sensor node is adaptable for Blockchain because of decentralized network. **Findings:** There are many application areas. The disadvantage of mining a few network seizures while granting proof rights to the computing power, but not the number of nodes, is a catastrophic idea, but the cost of network maintenance is very high. However, if the only entity that proves the transaction is a bank, the Sybil attack itself is impossible and the network maintenance cost is zero. **Improvements/Applications:** Therefore, a consortium Blockchain can solve this public Blockchain, and it will be able to contribute the development of an intelligent IoT and FinTech system technology as well.

Index Terms

IoT, Blockchain, Distributed Computing, Consortium Blockchain

Corresponding author : Sunghyuck Hong
sunghyuck.hong@gmail.com

• Manuscript received November 13, 2017.
• Revised November 25, 2017 ; Accepted December 2, 2017.
• Date of publication December 31, 2017.

I. INTRODUCTION

A. Background of Blockchain

Blockchain technology is a decentralized digital book that discloses transactions to all trading participants, unlike traditional methods of keeping records on a centralized server when trading data, It is a security technology that is virtually impossible to hack because it must forge a block chain at the same time. In addition, since it operates in P2P mode, it is expected that financial companies can save $ 2 billion annually (about 23 trillion won) in the short term because they can make safe financial transactions at low cost without having a conventional central network [1-5]. It is expected that the service will save $ 15-20 billion annually by 2020. Already, many global financial companies are beginning to expand their research and investment in block-chain technology. Forty global financial companies, including Goldman Sachs, Barclays, JP Morgan Chase, Citigroup, and UBS, have formed a block chain consortium called R3 CEV to jointly develop and test block-chain standard platforms. The block stock chain is based on a monthly block chain, and the US Stock Exchange gives the Overstock company the authority to issue block stocks to the Internet. Against this backdrop, there is a growing need for Korea to actively respond to financial-related block chain technology. However, the current block chain technology is a public block chain. Anyone can join a block-chain network, view all the details, and anyone can verify transaction history. On the other hand, a private block chain or a consensus block chain refers to a block chain in which a participant is restricted to participate in building an internal network with a restricted block chain or through a separate authentication method. In the case of the bit coin using the public block chain technique, the mining process is required in the network in order to prevent the Sybil attack (DDoS attack) which takes over the network by the number of nodes. The disadvantage of mining a few network seizures while granting proof rights to the computing power, but it is not the number of nodes, it's catastrophic idea, but the cost of network maintenance ($ 1.5 million per day) is very high [6-9]. However, if the only entity that proves the transaction is a bank, the Sybil attack itself is impossible, and the network maintenance cost is zero. Of course, decentralization loses its crucial ideological value, but since the bank is not interested in decentralization, it is bound to want to implement a financial transaction system using consortium block chain technology.

II. RELATED RESEARCH

A. Public vs. Private

Public Blockchain is decentralized. However, nobody is responsible for specific transactions, and there is no withdrawn. However, a consortium Blockchain is type of in the middle of centralized and decentralized [10-11].

Table. 1. PUBLIC VS. CONSORTIUM BLOCKCHAIN

Public block chain	Consortium Blockchain
· Because the transaction proof is anonymous, it has strong legal elements. There is a risk of 51% attack or double spending · It is very difficult to change one rule at a time. · The cost of network mining is high. · Network expansion is difficult and transactions are slow.	· There is no problem like 51% attack or double spending because the transaction certificate is known. · It can change the law to suit the owner of the block chain. · It is very little network maintenance cost. · Network expansion is easy, and transaction speed is fast.

FinTech, which is the most recent issue among financial services, is operated based on cooperation and linkage between various companies such as IT companies, financial companies and PG companies. Therefore, it is possible that personal financial information that is concentrated in financial companies [12-15]. If there is a blurred area of responsibilities between companies or a different level of security management system due to the increase of the management target, a security system blind spot can occur. If a security incident occurs in one place, the risk of accident spread is also high. Also, before the release of security patches such as zero-day attacks, website hacking, etc., cyber attack threats exploiting security vulnerabilities inherent in SW are increasing steadily [16-17]. In particular, more than 75% of these cyber-attacks are exploiting vulnerabilities in applications. If you do not verify the validity of the data entered in the DB-related software, you can manipulate the SQL statement to access information that is not readable in the DB, or you can download key files in the server through directory path manipulation. In addition, smartphone-based FinTech service apps are exposed to vulnerabilities in mobile devices, operating systems, and platform technologies, as well as threats from traditional network and IT Web security domains. FinTech includes IoT sensor network if it is extendable in the future [18-20].

Table 2. FINTECH RELATED SECURITY INCIDENTS

Type	Descriptions
Crypto-currency abnormal withdrawal accident	· In 2004, SK Telecom released an electronic money box similar to the current simple settlement, but the service was suspended due to an unexpected financial loss of KRW 33 million. · At that time, SK Telecom and banks delayed their responsibilities to each other.
Bitcoin hacking	· 2014.2 Japan's Bitcoin Exchange Mountain Music hit $ 470 million worth of hacking. · 2015.1 Europe bit coin exchange bit stamped $ 5 million worth of hacked. · 2016.8 Hong Kong Bitcoin Exchange Beat Phinets Hacked $ 65 Million. · 2017.7 Korea's biggest bit coin transaction hacking account information, account information, transaction information, request OTP authentication number to individual customers.
Paypal payment accidents	· Approximately 10 million payments are made daily, and about 33,000 payment accidents are caused by account leakage. · Minimize victims' relief and damage to consumers through insurance, etc. (Compensation for all or more of the accident amount)

For convenience of users, there are many simple payment services, but there is not enough technology for security countermeasures. Therefore, if we apply the security-enhanced consortium block chain technology to various financial services including FINTECH, we expect to create safe and convenient financial environment [21-25].

III. PROPOSED CONSORTIUM BLOCKCHAIN

A. Development of Consortium blockchain system model

Consortium block chain technology is a semi-centralized block chain controlled by preselected nodes, in which n financial institutions operate one node and transactions are generated only when the agreement between the nodes of each institution occurs. Therefore, the right to access the records of a block chain can be granted to the public as a public block chain, but it can be provided only to participants (eg. financial institutions) or only to specific persons through the API. Figure 1 is a network diagram of the consortium block chain platform network. Each network consists of a node, a permissioning service, a network map service, and a notary service.

Table 3. CONFIGURATION OF CONSORTIUM NETWORK

Type	Descriptions
Node	· Transaction nodes are divided into transaction nodes (hereafter, "transaction nodes") to which transactions are exchanged and service nodes that provide permit services, network map services, and notarial services (theoretically, transaction nodes can also be provided) Identified through the specified unique ID .
Authorization Service	· TLS certificate issuance and management service, all nodes can communicate directly by using encrypted communication channel based on issued certificate
Notary services	· A service that verifies and confirms a transaction (hereinafter "agreement"). There is at least one notarial service in each network. Each notarial service is provided by a cluster consisting of a single node or multiple nodes ('notary').
Network Map Service	· Provide the information of the nodes necessary for transaction and communication between nodes, and the node newly participating in the network should first register their own information in this service

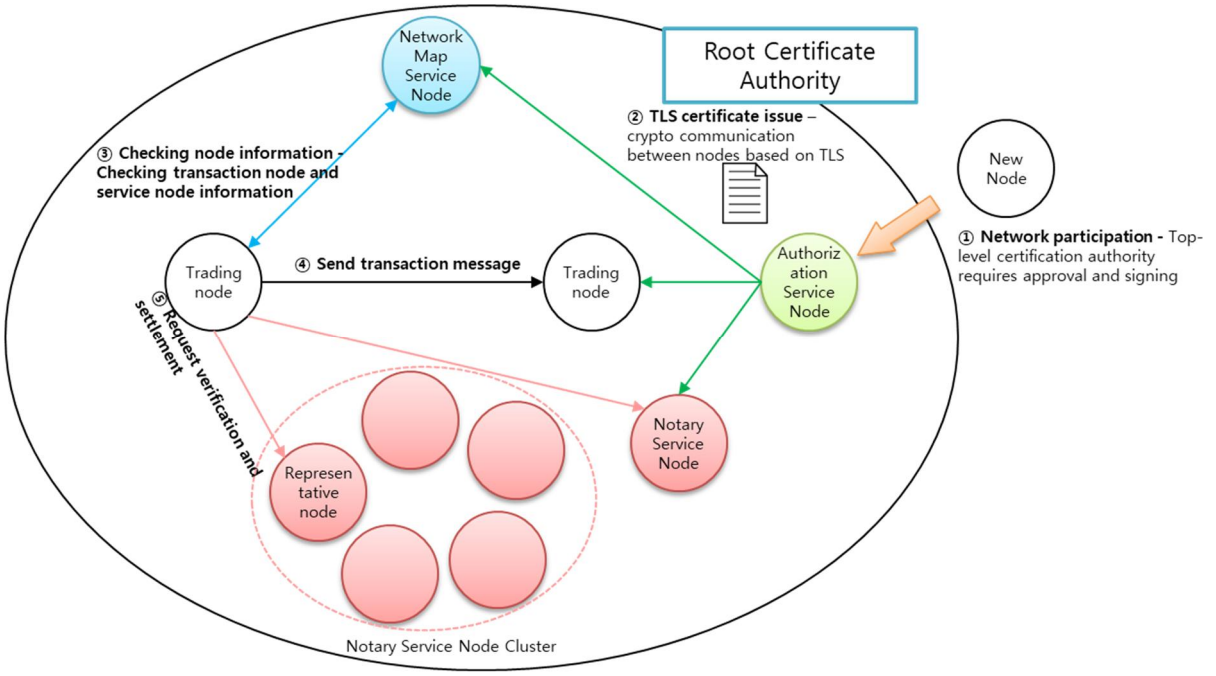

Figure 1. Consortium block chain platform network diagram

B. Development of PBTP (Practical Byzantine Fault Tolerance) based algorithm

The problem of the existing consensus algorithm is that a compensation system such as an internal virtual currency is required to operate a block chain to which an operation proof algorithm and a equity proof algorithm are applied. Therefore, the energy consuming method is important. Equity proof is also true, without internal money and compensation, there is no reason to create a block and the equity verification mechanism itself cannot be used. Therefore, in the case of a private block chain that performs many services other than virtual currency, it cannot use an agreement algorithm that requires such an internal currency. For example, if the A and B blocks are generated at almost the same time, then each node selects A and B blocks according to its own selection, . However, there is a problem that it is difficult to apply to a service that requires an immediate transaction confirmation due to the problem that the previous blocks are surely agreed upon [25].

C. The proposed PBTP (Practical Byzantine Fault Tolerance) based algorithm

PBFT is a consensus algorithm which is a functionally complemented algorithm that allows all nodes participating in a distributed system to successfully negotiate when a distributed system is an asynchronous system where a promiscuous node may not exist. PBFT will solve the problem that the existing BFT consensus algorithm can only be agreed upon in a synchronous network, so that it can be settled in an asynchronous network with a Byzantine node.

Figure 2 shows how PBFT algorithm works. In this conventional distributed algorithm, there exists a special node called Primary or Leader. This node arranges the order of the request of the client, writes the result of the request, and distributes it to other nodes. The detailed procedure is as follows.

- PBFT agreement algorithm execution procedure

· Leader collects and sorts clients' requests and propagates them to other nodes along with execution results
· The nodes that received the message of the leader propagate the message received from other nodes to the remaining nodes once again.
· All nodes propagate to the other nodes what the same message (quorum or more) they received the most from other nodes
· After all of the above steps have been completed, all nodes have the same data agreed upon by the quorum.

The PBFT will be developed using two broadcasts to ensure that all nodes in the network have the same message, even if the Byzantine leader or the Byzantine verification node sends a strange or arbitrary message for the network branch [25].

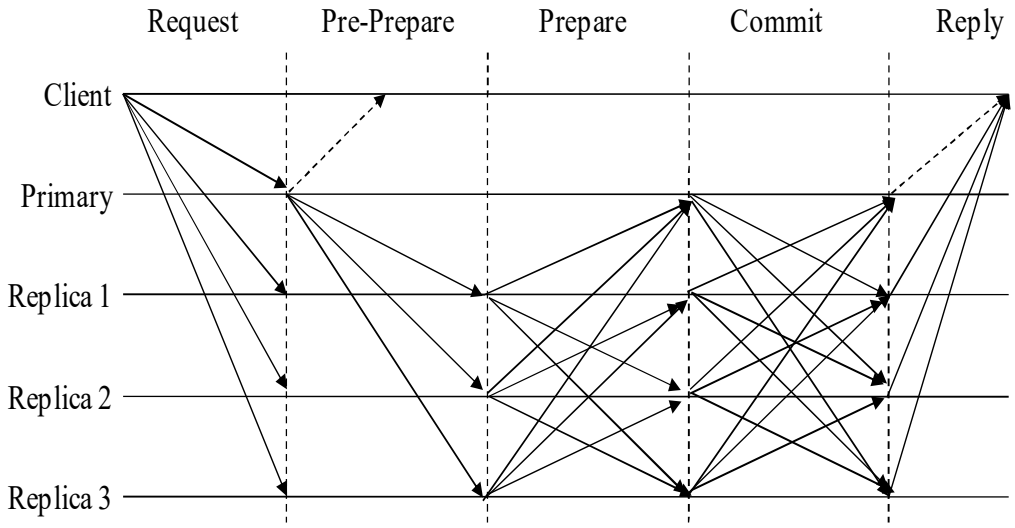

Figure 2. Overview of how the PBFT algorithm works

IV. CONCLUSION AND FUTURE WORK

This paper focuses on the common problem of public chain. In order to overcome the limitations of the characteristics of archives, secure and intelligent IoT environment is needed. Designing a block chain based data management system There is no guarantee that integrity of data cannot be changed, it provides availability through database sharing, sharing of authentication information confidentiality. In addition, it is evaluated by type according to evaluation criteria. In this paper, the essential elements of security, lowering the cost of construction, and there is a difference. The proposed design method is not only electronic form but also paper form.

It is also applicable to Apostille certificates. It can flexibly respond to privacy policy in all situations, and there are various electronic content sectors that require legal validation. It provides scalability that can be used. In the future, it will be possible to supplement the shortcomings of the consortium block chain. Further research on sharing policy and work is still undergoing. It is necessary to expand the transmission function of official documents.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (NRF-2017R1A2B1003394)

REFERENCES

[1] Morabito, V. (2017). Blockchain Value System. Business Innovation Through Blockchain, 21-39. doi:10.1007/978-3-319-48478-5_2

[2] Magyar, G. (2017). Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. 2017 IEEE 30th Neumann Colloquium (NC). doi:10.1109/nc.2017.8263269

[3] Kuzmin, A. (2017). Blockchain-based structures for a secure and operate IoT. 2017 Internet of Things Business Models, Users, and Networks. doi:10.1109/ctte.2017.8260937

[4] Backman, J., Yrjola, S., Valtanen, K., & Mammela, O. (2017). Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. 2017 Internet of Things Business Models, Users, and Networks. doi:10.1109/ctte.2017.8260929

[5] Umeh, J. (2016). Blockchain Double Bubble or Double Trouble? Itnow, 58(1), 58-61. doi:10.1093/itnow/bww026

[6] Baxendale, G. (2016). Can Blockchain Revolutionise EPRs? Itnow, 58(1), 38-39. doi:10.1093/itnow/bww017

[7] Xu, C., Wang, K., & Guo, M. (2017). Intelligent Resource Management in Blockchain-Based Cloud Datacenters. IEEE Cloud Computing, 4(6), 50-59. doi:10.1109/mcc.2018.1081060

[8] Smith, T. (2017). The blockchain litmus test. 2017 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258183

[9] Wright, C., & Serguieva, A. (2017). Sustainable blockchain-enabled services: Smart contracts. 2017 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258452

[10] Lemieux, V. L. (2017). A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. 2017

IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258180

[11] Chen, Y., Li, H., Li, K., & Zhang, J. (2017). An improved P2P file system scheme based on IPFS and Blockchain. 2017 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258226

[12] Banerjee, A., & Joshi, K. P. (2017). Link before you share: Managing privacy policies through blockchain. 2017 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258482

[13] Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain — Literature survey. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). doi:10.1109/rteict.2017.8256979

[14] Pinno, O. J., Gregio, A. R., & Bona, L. C. (2017). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. GLOBECOM 2017 - 2017 IEEE Global Communications Conference. doi:10.1109/glocom.2017.8254521

[15] Bhattacharya, R., White, M., & Beloff, N. (2017). A blockchain based peer-to-peer framework for exchanging leftover foreign currency. 2017 Computing Conference. doi:10.1109/sai.2017.8252284

[16] Teslya, N., & Ryabchikov, I. (2017). Blockchain-based platform architecture for industrial IoT. 2017 21st Conference of Open Innovations Association (FRUCT). doi:10.23919/fruct.2017.8250199

[17] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017). Towards using blockchain technology for IoT data access protection. 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB). doi:10.1109/icuwb.2017.8251003

[18] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI). doi:10.1109/icsai.2017.8248427

[19] Marsal-Llacuna, M., & Oliver-Riera, M. (2017). The standards revolution: Who will first put this new kid on the blockchain? 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). doi:10.23919/itu-wt.2017.8246988

[20] Backman, J., Yrjola, S., Valtanen, K., & Mammela, O. (2017). Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. 2017 Internet of Things Business Models, Users, and Networks. doi:10.1109/ctte.2017.8260929

[21] Baxendale, G. (2016). Can Blockchain Revolutionise EPRs? Itnow, 58(1), 38-39. doi:10.1093/itnow/bww017

[22] Bhattacharya, R., White, M., & Beloff, N. (2017). A blockchain based peer-to-peer framework for exchanging leftover foreign currency. 2017 Computing Conference. doi:10.1109/sai.2017.8252284

[23] Chen, Y., Li, H., Li, K., & Zhang, J. (2017). An improved P2P file system scheme based on IPFS and Blockchain. 2017 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata.2017.8258226

[24] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI). doi:10.1109/icsai.2017.8248427

[25] Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain — Literature survey. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). doi:10.1109/rteict.2017.8256979