

Randomly Elected Blockchain System based on Grouping Verifiers for Efficiency and Security

DanaYang*, Sol Jeon*, Inshil Doh**, Kijoon Chae*

*Department of Computer Science and Engineering, Ewha Womans University, Republic of Korea

**Department of Cyber Security, Ewha Womans University, Republic of Korea

yangzzzz@ewhain.net, jsoul92@ewhain.net, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

Abstract— Many systems have been built for transactions without a central manager by introducing blockchain in various fields such as industry, public sector, and trading economy. The blockchain system is also contributing to the advancement of technology to enable reliable transactions in distributed networks like P2P or D2D. Consensus algorithm for each operating environment is used to verify whether a transaction is valid. Transactions are verified generally with Proof-of-work (PoW) in public blockchain and Practice Byzantine Fault Tolerance (PBFT) in private blockchain. The PBFT is only available to a group of limited participants and is used for small groups. However, these small groups can be compromised by the collusion of malicious users, making it impossible to trade or forge. In addition, the blockchain does not define any security structure on users, devices, transaction history accessibility, etc., which causes issues with system permission. Therefore, this paper analyzes the problem of the conventional blockchain in terms of participant-collusion, authentication, and confidentiality, and proposes a Randomly Elected Blockchain (REBC) to solve each problem. In the first participant-collusion, the private blockchain enables the system to operate without any cost for verification. Thereby solving the problem of grouping nodes for malicious collusion, the proposed mechanism is to randomly elect the nodes in the unit group, and then conduct consensus algorithms. Besides, many participants are able to participate in the consensus experiment without degraded performance. In the second problem, a smart manager system provides authentication of users and devices. The solution to the third problem related to confidentiality is to analyze the current RSA encryption method and supplement it with a proxy re-encryption method.

Keywords— private blockchain, consensus algorithm, authentication, proxy re-encryption, collusion

I. INTRODUCTION

To redesign significantly individual interactions in politics, business and society, blockchain technology is a massively unprecedented disintermediation process based on automated and unreliable transactions [1]. However, current infrastructures for diverse IT service requires a centralized system approach and there are some disadvantages. First, the central repository is more likely to be attacked and lost by malicious users and security solution is expensive. In addition, disadvantage is that it takes a lot of time because the authorization procedure of the central agency and various

organizations are required for the transaction to be approved. Therefore, blockchain technology in distributed network has attracted attention as a solution to the problems of the central management system. The blockchain is a decentralized ledger structure, where everyone can participate in the blockchain network and own a ledger that records all transactions. Also, the most attractive feature is also that the transaction transparency is high [2]. The participants of the distributed network jointly distribute data to prevent centralized attacks on behalf of the central management system. This saves the cost of managing the central system. By distributing and authenticating data, reliable transactions are possible without third party certification and the approval process of various organizations can be skipped. The blockchain is a mechanism to ensure the safety of data and make transactions in a short time.

However, there are issues with intentional changes and agreements, attacks by unauthorized users, and privacy of transaction details. First, blockchain is divided into two types. A public blockchain in an open environment and a private blockchain in a closed environment are appropriately used for each system. A Proof-of-Work (PoW) algorithm in public blockchain and PBFT (Practice Byzantine Fault Tolerance) in private blockchain are used to verify the transaction [11]. These algorithms should be given the cost of proof of transactions, which implies the problem of accuracy and safety. Abnormal transactions can be generated due to malicious collusion. Besides, the more number of validators also increases the processing time of the validation. Other problems may occur in which an unverified user attempts a transaction creation and the malicious transaction information is transmitted [12].

This paper proposes a Randomly Elected Blockchain (REBC) system based on a group to solve this problem. The REBC system proposes a randomly elected delegator of PBFT nodes (DBFT) to guarantee integrity, a smart manager system to ensure authentication, and a mechanism using proxy re-encryption to limit the possibility of invasion of existing personal information to ensure confidentiality [14]. There are a few advantages, i.e. a large number of users can participate to verify the transaction and efficiency indicates high throughput. Therefore, the REBC system is suggested for the

improvement of the conventional blockchain to guarantee safety and efficiency.

This paper is organized as follows. Followed by the introduction in Section 1, Section 2 discusses the traditional blockchain problems and describes authentication, proxy re-encryption techniques and PBFT consensus algorithms as the basic mechanism of the REBC system. In Section 3, the proposed REBC system is divided into the components, smart manager system, proxy smart contract, and DBFT. In Section 4, this paper experiments with the existing algorithm and compares it with the proposed mechanism. Chapter 5 concludes with some results and discussions.

II. RELATED WORKS

This section describes the authentication scheme used for the blockchain and proxy re-encryption concerning the proposed system. It also describes the PBFT that is the consensus algorithm in the private blockchain and the basic structure of the proposed system.

A. Authentication

In blockchains, there is a possibility of an attack by a malicious user who is not authorized. There is also a problem that arises because access to information is not adequately guaranteed. Therefore, participant identification such as certificate should be managed and should control access to transaction information. In the private blockchain, the participants are restricted by membership service and even the participants need continuous management of authentication. It is also necessary to confirm whether or not the request contents for the transactions have been changed by the malicious user. Recently, researchers on blockchain authentication has studied a lot of authentication procedures in exchanging critical data such as blockchain-based medical information in the cloud environment [3].

The main nodes is divided into user, issuer, and verifier. The authentication process is divided into an authentication between user and issuer and another authentication between user and verifier. In the first authentication procedure, the user's information is encrypted and sent to verify the identity and issue a key. The second authentication utilizes a random number to register membership and send a credential to create a transaction.

However, the study of authentication protocols with user and its device has not been fully studied. Therefore, this paper describes the authentication mechanism for communication of each user based on the smart manager system to prevent the authority for malicious access.

B. Proxy re-encryption

The best feature of the blockchain is its transparency, which has the advantage of allowing open access to all transaction records [4]. However, it means that the transaction information is exposed at risk and potentially misused. Even though the blockchain maintains some security in a private blockchain type, the information is still exposed to limited participants. It is possible that the information may be infringed from attacks. Therefore, some companies encrypt

and transmit information RSA encryption. In the case of Hyperledger of private blockchain technologies, the user writes down the transaction details, encrypts them, and delivers them to the endorsement validation. The endorsement encrypts the transactions with the public key of the verifier and sends it to the verifier. To pass on to not only one verifier, but also to other verifiers, the encrypted one must be decrypted and encrypted again with the other verifier's public key. In this case, the encryption and decryption process is repeated. Whenever the decryption process is performed, the information may be exposed by a malicious user and a time-consuming problem appears [5].

Proxy re-encryption technique is a scheme in which the proxy server re-encrypts a sender's ciphertext with a receiver's key and a receiver can decrypt it [6]. It means that the sender and the receiver share key information through a proxy server. The sender encrypts the plain text with its public key and generates a re-encryption key from its private key and the receiver's public key. Then the proxy server re-encrypts the ciphertext with the re-encryption key and sends it to the receiver without decrypting the ciphertext. The receiver can then decrypt the ciphertext with its private key. [7]

This scheme uses a bilinear map to generate a key which is cryptography with short key-lengths instead of complex RSA algorithms [8]. This paper based on this mechanism improves efficiently the confidentiality problem to protect transactions.

C. PBFT(Practical Byzantine Fault Tolerance)

The Byzantine Generals problem assumes that it can win when 300 soldiers attack Byzantine Castle of 100 soldiers. The generals with each 100 soldiers can communicate, but not trust each other. Since there is a traitor in the crowd, the attack may fail. In other words, the BFT algorithm is a solution to how the attack time can be agreed in an unreliable environment [9]. The PBFT algorithm is a kind of these consensus algorithms, so that all nodes participating in the distributed network can achieve one decision. Even if the traitor tries to attack fraudulently, the number of other participants should get a majority. Even though the primary lies, all participants can watch the leader's movement and judge it to be a lie [10]. The differences between these two algorithms are as follows: The BFT algorithm can be used only when the network is synchronous, whereas the PBFT algorithm is developed for the asynchronous network. The PBFT also consists of nodes called Leader who receives and delivers the client's transaction and nodes called Primary who share and verify the transaction [13].

The PBFT is a consensus algorithm commonly performed in private blockchains to make sure that the correct transaction is generated while taking into account some malicious users. The number of participants is generally $3f + 1$, $5f + 1$. etc. and f is the number of traitors. It means that the entire system proceeds without problems although there are a certain number of traitors. When the number exceeds a limited number, the transaction becomes impossible. It is restricted as the users in specific companies or groups. It can be also easy to know each other's identity and who can participate and verify. This property causes malicious collusion as a certain

number of malevolent users can be exceeded easier than the public blockchain.

As such, there are some problems with the algorithms currently used in the blockchain. The expansion problem of the blockchain nodes is critical due to the limited level of participants and throughput. Therefore, this paper deals with grouping the nodes and randomly elected verifiers as a solution to this problem.

III. PROPOSED SYSTEM

A. Overview

The proposed REBC system is divided into four parts shown in Fig. 1. Part 1 shows where unauthorized users wait for authentication. The authentication process is performed in the second part (smart manager system). After the authentication process, the smart manager owns a list of the users and its devices information including public key and verifies whether the requested member is correct. In the next part 3, transactions including businesses and finance can be written by authenticated users. These transaction requests will be validated on the private blockchain in Part 4. The transaction goes through the verification operation while maintaining the confidentiality of the transaction based on the proxy re-encryption scheme. Therefore, these functions ensure the integrity, authentication and confidentiality to enable secure blockchain to be created.

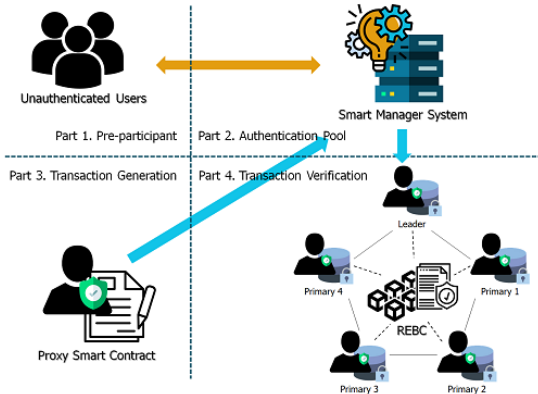


Figure 1. Whole architecture of REBC system

B. Smart Manager System

The smart manager plays two operations. The first operation is to check whether the user requesting the smart contract is the authenticated member and device as shown in Fig. 2. If a malicious user manipulates the smart contract details and sends them to the device, the wrong transaction can be executed. Therefore, the smart manager determines whether the member is authenticated and executes the smart contract. The second operation encrypts the transaction details with re-encryption key of Leader of the verifiers and transmits it to Leader. This is explained concretely the part of Proxy smart contract.

The smart manager system operates on a private blockchain and owns a list of who participates in advance. When an unauthenticated user tries to request authentication with its ID

(ID_{us}) it sends the request to the smart manager. The smart manager searches the user device's UUID with ID and generates a random number (X). Then the manager sends it with its ID (ID_{sm}) encrypted by the public key of the user (pk_{us}) and calculates X^{UUID} . The user calculates the random number X based on the previously promised UUID value of the device. The calculated value is transferred to the smart manager. If the value is the same, authentication is successful. If the value is not the same, it is rejected. The authorization is granted for transaction creation or verification. The smart manager and the blockchain can be separated to reduce the overhead of the blockchain. The UUID is a unique value of the device and squared in a random number, calculated as an unsolvable number in the polynomial time.

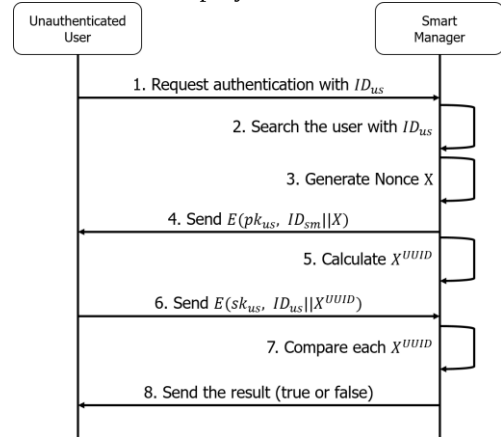


Figure 2. Authentication process for membership service

C. Proxy smart contract

The public blockchain is a peculiarity that allows anyone to be connected to the network maintaining confidentiality. On the contrary, the private blockchain is a property that only limited members can participate and transmit transaction details without encryption, before the consensus process. Even if it is encrypted and then shared, it is based on the conventional RSA algorithm. This is a repetitive process of decrypting the transaction and then encrypting it again with another user's key. There is a possibility that the information is exposed to the malicious user, and a problem that takes a lot of time appears. Therefore, this paper uses proxy re-encryption to provide the confidentiality of the transaction while sharing information.

Figure 3 is a flow chart of proxy re-encryption using the traditional RSA encryption method. When a member A requests a transaction, it is encrypted with the Leader's public key of the verifiers and delivered to the smart manager. The smart manager receives a re-encryption key from the Leader and passes the cipher-transaction by re-encryption key to each verifier. The Primaries can decrypt and share the cipher-transaction. This process ensures the confidentiality of the transaction details due to the characteristic of the bilinear map not solved in the polynomial-time and eliminating the decryption process.

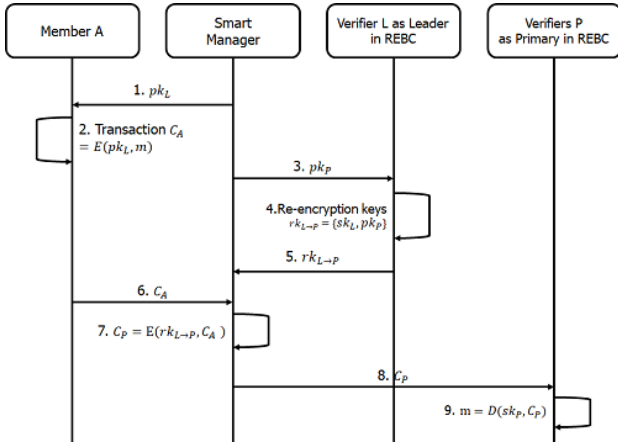


Figure 3. Sharing transactions based on proxy re-encryption

D. DBFT

The REBC system is composed of two consensus algorithms as shown as Fig. 4. The first consensus process uses a PBFT based on proxy smart contract in the group that received the transaction request. It is composed of a small group, so that the majority of them remain collaborative and deteriorate problem. In the second consensus process called The DBFT (Delegator of Byzantine Fault Tolerance), a delegator of validators are randomly selected in each group, and the delegators go through the PBFT process once again. If the result of the first consensus process and the second consensus process coincide with each other, the block is generated and broadcasted. If they do not match, the transaction is rejected.

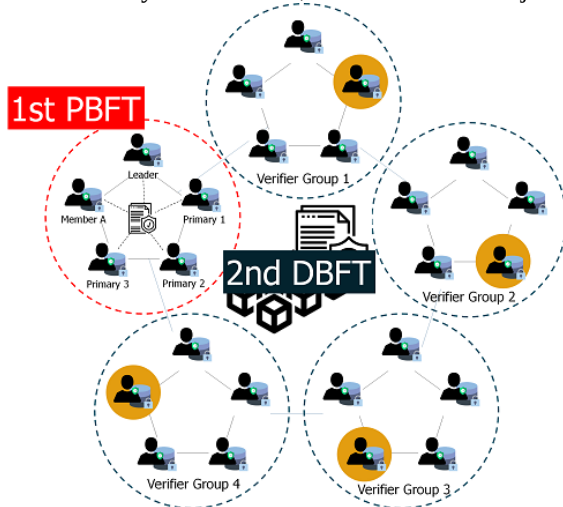


Figure 4. Whole Architecture of REBC

As a result, when verifiers agrees with a randomly selected verifiers from another group, the transactions can be judged more objectively from a third party's point of view. This consensus process allows the second group to filter out incorrect results, even if the first group produces wrong results. The probability of malicious collusion can be reduced. Fig. 5 illustrates the flow of the 2 stage process for consensus in REBC system.

The member A writes a transaction with proxy smart contract and asks the blockchain network for validation. Verifiers accepts these requests and share the transaction. After this transaction is proved through the first PBFT, the delegators are randomly elected in other verifier groups and again perform PBFT process, called DBFT. After DBFT processes, all verifiers share the results of the two verified transactions and confirm whether those are matched. The final transaction is delivered as the block and is added to the blockchain.

Therefore, proxy smart contracts are used in a private environment and the DBFT algorithm is proposed to reduce the probability of malicious collusion and to ensure the accuracy and safety of transactions.

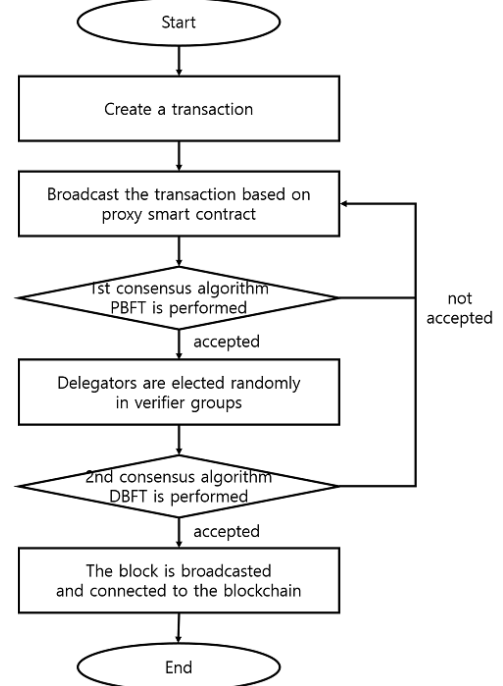


Figure 5. Flow of the 2 stage process for consensus in REBC system

IV. EVALUATION

The verifier is selected with the randomized characteristics of the proposed REBC. In this section, the probability of malicious collusion was analyzed. In addition, the experimental results are derived based on the scalability of the consensus algorithm. We experimented with the PBFT to derive the performance speed according to the number of users and to compare and analyze the throughput with the proposed algorithm.

A. Environment

The PBFT algorithm used Hyperledger Fabric from IBM and experimented with the Docker engine. It works based on Linux, and the result is shown by the Rest API. We experimented by increasing the number of participants by converting peers and members to the main libraries used. We tested the transaction process using a chaincode of the smart contract based on the Go language. The DBFT algorithm was

also compared with the current PBFT using Hyperledger's open source provided by IBM.

B. Collusion rate

The private blockchain can be used only by a confined number of participants, so the number of people is defined. Compared to the public blockchain, it is more likely to know each participant and collaborate with malicious behavior. This causes the wrong transaction to be accepted. Therefore, this paper proposes a method to randomly elect delegators of validators that perform consensus algorithms to reduce the probability of collusion. Equation (1) means the probability of malicious collaboration and is lower when using a randomized selection method.

$$P_{a_i} = \frac{\text{degree of closeness}((R_{IE_i} \times R_{P_i} \times R_{ac_i})/node_{c_i})}{\sum_{i=1}^n ((R_{IE_i} \times R_{P_i} \times R_{ac_i})/node_{c_i})} \quad (1)$$

TABLE 1. SYMBOL EXPLANATION IN EQUATION

Symbol	Explanation	Level
R_{IE}	Internal/External	1~10
R_P	Position	1~10
R_{ac}	Acquaintance	1~10

The private blockchains are commonly used in environments with organizations such as companies. To indicate the probability of fixing by randomization considering this issue, the correlation as a reference is shown in Table 1. The parameter R_{IE} shows the relationship level from level 1 to 10 indicating whether or not the transaction is related to the requested group. If the department is the same department, the level is 10, and if it is not absolutely related to the department, the level is 1. For example, as the department of neurosurgery was included in the department of internal medicine, the level was divided considering the mutual inclusion relation. The parameter R_P shows a correlation based on high probability of intimacy when the position of the organization like editor, are the same. The smaller the difference between the ranks, the level is 10. The parameter R_{ac} classifies the relationship of intimacy into a level by judging whether or not a person actually knows it, regardless of position and related department. The higher the intimacy, the level is expressed as 10. Based on this, Fig. 6 shows the probability of malicious fixing between PBFT and DBFT algorithm.

Fig. 6 shows the application of Equation (1) to analyze the intimacy about all nodes of the PBFT and DBFT. As the number of nodes increases, both algorithms show a lower fixing rate. However, small organizations have a higher probability of malicious collusion in the PBFT. The DBFT, on the other hand, shows that the probability of malicious collusion can be reduced by randomly selecting consensus validators although it has a small number of people. Therefore, the DBFT algorithm means that agreement can be achieved on an objective basis.

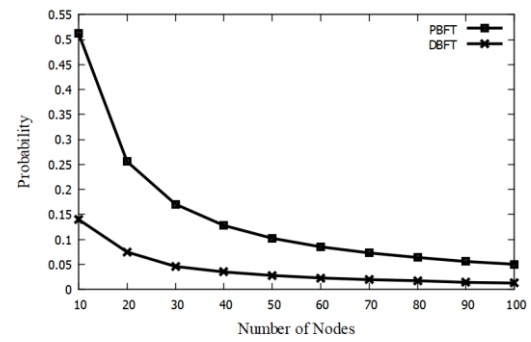


Figure 6. Comparison with probability of malicious collaboration of the PBFT and the DBFT

C. Time efficiency

The DBFT takes less time than PBFT because it is performed with a small number only including the delegators of each group. The group in Fig. 7 is created and restricted to lower 15 people in each group. In case of one group, the DBFT takes more throughput than a PBFT. If there are enough nodes to create more than one group, it can maintain a constant execution speed. Therefore, it is important how many nodes are included per group.

Fig. 8 compares and analyzes the maximum number of groups participating in the DBFT algorithm. The units of the group were divided into 10, 12, and 15 people for comparative analysis. It can be seen that when the 10-member group was formed, the consensus time is less than the 15 people in a group. It means that the smaller the number of participants of groups, the less time is taken.

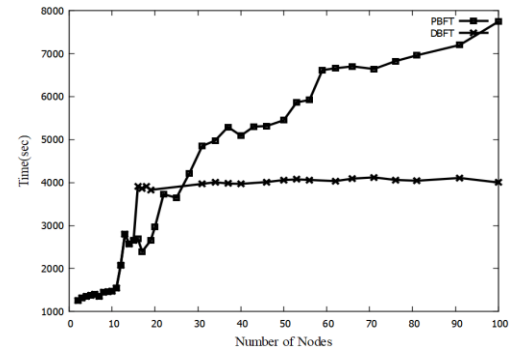


Figure 7. Comparison with performance time of the PBFT and the DBFT

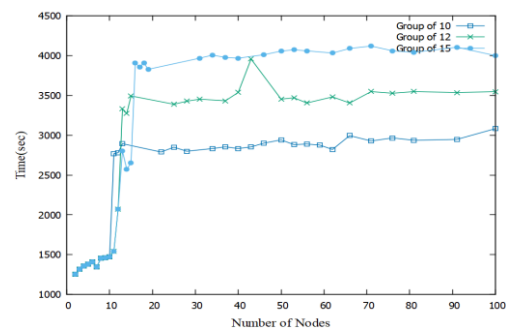


Figure 8. Comparison with performance time according to the number of people in group

D. Security Analysis

The authentication has not been considered as an important topic and has provided not much detail protocols in the blockchain. The public blockchain even does not require any authentication step because everyone should be able to participate in the blockchain network. Therefore this paper presents the user authentication based on the smart manager system. The members requesting the transactions are included in the authentication pool and are authenticated separately from the smart manager. It means that the role of the blockchain is parted to reduce the overhead of the network except the payload for the transactions. The presented authentication can ensure more secure transactions from malicious users.

The properties of the blockchain are basically to reveal transparently the transaction details and to provide the integrity of the transactions. It is difficult to provide confidentiality to conceal the contents. The transaction contents are encrypted and verified commonly on the RSA algorithm in the private blockchain. However, the exposure of the contents may occur in the repeat process of encrypting and decrypting the transactions. Therefore, this paper encrypts the transaction on the proxy re-encryption algorithm to eliminate the decryption process and to reduce the processing time.

The consensus algorithm of the blockchain is used to verify and share the blocks, but each algorithm has some disadvantages. Since the PoW algorithm able to participate anyone is performed by so many users, more than half of participants take too long time to complete the consensus process. Whereas, the BFT which allows the authenticated users to participate and to verify the block takes less time than the PoW. But the probability of malicious collusion attack increases, because only the small number of users generally participates in the consensus process. Therefore, this paper shows that the attack is sufficiently prevented by the DBFT algorithm. In addition, the DBFT improved the limitations of each algorithm and produced better performance.

V. CONCLUSIONS

Currently, blockchain is being developed and applied in various fields. Starting from the financial sector such as Bitcoin, Ethereum, and Ripple, it is expected to be actively applied in various fields such as fintech, e-commerce, and industrial application. Blockchain is largely divided into two methods: the public blockchain is a mechanism commonly in where everyone can participate in the network, and the private blockchain is used in industries and companies. The private blockchain especially has a disadvantage of the higher probability of malicious collusion than the public blockchain. To block these malicious users, the total number of users must be increased, but it can not be increased beyond a certain number. As a result, there is a problem of trust issue in the private blockchain. Therefore, this paper proposed the authentication scheme, proxy smart contract for the information disclosure problem that may occur during the transaction and secure consensus process. Lastly, this paper

presents the mechanism to derive and analyze the results of security and time efficiency. Based on this, this blockchain technology suggests that it can be used in various fields in the future.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No.2019R1F1A1063194). Corresponding author is Kijoon Chae (e-mail : kjchae@ewha.ac.kr).

REFERENCES

- [1] Atzori, Marcella. "Blockchain technology and decentralized governance: Is the state still necessary?." Available at SSRN 2709713 (2015).
- [2] Hwang, Junyeon, et al. "Energy prosumer business model using blockchain system to ensure transparency and safety." *Energy Procedia* 141 (2017): 194-198.
- [3] XIA, Qi, Emmanuel Boateng Sifah, Alba Smahi, Sandro Amofa, Xiaosong Zhang. "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," MDPI AG, Basel, Switzerland, April. pp 44, 2017 8.
- [4] Benchoufi, Mehdi, Raphael Porcher, and Philippe Ravaud. "Blockchain protocols in clinical trials: Transparency and traceability of consent." *F1000Research* 6 (2017).
- [5] Junggab Son, Donghyun Kim, Rasheed Hussain, Heekuck Oh, "Conditional Proxy Re-Encryption for Secure Big Data Group Sharing in Cloud Environment," 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data.
- [6] Song, You-Jin, and Jeong-Min Do. "Secure Data Management based on Proxy Re-Encryption in Mobile Cloud Environment." *The Journal of Korean Institute of Communications and Information Sciences* 37.4B (2012): 288-299.
- [7] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." *IEEE transactions on computers* 62.2 (2011): 362-375.
- [8] Woo, Chan-Il, and Eun-Hee Goo. "A Study on the Operation Components for Elliptic Curve Cryptosystem based on a Real Number Field." *Journal of the Korea Academia-Industrial cooperation Society* 13.2 (2012): 795-800.
- [9] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4.3 (1982): 382-401.
- [10] Sukhwani, Harish, et al. "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)." 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE, 2017.
- [11] De Angelis, Stefano, et al. "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain." (2018).
- [12] Baliga, Arati. "Understanding blockchain consensus models." Persistent. 2017.
- [13] Zhiguang Qin, Hu Xiong, Shikun Wu and Jennifer Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing, LCNS* 1939-1374, April. 2016.
- [14] Jeon, Sol, Inshil Doh, and Kijoon Chae. "Rmbc: Randomized mesh blockchain using dbft consensus algorithm." 2018 International Conference on Information Networking (ICOIN). IEEE, 2018.



Dana Yang received the B.S. degree in the Department of computer software at Korean Bible University in 2013. She is currently a Ph.D. candidate in the Department of computer science and engineering at Ewha Womans University, Seoul, Korea. Her research interests include authentication, blockchain, steganography, FANET (Flying Adhoc Network) security and D2D network security.



Sol Jeon received M.S. degrees in Computer Science at Ewha Womans University, Korea in 2018. She currently works for a network establishment and service provider in IT companies in Korea. Her research interests include blockchain, authentication, authority and VANET security.



Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009-2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul. Her research interests include wireless network, sensor network security, and M2M network security.



Kijoon Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984. He received a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in the Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include blockchain, security of FANET(Flying Ad Hoc Networks), sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.