RMBC: Randomized Mesh Blockchain Using DBFT Consensus Algorithm

Sol Jeon
Department of Computer Science and Engineering,
Ewha Womans University
Republic of Korea
jsoul92@ewhain.net

Inshil Doh
Department of Cyber Security
Ewha Womans University
Republic of Korea
isdoh1@ewha.ac.kr

Kijoon Chae
Department of Computer Science and Engineering
Ewha Womans University
Republic of Korea
kjchae@ewha.ac.kr

***Abstract*— The blockchain is decentralized network system that verifies the validity of the transaction through the consensus of the verifiers without trusted third parties. This mechanism ensures transaction integrity disclosing transaction information transparently. Therefore, it is emerging as the core technology of the 4th industrial revolution by improving reliability and efficiency with features of decentralization, ensuring the integrity, and economic cost reduction. However, there are some problems with the growth of the blockchain. The popularly used PoW (Proof of Work) consensus algorithm applied to the public blockchain requires the price to be compensated in order to agree on the validity of the transaction. This has the disadvantage that the system doesn't operate without compensation. Also, the BFT (Byzantine Fault Tolerance) Algorithm using private blockchain has a limited number of acceptable malicious users. In this case, if the users collude with malicious and exceed the limited number, the transaction is rejected. In this paper, we propose a Smart Manager System and RMBC-DBFT (Randomized Mesh Blockchain Diversity of opinion BFT) enables the safe transaction to the problems above.**

***Keywords*— RMBC, DBFT, BLOCKCHAIN, PUBLIC, PRIVATE, BYZANTINE FAULT TOLERENCE, PROOF OF WORK, CONSENSUS, RANDOMIZED, SMART CONTRACT, SMART MANAGER**

I. Introduction

Recently, with the emergence of the era of the fourth industrial revolution, peer-to-peer (P2P) and machine-to-machine (M2M) technology to connect individuals with objects and machines have come to the fore. However, as these technologies are centered on the central management system they have several disadvantages as follows. First, since all the data is concentrated in the center, it is easy to lose data when the central repository is attacked by the hacker which is also very expensive to protect. In addition, in order for a transaction to be approved, it is necessary to go through the approval process and the procedure of various institutions through the central agency takes a lot of time. Therefore, a blockchain technique applying a decentralized distributed network has attracted numerous attention as a solution to the problem of the central management system. The blockchain is a public transaction ledger and a technique to prevent hacking that may occur in the transactions using virtual currencies. It is a form of distributed database. It provides the advantage of saving cost to manage the central management system by distributing data jointly via the participants of the distributed network. In addition, it operates without any third-party certification authority, ensuring reliable transactions and data security.

Currently, such a blockchain is applied in various fields. The blockchain can be used for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money, hard assets and intangible assets (votes, ideas, reputation, intention, health data, etc.) [1]. They can be classified as a public blockchain and a private blockchain. In the public blockchain, anyone can participate in the network and create a transaction, as it is free to participate. In order to make such a system operate smoothly, there should be compensation for executing the proof task. It proves transactions through mining work by collecting transactions in a block in every minute using a Proof-of-Work (PoW) algorithm. In PoW algorithm, the Proof-of-Work is implemented by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the Proof-of-Work, the block cannot be changed without re-doing the work [2]. Representative services using this algorithm are Bitcoin and Ethereum.

On the other hand, in a private blockchain, authorized users and verifiers only can validate transactions, and only those with legal responsibility can create transactions. It is, therefore, suitable for private organizations or small institutions that place importance on the protection of data. It proves the transaction in such a way that the participant will obtain the specified majority of the agreements for the transaction using the BFT types agreement algorithm. BFT is the first Byzantine-fault-tolerant, state machine replication algorithm that is safe in asynchronous systems such as the Internet: it does not rely on any synchrony assumption to provide safety. In particular, it never returns bad replies even in the presence of denial-of-service attacks [3]. Typical fields of using it include IBM's Hyperledger Fabric and R3 Corda. However, there are two major problems when using the above two algorithms.

- First, in the PoW algorithm, systems can be maintained only when the compensation for the transaction proof is

978-1-5386-2290-2/18/$31.00 ©2018 IEEE

made. Thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees [4].

- Second, in the algorithm of BFT, a transaction is concluded with a number of agreements, and there are some possibilities to lead to incorrect transactions when there are many malicious users. That is, some of the generals may be traitors, trying to prevent the loyal generals from reaching an agreement [5]. To exclude such malicious users 3f + 1 algorithm is used. But when malicious users are increasing, such an abuse cannot be prevented, because the number of nodes of all participants is limited. In addition, if a high weight is given to a specific user, the user having a large weight can also be a malicious user.

In order to solve this problem, this paper proposes possibilities to solve the above problem by applying RMBC (Randomized Mesh Blockchain) using DBFT (Diversity of opinion Byzantine Fault Tolerance) algorithm. Section □ discusses the fields to which PoW and BFT are applied and the associated problems. Section □ describes the overall structure of RMBC to solve the PoW and BFT algorithm problems. Section □ describes the technical simulation in detail and concluding remarks can be found in section □.

II. THE PROBLEMS ABOUT POW & BFT ALGORITHM

The blockchain is a decentralized method that is different from the existing transaction methods. So, the technique is a technology that allows a secure transaction with an unreliable third party without a certification authority. This blockchain technology is based on a distributed ledger and a common ledger is held by each individual. When a user requests a transaction, the integrity of the blockchain can be verified based on the ledger and the reliability can be guaranteed. Integrity assurance is the task to include the hash value of the previous block in the block header so that the contents of the verified block cannot be changed when the current block is created. By connecting the blocks in this way, the reliability of the block improves as the chain increases, which eventually enables safe transactions. In addition, when using a blockchain, the transaction is very economical because it only took a day which used to take 3-4 days in the existing transaction methods. These blockchains are classified into two categories: public blockchain, in which everybody can participate in and prove transactions, and private blockchain, which is suitable for private institutions in a semi-centralized form.

A. *Public Blockchain*

A typical example of a public blockchain is a Bitcoin. Bitcoin is a digital currency created by Nakamoto Satoshi in 2009. It is a virtual currency that does not have a central management system for issuing and managing the currency. The transaction is made by trading using a p2p-based distributed database and verifying the data through the PoW agreement algorithm. The PoW algorithm is a calculation process to find a value that matches the target value. This calculation process is a process of finding a target value by adding a value obtained by calculating the current transaction details, a header value of a previous block, and a random numeric value. However, it is necessary to pay a certain price to the miners in order to find the target value and to prove the transaction [4]. Bitcoin pays for it in a form of fees. Therefore, the process of verification incurs a certain fee. In this paper, we tried to solve this problem through Smart Manager based on Smart Contract.

B. *Private Blockchain*

A typical example of a private blockchain is IBM's Hyperledger Fabric. The Hyperledger Fabric project is a collaborative project to develop blockchains by identifying important functions for industrial standards for Distributed Ledger. The transactions are made by proving data through PBFT algorithm. The PBFT algorithm is a method to ensure that the agreement of the users participating in the distributed system can be made correctly even when malicious users do not follow the prescribed rules. In order to prevent malicious users from making the incorrect decision, the transaction is made with the agreement of the pre-defined majority such as 3f + 1 and 5f + 1. This means that if there are three malicious users (f = 3), the number of total users must be at least over ten to get the correct agreement result.

However, since this algorithm is based on a private blockchain, there is a limitation on the total number of users. Therefore, if the number of malicious users exceeds the number that the algorithm can defend, it will not be possible to obtain a correct result [5]. For example, if the limit of the total number of users is 100, then this algorithm can work properly only when the number of malicious users corresponding to f is 33 or less. If malicious users are 33 over, the algorithm cannot prevent malicious users from abusing the system. Besides, due to the nature of the private blockchain, it is highly likely that malicious collusion exists within the members because it is composed of small groups within the enterprise. If malicious users exceed majority and make collusion to pass a transaction, it is impossible to get the right result. If the system gives a higher weight to a specific user to prevent this, the above problem may occur because the specific user may also become a malicious user. Therefore, in this paper, we proposed a solution to the problem by a randomized mesh blockchain (RMBC) using DBFT algorithm.

III. DESIGN OF RANDOMIZED MESH BLOCKCHAIN

The structure of the proposed system is as follows. First, we propose a system that does not have to pay a price when trading a smart contract by applying Smart manager. Second, we propose a technique to eliminate the possibility that a majority of users become malicious users by applying RMBC based on DBFT as Fig. 1 shows. Fig1 shows a structure where Smart Manager reduces the overhead of blockchain by managing the authentication part to the general private blockchain. First, when a user requests a transaction, it is transferred to a blockchain to generate a block. The transaction in the block is verified by the verifier. The Smart Manager checks whether the transaction is verified by the blockchain. After that Smart Manager executes the transaction. The structure consists of next elements.

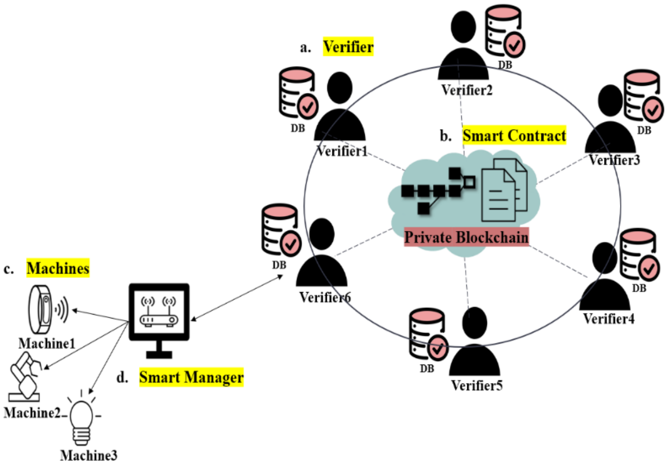

Fig. 1. The Smart Manager System Smart Manager System based on Smart Contract

A. *Smart Manager System*

Consists of a verifier that verifies the transaction, a Smart Contract to which rules of a specific group are applied, and machines that execute the contract based on them. There is also a Smart manager that manages the relationship between Private Blockchain and Machines. Detailed explanations of such elements are given below.

1) *Verifier*

Since the blockchain applied to the system operates on a private basis, users can participate only when they are verified by the central administrator. This requires authentication between the user and the server, which will be covered in the next extended paper. Thus, authorized users can request jobs based on their individual databases. The requested block is passed to the block chain after the verifier has verified the transaction and then a new block is added and the transaction is approved. In addition, they determine whether the transaction details have been correctly created with their own databases.

2) *Smart Contract*

A Smart Contract is a contract that specifies actions that must be performed according to proven conditions. This is a document specifying "what should be delivered to whom" based on the rules of a certain group to make the correct result. In this system, Smart Manager is applied to this Smart Contract so that correct operation can be performed without any cost. For example, assuming that A pays $ 2 to B and exchanges with papers, A first pays $ 2 according to established rules. Later, the Smart Contract checks if the $ 2 has come to B and then it gives the paper to A. As these decisions are made based on rules written in details in the Smart Contract, right transactions can be made without compensation.

3) *Machines*

Machines or equipment will perform the Smart Contract agreed by the verifier. They can participate only when they are verified by Smart Manager System's administrator. These kinds of devices include IoT devices, low-power devices, and small storage devices, and devices with small storage space to perform simple functions according to the command.

4) *Smart Manager*

Smart Manager plays two roles. The first role is to determine whether the Smart Contract has been verified by the verifier or not. This is because if a malicious user manipulates a Smart Contract that has not undergone an agreement process and delivers it to the device, the wrong command can be executed. Therefore, in order to prevent this, the Smart Manager judges whether the smart contract is verified or not before the execution. Second, it judges if the device is authorized by the Manager. This prevents malicious manipulations so that Smart Contract can be performed correctly.

The Smart Manager System enables safe transactions and ensures data integrity based on Smart Contract, thereby preventing compensation problems caused by PoW consensus algorithm. In addition, an unnecessary connection can be blocked by authenticating the device. This replaces the role of the block chain, which reduces the overhead incurred in the authentication confirmation part of the block chain.

B. *RMBC based on DBFT Algorithm*

The BFT algorithm is a way of getting the majority of the consent and operating the system with the result. However, in a small group using a private blockchain, there is a possibility of rejecting that a majority of the users becomes malicious users and make collusion. To solve this problem, we propose DBFT algorithm and RMBC blockchain as shown in Fig. 2.

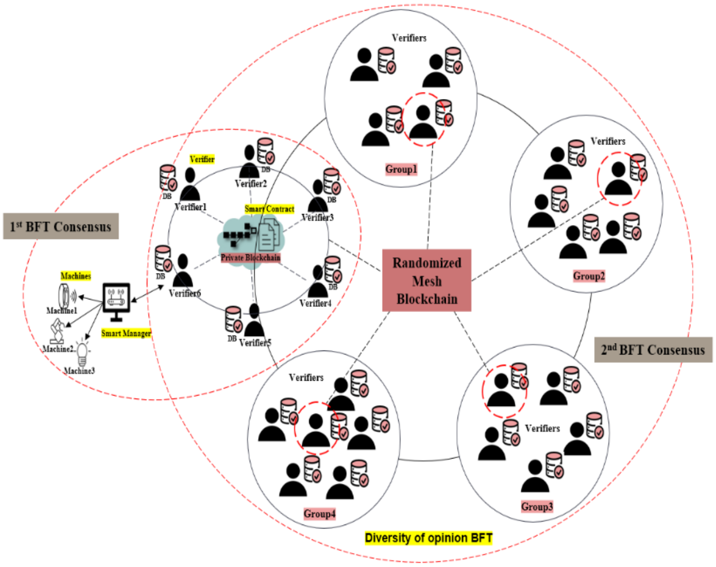

Fig. 2. RMBC using DBFT algorithm

The proposed DBFT (Diversity of opinion Byzantine Fault Tolerance) goes through two-layer consensus agreement processes. The first agreement process uses the general BFT algorithm. This is a structure where there is a possibility that a majority of the users will collude and maliciously change the process when it is composed of the small group. Therefore, there is the second agreement process. The second agreement process involves grouping the related departments and dividing them into groups. After that, an RMBC randomly selects verifiers from each department and they go through the second agreement process. At this time, if the first agreement process and the second agreement process coincide with each other, it will perform the transaction. If they are not identical, the transaction will be rejected. If we compare two processes such as having an agreement process among users in the same group and having an agreement process with a user who is randomly selected in another group, the latter seems more objective and the verifiers randomly selected from other groups may judge the transaction from the third party's perspective. Therefore, it is expected that the probability of collusion is reduced.

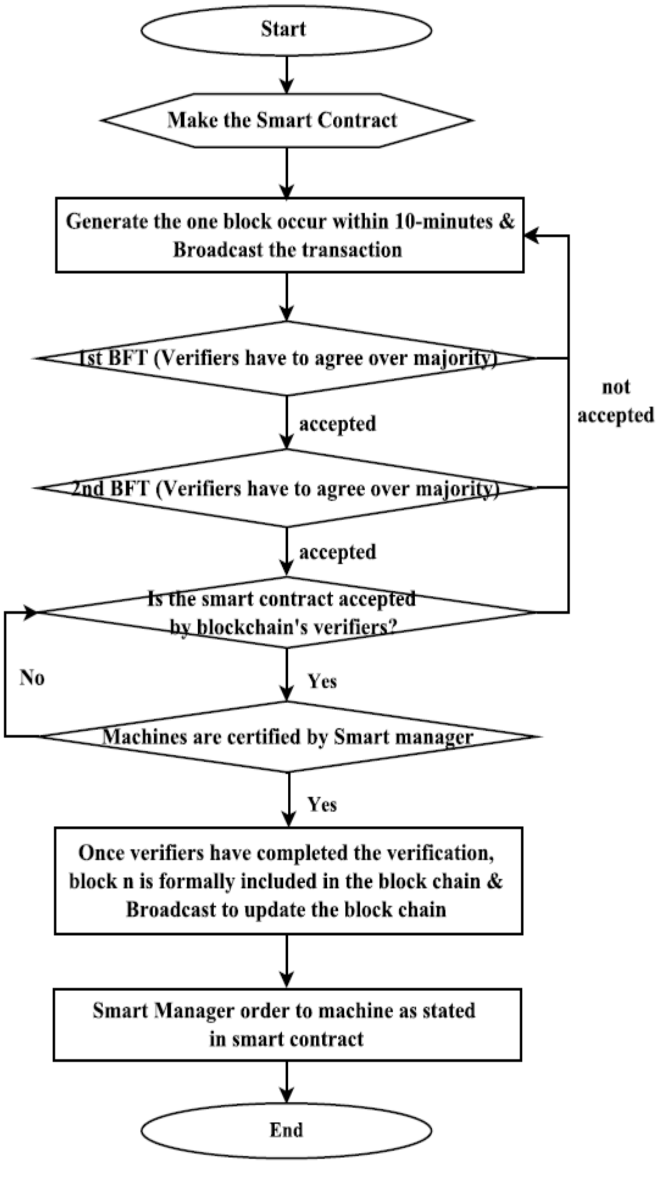
Start
Make the Smart Contract
Generate the one block occur within 10-minutes & Broadcast the transaction
1st BFT (Verifiers have to agree over majority)
not accepted
accepted
2nd BFT (Verifiers have to agree over majority)
accepted
Is the smart contract accepted by blockchain's verifiers?
No
Yes
Machines are certified by Smart manager
Yes
Once verifiers have completed the verification, block n is formally included in the block chain & Broadcast to update the block chain
Smart Manager order to machine as stated in smart contract
End

Fig. 3. RMBC structure flow chart

RMBC structure is closer to the characteristics of the private blockchain, but it is different from the private blockchain because it randomly selects verifiers from each group by grouping users. Thus, the first consensus makes agreement within groups of a user which requested transaction. And the second consensus makes an agreement external groups of a user which is selected to randomization. With these countermeasures, it becomes a more secure agreement process. It performs the following flowchart as shown in Fig. 3.

A user creates a Smart Contract and asks the blockchain to reach an agreement. The blockchain accepts this request, creates a block, and broadcasts the transaction. This transaction is verified through the first BFT agreement and then the second agreement is made based on the result. After confirming the correct transaction through two agreement processes, the transaction details are transferred to Smart Manager. Smart Manager will verify if the agreed contents meet the conditions of the Smart Contract. Additionally, it judges if the devices operating on this are authenticated. When it is verified through these processes, the transaction history is added to the block and the completed transaction details are broadcasted to update the blockchain. Finally, Smart Manager orders the command as written to the authenticated device.

IV. Simulation-Analsis

A. Detailed Numerical Analysis

The above proposed RMBC method based on the DBFT is capable of blocking malicious collusion when verifiers are selected at random. To verify this, the following formula in (1) [6] is applied.

$$P_{a_i}(\%) = \frac{degree\ of\ closeness((R_{IE_i}\times R_{p_i}\times R_{ac_i})/node_{c_i})}{\sum_{i=1}^{n}((R_{IE_i}\times R_{p_i}\times R_{ac_i})/node_{c_i})}\times 100 \qquad (1)$$

The parameters used are shown in Table I.

TABLE I. Probability Parameters

R_{IE_i}	R_{p_i}	R_{ac_i}
Relation (Internal/External)	*Relation (Position)*	*Relation (acquaintance)*
Level 1-10	*Level1-10*	*Level1-10*

R_{IE} judges whether it belongs to the department related to A that requested the transaction or whether it is an external department, and indicates the level from 1 to 10. The higher the level is, the more likely it is to be involved with the requesting department. In addition, R_P expresses the difference between the job position by comparing the positions. If they are on the same level, it is calculated as 10. The higher the level is, the closer their grade difference is. Finally, R_{ac} expresses whether they know each other or not. In Fig 4, it can be seen that in the first agreement, the probability of collusion is high when the number of users is small and when they are in the same field. However, if randomization is applied to these equations and applied to the second agreement process, the probability of collusion may still be higher when the number of users is smaller. However, the probability of collusion is smaller than when only the first agreement process is applied.

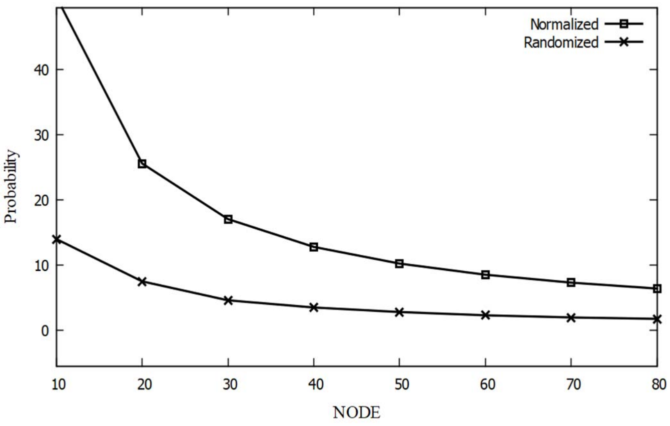

Fig. 4. Nornalized BFT vs Randomized Mesh BC_DBFT

This is because the external group randomly selects the verifier. As it is impossible to know who is being elected, and because the less relevant user verifies the transaction, it is possible to make the right judgment objectively from the third party's perspective. Therefore, using RMBC based on DBFT can reduce the probability of malicious collusion without the payment for the transaction verification.

B. Graphical Analysis

In the BFT algorithm, the number of participants is limited as shown in the following graph of Fig 5. When the number of users increases by a predetermined number, the amount of throughput is not increased any more. This stems from the fact that the message pattern of PBFT is a very complex one, which increases the response time and limits the throughput of PBFT [8]. However, since it consists of a number less than PoW users of users as shown in Fig 5, it shows the relatively high throughput. So, the graph shows that BFT has limited participants while maintaining a higher performance.

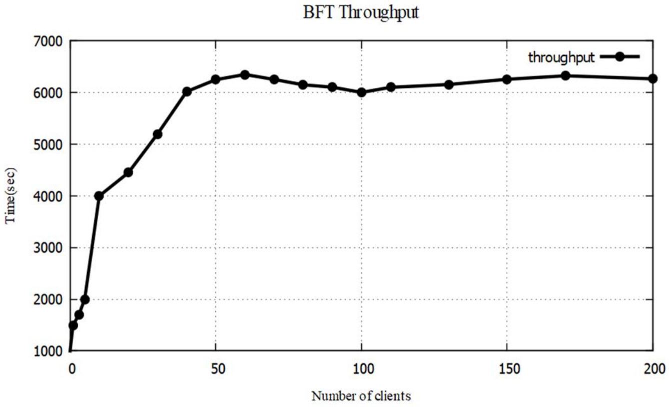

Fig. 5. Throughput for the BFT Algorithm based on data provided by [3]'s figure 8-8, 8-10, 8-11.

This graph (Fig 5) shows that the BFT algorithm provides high performance. Therefore, since the proposed DBFT algorithm is based on BFT, the as much performance as of BFT is guaranteed.

TABLE II. SIMULATION ENVIRONMENT

Algorithm	Proof of Work
OS	Window 10
Tool	Eclipse Jee Neon, Gnuplot 5.2
Language	Java, C
Java version	JDK 8
Open Source	Proof of work (github)
Block Contents	sha512Hash + startTime + nonce + createZeroNum + Contents
Main Library	Java.io.* Java.util.* Java.security.* Java.time.* Java.nio.*

On the other hand, as shown in the following graph of Fig. 6, the PoW algorithm has a structure in which anyone can participate and so there is no limit to the number of users. However, throughput gets smaller when there are more users. Because the transaction is determined via consensus by all nodes in order to achieve an average of only one result every 10 minutes in the entire network [9]. Thus, the graph (Fig. 6) show that PoW can enable participation of lots of users, but has a low performance with the increase in the number of users.

Table □ shows the PoW Algorithm simulated environment. We used window 7 for OS, and the tool is coded using eclipse. The coding language used Java as the main, and the graph was drawn using Gnuplot 5.2 version. The requested transaction details include the following block contents. Blocks are created by encrypting the transaction history with the hash function, the first time the block was created, the nonce that increases from zero to the desired value, the number of zeroes that produce the correct answer, and the transaction contents.

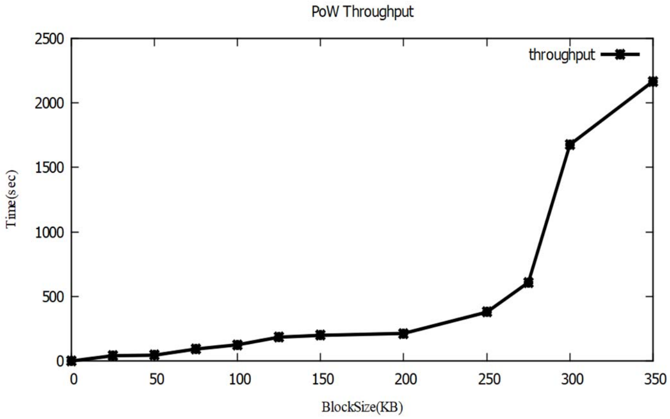

Fig. 6. Throughput for the PoW Algorithm

The following is a graph (fig 6) of the result of performing the mining of hashed blocks as the number of nodes increases. And the time is the result of excluding 10minutes time to mining. As a result, the BFT is characterized by a small number of nodes participating, but with high throughput and PoW is characterized by low throughput, but large numbers of nodes can participate.

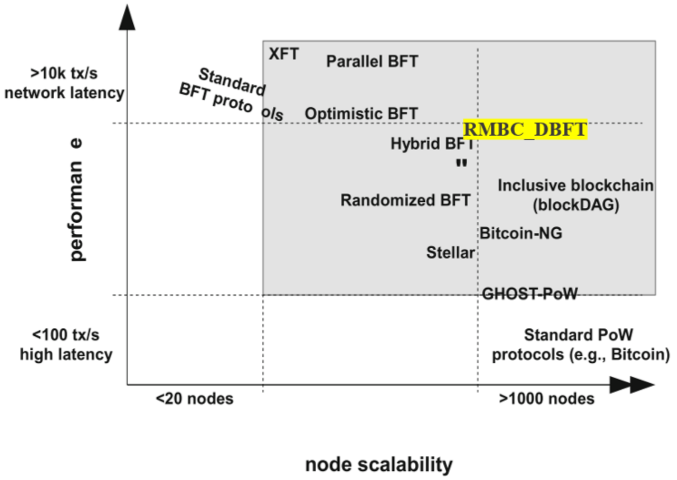

Fig. 7. Throughput for the PoW Algorithm

The presented RMBC_DBFT satisfies the following conditions in the reference graph of Fig 7. This shows that the algorithms associated with PoW, Bitcoin NG[11], and Ghost-pow[12] accommodate a large number of nodes, but with low throughput. Conversely, we can see that the number of nodes is low, but the throughput is high like BFT is Zyzzyva[13] and BFT SMART[14]. Roughly speaking, PoW based blockchain offers good node scalability with poor performance, whereas BFT-based blockchain offers good performance for small numbers of replicas, with not-well explored and intuitively very limited scalability [7]. But proposed RMBC-DBFT achieves inclusion of lots of participants and as high performance as BFT as shown Fig 7.

The proposed method based on a private blockchain, thus can enable lots of users to participate in RMBC as they are divided into groups. In addition, RMBC-DBFT has high throughput using twice BFT algorithm. Because the verifier is selected to the group one by one and verify with a small number, so it can have throughput like BFT. However, overhead can be incurred by applying the BFT twice in the transaction processing section. Therefore, the proposed method in this paper can have a large number of participants by grouping with similar fields and few number of verifiers by randomized selection without reducing performance.

V. Conclusion

The following problems may arise when the existing Blockchain algorithms such as PoW and BFT are used. First of all, with PoW, verification payment should be made to operate the system smoothly. If BFT, the likelihood of malicious collusion increases as it is composed of a small group. Therefore, in order to solve these problems, this paper proposed RMBC based on the DBFT algorithm and proposed the possibility that malicious collusion could not happen by using the prescribed formula. In addition, the proposed technology can expand the number of participants like PoW and can expect better performance than PoW as it uses the BFT algorithm. Therefore, the Smart Manager System reduces the overhead incurred in the authentication part of the blockchain and the RMBC-DBFT solves the problem of malicious collision, ensuring the safer integrity and enabling reliable transactions. This can be applied to various fields. Some possible scenarios could be the Smart Home, Smart City, manufacturing businesses, and management systems using IoT. In the future, we will discuss authentication problems between the server and the user and will discuss the privacy issues that arise when dealing with transactions.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016R1A2B4015899). Kijoon Chae is the corresponding author.

References

[1] SWAN, Melanie. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[2] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] CASTRO, Miguel; LISKOV, Barbara. Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 2002, 20.4: 398-461.

[4] KING, Sunny; NADAL, Scott. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 2012, 19.

[5] LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 1982, 4.3: 382-401.

[6] WU, Wenbo; KANG, Rui; LI, Zi. Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities. In: *Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on*. IEEE, 2015. p. 1618-1622.

[7] VUKOLIĆ, Marko. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: *International Workshop on Open Problems in Network Security*. Springer, Cham, 2015. p. 112-125.

[8] AUBLIN, Pierre-Louis, et al. The next 700 BFT protocols. *ACM Transactions on Computer Systems (TOCS)*, 2015, 32.4: 12.

[9] DECKER, Christian; WATTENHOFER, Roger. Information propagation in the bitcoin network. In: Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, 2013. p. 1-10.

[10] SOMPOLINSKY, Yonatan; ZOHAR, Aviv. Secure high-rate transaction processing in bitcoin. In: *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2015. p. 507-527.

[11] EYAL, Ittay, et al. Bitcoin-NG: A Scalable Blockchain Protocol. In: *NSDI*. 2016. p. 45-59.

[12] SOMPOLINSKY, Yonatan; ZOHAR, Aviv. Secure high-rate transaction processing in bitcoin. In: *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2015. p. 507-527.

[13] KOTLA, Ramakrishna, et al. Zyzzyva: speculative byzantine fault tolerance. In: *ACM SIGOPS Operating Systems Review*. ACM, 2007. p. 45-58.

[14] BESSANI, Alysson; SOUSA, João; ALCHIERI, Eduardo EP. State machine replication for the masses with BFT-SMaRt. In: *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*. IEEE, 2014. p. 355-3