Blockchain-based Perfect Sharing Project Platform based on the Proof of Atomicity Consensus Algorithm

Eunhee Lee, Yongik Yoon, Gyu Myoung Lee and Tai-Won Um

Abstract: The Korean government funded 12.8 billion USD to 652 research and development (R&D) projects supported by 20 ministries in 2019. Every year, various organizations are supported to conduct R&D projects focusing on selected core technologies by evaluating emerging technologies which industries are planning to develop. To manage the whole cycle of national R&D projects, information sharing on national R&D projects is very essential. The blockchain technology is considered as a core solution to share information reliably and prevent forgery in various fields. For efficient management of national R&D projects, we enhance and analyse the Perfect Sharing Project (PSP)-Platform based on a new blockchain-based platform for information sharing and forgery prevention. It is a shared platform for national ICT R&D projects management with excellent performance in preventing counterfeiting. As a consensus algorithm is very important to prevent forgery in blockchain, we survey not only architectural aspects and examples of the platform but also the consensus algorithms. Considering characteristics of the PSP-Platform, we adopt an atomic proof (POA) consensus algorithm as a new consensus algorithm in this paper. To prove the validity of the POA consensus algorithm, we have conducted experiments. The experiment results show the outstanding performance of the POA consensus algorithm used in the PSP-Platform in terms of block generation delay and block propagation time.
Keywords: distributed system; Perfect Sharing Project (PSP)-Platform; information sharing; consensus algorithm

1 INTRODUCTION

Korea invests a budget of more than 10 billion USD every year to the national research and development (R&D) projects. This is not only securing the innovations of information and communication technology (ICT), but also making continuous investment in order to prevail the superiority of technology in the global market [1],[2]. Thanks to continuous advances of ICT and industrial development, Korea's ICT industries have received worldwide attention [3-10]. Although the ICT R&D projects in Korea are carried out by various organizations and a lot of researchers, it is difficult to efficiently and effectively share information related to the research projects in the overall life cycle of planning, evaluation, task management and performance management [11-13]. To manage the whole cycle of national R&D projects, this paper aims to develop an innovative technical solution for reliably sharing information on national R&D projects.

Information sharing is a multi-disciplinary process which combines information from different sources (e.g., devices, data bases, etc.) while identifying and applying the business intelligence related rules. The communication and metadata standards enable the effective use of information owned by different stakeholders and stored and processed by using different technologies. To address concerns about trust and security, the mass sharing of information, peer-to-peer (P2P) and other distributed systems are considered to grant control over information access and sharing to participating stakeholders [14]. The decentralized information sharing model enables to create new mechanisms for secure information exchange between counterparties without requiring any single third party to handle the information. For this reason, the blockchain technology with a distributed ledger architecture is typically refereed as a good example for information sharing by facilitating reliable data transactions [15].

The blockchain is widely acknowledged as a potential solution for enhancing current centralization, privacy and security problems when storing, tracking, monitoring, managing and sharing data [16-19]. The blockchain usually consists of one or multiple distributed ledgers which contains all transactions ever executed within their networks, enforced with cryptography, and carried out collectively by P2P workgroups. The blockchain is a trust-free, tamper-proof, auditable and self-regulating system, with no human intervention required to execute computations [20-22]. Once the data or transaction is recorded in the blockchain, it cannot allow to be detected and rejected by the other nodes in the network. In addition, with using timestamp, the data in blockchain is traceable. Specifically, consensus in blockchain would help to identify illegal nodes and prevent malicious access, thus it is good to support device security and further to improve data security [23].

In this paper, we aim to develop a blockchain-based national ICT R&D projects information sharing platform. The purpose of this platform is to utilize the blockchain technology for information sharing on national R&D projects based on characteristics of data openness, security, stability and efficiency. In this paper, we enhance and analyse the platform called Perfect Sharing Project (PSP) Platform. To support the complete sharing of national R&D projects information, we emphasise a consensus algorithm as an important element of the blockchain technology for the PSP-Platform. The adopted consensus algorithm is called the atomicity proof (POA) method which uses a new concept for consensus. The POA algorithm should be able to store the same information in each node, considering that it is a distributed system. However, some nodes may not replicate blocks identically, or have defects in replicating unnecessary blocks. To solve this problem, in the POA algorithm, it is possible to generate blocks only for all participants in favour of block generation. To prove the validity of the POA consensus algorithm, we have conducted experiments. The experiment results show the outstanding performance of the POA consensus algorithm used in the PSP-Platform in terms of block generation delay and block propagation time.

The rest of the paper is organized as follow. In Section 2, we briefly introduce the recent research trends on blockchain and consensus algorithms. Section 3 introduces the features of our PSP-Platform. We also introduce our POA algorithm and compare it with the existing algorithms. In Section 4, we show the performance analysis results of the POA consensus algorithm. In Section 5, we conclude the experiment with an assessment of the performance of the POA consensus algorithm through a

simulator based on NS3. Then, we present the direction of future research.

2 RELATED WORK

2.1 Blockchain making data trusted to support data exchange and sharing

In the project information sharing scenarios, it is very important to build a trusted framework to ensure data processing, circulation, sharing and management to be all reliable operations. And project participants require the exchange of credit relations. Trust and credit are the basis of the project information sharing platform.

The blockchain technologies are arising, which have the specific characteristics as follows: trust, transparency, highly resistant to outage, tamper-proof, auditable, and self-regulating system. The blockchain can efficiently ensure integrity, authenticity, and auditability of all transactions. It could hence help to make data trusted to support data exchange and sharing as follows:

Realise trusted transactions between the parties. Blockchain could make distrusted parties to realise trusted transactions, and finally to reach trust relationships between the parties. So as long as a trust relationship is required, the blockchain can be used. Being trusted is the most important characteristic for the blockchain when it is applied in various application scenarios.

Data's terminal device became trusted. Consensus in blockchain would help to identify illegal nodes and prevent malicious access, it helps to guarantees data's terminal device trusted.

Data becomes trusted and verifiable. Data can be traced back to the origination based on blockchain.

Trusted data storage. Blockchain itself is an untampered database storage technology. The data can be recorded directly on blockchain, or be encrypted by blockchain technology before storing in distributed databases [23].

2.2 Blockchain Platform

There are several types of representative blockchains (e.g., Bitcoin, Ethereum and Hyperledger, etc.) which have features to process and manage data [24-25]. This section provides a reference model of blockchain with core functionalities to illustrate the common features of the blockchains as a result of ITU-T Focus Group on Data Processing and Management (FG-DPM) standardization activities [26].

Without loss of generality, a blockchain commonly consists of a group of logical functional components which can be divided into five layers (see Figure 1); i.e., fundamental layer, core layer, service supporting layer, application layer and cross layer.

Fundamental layer. It provides the running environment and basic components for normal operation of the blockchain as follows:

- P2P communication: It supports the blockchain peers to interact with each other and to exchange blockchain data with P2P communication technologies. The underlying communication networks are transparent to blockchain.
- Storage: It supports the blockchain peers to store and query blockchain data in an effective, secure and steady way.
- Computation: It provides the running environment and computing capabilities including container, virtual machine and cloud technologies which can be applied by each blockchain peer.

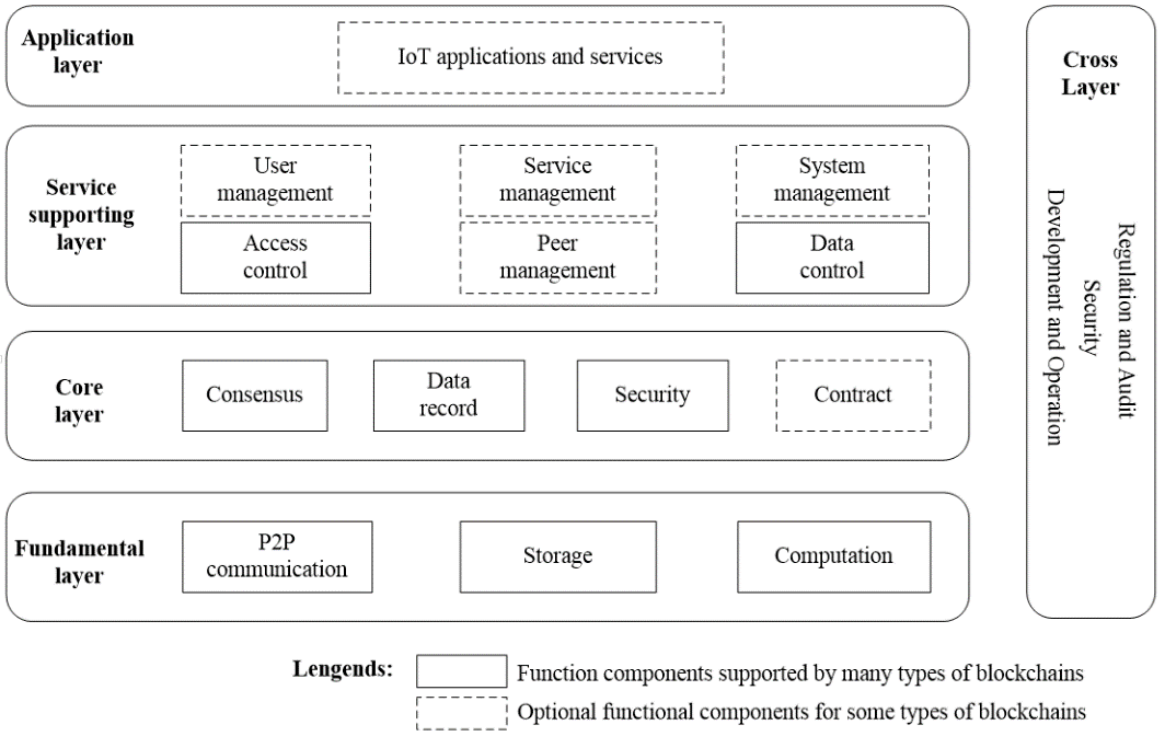

Figure 1 A common reference model of blockchain (ITU-T FG-DPM)

In fundamental layer, physical or virtual security infrastructures support to store, manage and control the access to participants' sensitive data, including the participants' private keys.

Core layer. It provides core capabilities based on the environment and capabilities provided by fundamental layer. The core capabilities for blockchain operations include consensus making, data recording, security protection and contract management [27-29]. The functional components in this layer include:

- Consensus: It supports the blockchain peers to make consensus with algorithms for achieving agreement.
- Data record: It provides distributed storage for saving blockchain data.
- Security: It supports security in blockchain operations like reliable transactions and data protection with mathematical tools and processes (e.g., encryption and decryption, digest and digital signature etc.).
- Contract: It supports the operations related to smart contract, such as deploying, executing and searching the smart contract [30].

Service supporting layer. It provides reliable and efficient access and monitoring of blockchain as well as unified access control, data control and managements for peers, users, services and systems in blockchain. The functional components in this layer include:

- Access control: It performs the access controlling to the blockchain data about the user accounts, ledgers, transactions and interfaces.
- Peer management: It supports the blockchain peer for information query and management, including peer configuration, monitoring and authorization.
- Data control: It supports the data residing in the blockchain peer distribution and exchange.
- User management: It supports user managements and transaction committing.
- Service management: It supports service selection and subscription, and cross chain linkage and data exchange.
- System management: It supports the managements for monitoring events and security.

Application layer. This layer includes blockchain applications which utilize the functionalities provided in the lower layers (i.e., fundamental, core and service supporting layers) and cross layer [31].

Cross layer. This layer is a vertical layer, which provides commons supporting functions across the multiple layers. Functional components in this layer include developing and operation, security, regulation and audit, etc. [32].

To investigate the state of the art on related platforms, we analyze the trends of blockchain platforms for information sharing, for applying to the management of national R&D projects. Representative examples are the blockchain platforms for carbon emission history management by the Ministry of Environment, national record document management by the National Archives of Korea, and waste battery history management by Jeju City [20-21]. The blockchain-based carbon credit history management system of the Ministry of Environment, led by the government, was developed to share information on carbon emissions. The platform is based on Hyperledger Fabric [24], and the platform was developed for the purpose of managing carbon emission certification performance and electronic document history management. Its main function is to approve external operators, to reduce certification, to transfer reductions, to offset offsets, and to share information using blockchain technology. The National Archives' trust-based records management platform was also developed for the management and sharing of electronic documents by constructing the platform based on Hyperledger Fabric. In particular, this platform is capable of real-time online verification of the originality of national records. This platform has the advantage of sharing information from the time when electronic documents are generated. The waste battery distribution history management system of Jeju City has adopted a blockchain technology-based platform as a waste battery distribution history management system to reuse the batteries discharged from electric vehicle junk cars. It's a platform based on Hyperledger Fabric to prevent history information sharing and forgery of transactions. A blockchain platform is a technology that can share information and prevent forgery of transactions. As mentioned earlier, an optimal consensus algorithm, platform design and optimal service linking are the main issues. We intend to develop an optimal platform for the lifecycle management of national ICT R&D projects information in this paper.

2.3 Consensus Algorithm

The blockchain technology records and manages data by distributing transaction and management authorities over P2P networks. The blockchain technology creates a block that records all transaction information generated during a specific period and sends it to all members. Once the block is verified by the member, a chain among blocks is formed by connecting to the existing blockchain. In this process, all nodes have the same distributed ledger that records the transaction information and the blockchain updates identically by participant consensus. All participants in the agreement must determine the suitability of the data and consensus [33-40].

This process uses a consensus algorithm to share and manage the distributed ledgers of each node. A representative consensus algorithm is POW (Proof of Work) [41]. Recently, other consensus algorithms, POS (Proof of Stake) [42] and DPOS (Delegated Proof of Stake) [43], which have solved the shortcomings of POW, are used as representative consensus algorithms. As a consensus algorithm is one of the very important elements of the blockchain technology, we summarize various consensus algorithms here.

POW (Proof of Work). The proof of work (POW) method introduced in the paper of Satoshi Nakamoto [41] has been widely used in an open blockchain, such as Bitcoin [14]. To create a block, the miner must verify that the work to find a specific value (Nonce) is performed by executing an operation to find a hash value. The nodes of the network select either A or B to create a next block. In Bitcoin, the hash value of a block (B) defined as follows.

$$\text{Hash}(B) \leq M/D \quad (1)$$

In Equation (1), D is difficulty and belongs to the range of [1, M]. M is the maximum value (2^{256}-1) of D, and is

obtained by miners repeatedly solving the hash value of block B that meets the condition. The miner that successfully solves the hash value informs the entire blockchain nodes of the value and completes the blockchain by connecting its block to the last block of the blockchain. In other words, forgery prevention is possible because the above process must be performed once more in order to attempt forgery.

POS (Proof of Stake). POS is a consensus algorithm to supplement the shortcomings of POW. The POW method may cause monopoly-related problems, such as information monopoly and transaction omissions, by a miner or a group that has a monopoly of more than 50%. As an alternative to the POW method, the POS method, in which the stake of a participant affects block creation, was proposed. In other words, owing to POS, blocks created according to the proportion of the stake are held by a miner. The hash function defined as follows [42].

$$\text{Hash}(\text{hash}(\text{Bprev}),A,t) \leq \text{bal}(A)M/D \quad (2)$$

In Equation (2), Bprev is the previous block, A is the Address, t is Timestamp, and bal(A) is the currently owned stake. D is difficulty and M is the maximum value of D. The hash value of block B is affected by the stake owned by A and difficulty. Therefore, an owner of a large stake can solve problems easily. The POS method can shorten the block creation cycle. However, as block creation is much easier as the stake amount increases, a fairness problem occurs when initial stakes are allocated. As the fairness problem in a consensus algorithm is a very important engineering point of blockchain technology, it is being researched with various methods other than those mentioned in this paper.

DPOS (Delegated Proof of Stake). The DPOS (Delegated Proof of Stake) method delegates authority to create and prove a block only to a certain number of people in order to compensate the unfair distribution method of the share, which is a disadvantage of the POS method [42]. In the case of the POS system, it takes a lot of time because all the nodes having a certain stake are given the block generation and proof authority.

However, for the DPOS method, the result of the vote determines the nodes that generate and prove the blocks, thus reducing the time and cost of the agreement due to relatively few nodes. Instead of creating blocks themselves, the nodes voted can delegate their shares to the elected representatives, and the nodes delegated can create/prove blocks instead of the nodes elected. The number of block generators and the number of verifiers in the DPOS algorithm may vary depending on the rules of agreement in the corresponding chain.

For example, when there are N block generators, the DPOS blockchain proceeds in the following order

- N block producers are selected from the block producer candidates and the representative node selected should satisfy the following equation. In Equation (3), *n(Voter A)* denotes the number of users who elected the node *A* as a representative, and *n(Voterall)* denotes the number of users who participated in the voting.

$$n(VoterA) > \frac{n(Voterall)}{2} \quad (3)$$

- If a block generation/verification representative votes more than (2/3+1) for the block producer, the block is established and created until the first block is signed (*I=N*).

If an elected representative maliciously creates a block, the next voter will not vote for that block creator, so it is natural to exclude it from the block creator. Since the number of block producers is limited, DPOS has the advantage of handling transactions larger than POW and POS. However, since only the representative node participates in the block generation, it is controversial whether it is a truly decentralized system. Even if the number of blocks is small, it selected as a representative node, and there is a weak point in security.

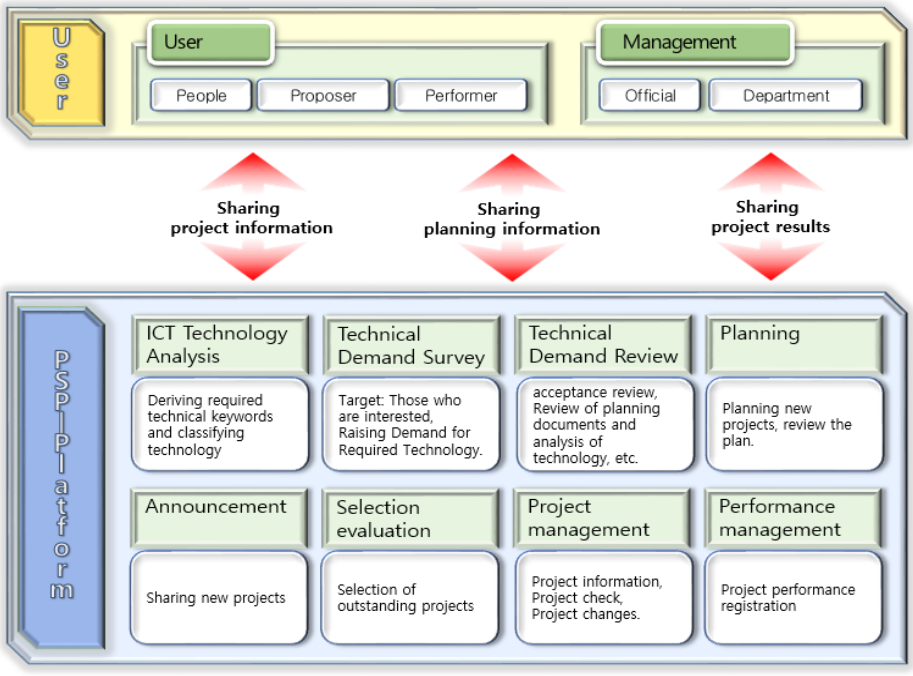

Figure 2 PSP-Platform

3. PSP (Perfect Sharing Project) PLATFORM

The integration of the planning, evaluation, and management processes of national R&D projects, which are operated differently by departments and agencies, is necessary. In Korea, 20 ministries operate the entire lifecycle of national R&D projects as a system, and each department manages national R&D projects with a different system.

3.1 PSP Platform

In order to facilitate the secure sharing of project information associated to the overall management process of the national ICT R&D projects, namely planning, evaluation, task management and performance management, we enhance and analyse the Perfect Sharing Project (PSP)-Platform [43],[44] based on a blockchain-based platform as shown in Figure 2.

The PSP-Platform is a platform for managing national ICT R&D projects. In other words, it is proposed to support sharing of project information on planning - evaluation - project task and performance management - research achievement management. Generally, the blockchain technology is a technology that can prevent transaction forgery in principle. It also provides a process for block generation and verification for information related to national ICT R&D projects. However, in the phase of providing project related information, each user needs to be authorized in order to restrict the right of access to the information. The user gets the desired information according to the given authority. As shown in Figure 3, users can get task information through the PSP-Platform.

Stakeholders are divided into two categories: user and manager. Users are further classified into three categories: general user, project proposer and project performer. General users can easily read a summary of each project in the PSP-Platform. The project proposer can read and review most of the project information. If the proposer doubts the duplication of information on the project and the research results, the proposer can suggest the block generation. The proposer can then propose new projects for future R&D based on the project information of the PSP-Platform Since the proposer can confirm the project information that performed in the past it is possible to prevent the problem of suggesting the duplicated projects. The performer can read and write project information but can only read about almost all project information. The performer can create a block. The performer is responsible for the project. We can share information about national R&D projects with users through a blockchain based PSP-Platform. The manager registers project information in the PSP-Platform to share project progress information.

Figure 3 shows how the user can access the PSP-Platform and use the project results and project information [43]. Users should access the PSP-platform to search for information on national R & D projects. The user logs in to the platform first, and the administrator generates the user's unique key and sends it to the user. With this unique key, user can search for project information on the PSP-platform. That is, Step 1 shows the account creation process. In Step 2, the user can view information. The user can access information using the received unique key. That is, the unique key can be said to be an electronic signature for identification. Digital signatures are also used to propose the creation of ledgers and to verify ledgers. In Step 3, the user wants to create a ledger to raise the redundancy of the project. The user first creates a ledger that raises redundancy. And then the user transmits it to a neighbor node and transmits it to all nodes. The ledger sent to all nodes changes the state to the previous stage for verification by the node that received the ledger first. In the pre-validation step, all nodes verify whether the ledger is a

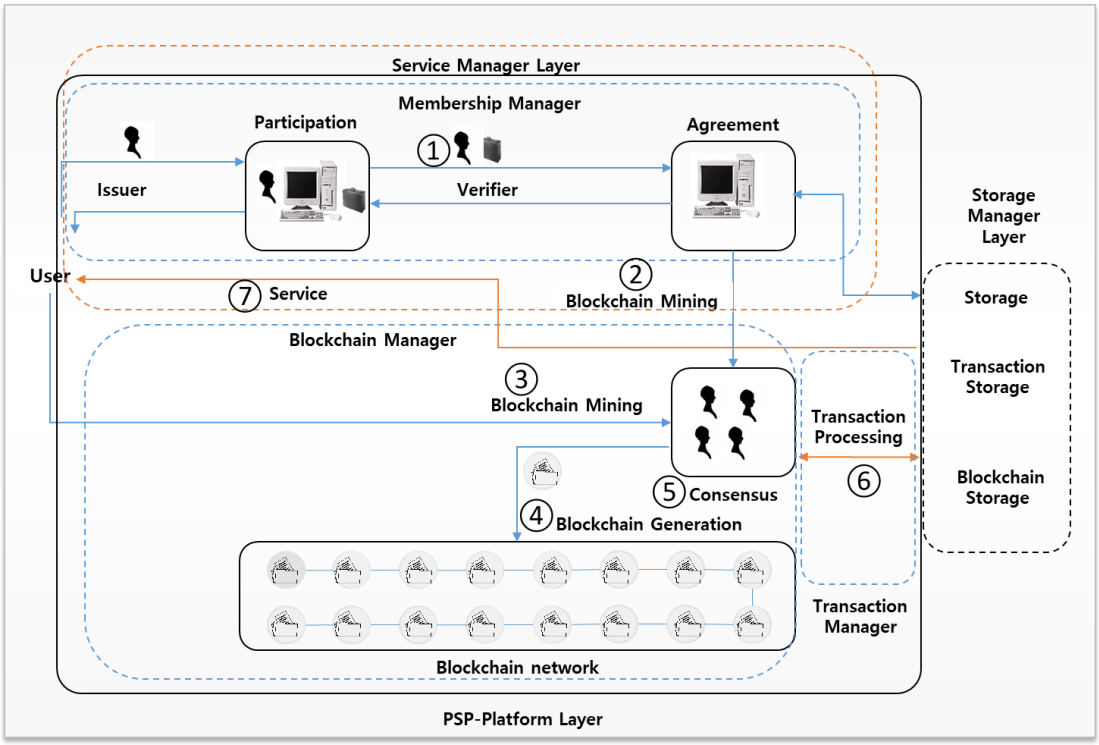

Figure 3 PSP-Platform Process

verifiable ledger and then perform verification. If the structure of the ledger is incorrect, the ledger is deleted before the verification. The verification of the ledger is made by considering the following three values:

- Check the ledger's syntax and data structure
- Check whether the size of the ledger is appropriate
- Check if the input value of the ledger is smaller than the output value

In Step 4, ledgers verified in the verification step are all sent to the manager on the platform. At this time, the ledger is composed of blocks and sent to all managers. The block is composed of a header and a body, and the block size is 1Mbyte to 9Mbyte. The hash function is used to store and manage the ledger of R&D projects.

In Step 5, among the N administrators in the online nodes, the first administrator who receives the ledger is assigned a role as a coordinator. In order to verify the ledger, the arbitrator sends Proofs to the N-1s for verification. When the Proof sent by the arbitrator is approved by all managers, it is considered that an agreement has been reached, and this ledger is stored in the blockchain as valid project information. If the Proof sent by the moderator is not approved by even one manager, the agreement has not been reached by all managers, so this ledger is deleted because it has no value as project information. Participant agreement procedure is as follows:

o Proof request

o Request for agreement

- All managers agree
- Proof verification
- Occurs when all managers do not agree

In Step 6, the verified block is now a new block that connects to the existing blockchain. Simultaneously with the creation of the blockchain, it is stored in the PSP-Platform as new project information and provides information to users.

In Step 7, R&D projects information stored in the blockchain is shared with users and used for planning, evaluation, management, and post-management of national R&D projects.

In the PSP-Platform, it needs to rely on a trusted third party to share trusted data information which impacts the cooperation between parties. However, at times there is no trusted third party, or the cost of trusted third-party entities are too high, or the effect of utilizing trusted third-party entities is not ideal. In this situation, the blockchain would offer a potentially viable and optimized solution and it would help to optimize procedures, improve efficiency and reduce cost, etc.

The roles of blockchain in data exchange and sharing in PSP-Platform are as following:

- Blockchain is used in data exchange and sharing for achieving data asset transaction as well as safeguarding related rights and interests of data owners.
- Blockchain is used for sharing the trusted information in projects. It is helpful to optimize procedures, improve efficiency or reduce cost specially when there is no trusted third party, or when the cost of trusted third-party entities is too high or the effect is not ideal [23].

3.2 POA (Proof of Atomicity) Algorithm

The problem of sharing arises from the planning stage of national R&D projects. In order to connect the ledgers generated at the planning stage with blockchain, it is necessary to go through the process from ledger generation to verification by a consensus algorithm.

One of the factors affecting the performance of blockchain systems is a consensual mechanism. A consensus algorithm creates new nodes and many nodes can have the same information. However, if many nodes participate in the agreement to give the agreement fairness, there can be a lot of energy consumption in terms of performance.

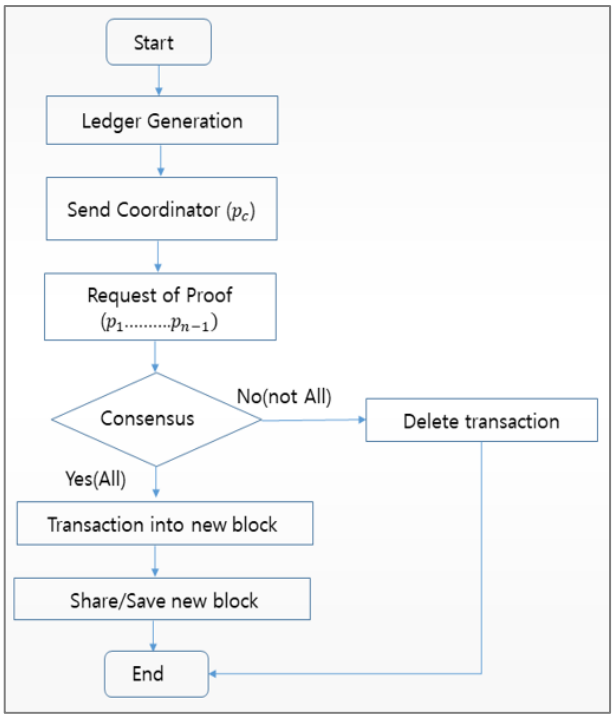

Figure 4 POA (Proof of Atomicity) Algorithm Process

In recent years, a variety of consensus algorithms such as POS and DPOS have been developed to supplement this aspect. However, there is no perfect algorithm yet, and as described above, it is necessary to complement each of the disadvantages. In this paper, we adopt the POA algorithm to overcome the problem of excessive energy use without damaging the fairness problem.

The POW algorithm proposed by Satoshi Nakamoto can generate a block if 51% of the block verifiers agree when trying to create a new block [44]. However, in the process of planning, evaluating and managing the national R&D project, only 51% of the participants agree to change the project information, which could cause serious damage due to wrong information sharing.

A public blockchain method is a good way to decentralize in terms of sharing information to everyone. However, in terms of generating and sharing reliable information, it is necessary to supplement the public blockchain and the private blockchain. Therefore, we adopt and enhance the POA (Proof of atomicity) algorithm [44]. The POA algorithm's process is illustrated in Figure 4. The POA algorithm can create blocks only with 100% consent

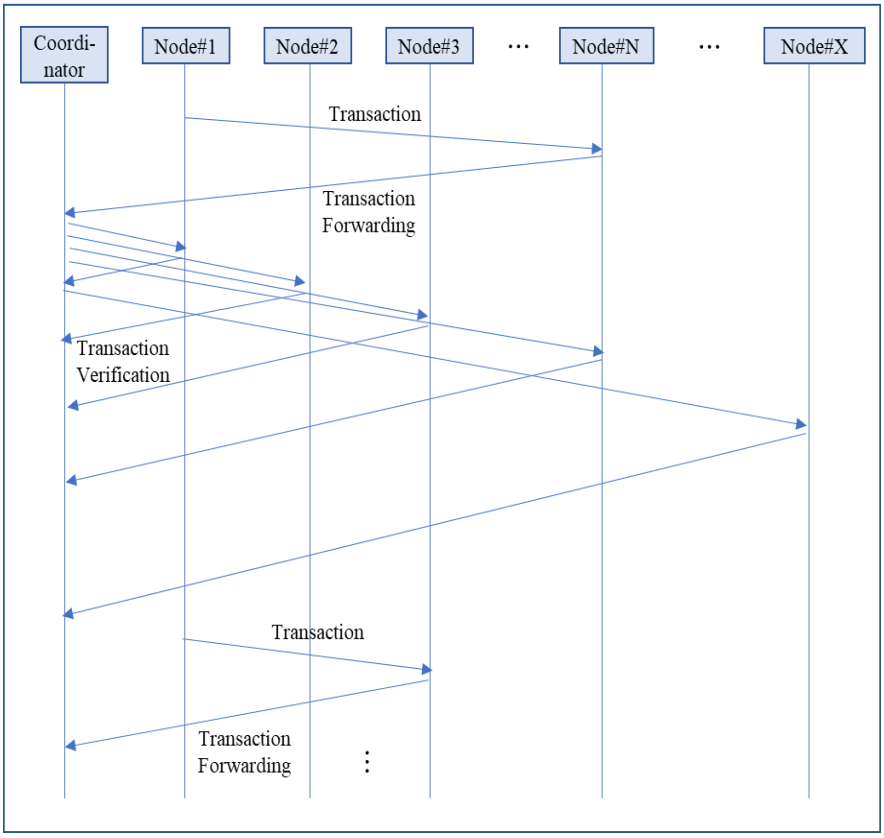

Figure 5 NS3-based POA simulation operation procedure

from managers who can create them. The generated blocks can provide the same information for all participants. For example, if project information is changed or generated by malicious intent, problems arise from the planning stage of the national R&D project to the duplicated project planning. In order to prevent this problem from occurring in advance, the participant who generates the block must 100% agree and generate reliable information. And the POA algorithm features atomicity and consistency. The atomicity and consistency of the POA algorithm can increase reliability.

- Atomicity: A block created only when 100% of the participants agree. However, if the agreement is not realized in the interim, the block will be deleted.

- Consistency: If the agreement is successful, the transaction information will be updated. This information provides the same information on any node.

4. EXPERIMENT

4.1. Experimental Environment

Performance analysis of the actual POA algorithm requires a large testbed configuration that operates a blockchain system based on hundreds of POA consensus algorithms. However, in reality, there are many limitations in testbed construction, so performance analysis is conducted through simulations that mimic the behaviour and characteristics of POA-based blockchain networks as closely as possible. NS (Network Simulator)-3 is a discrete-event network simulator developed at the University of California, Berkeley, for the purpose of performance analysis of packet-based network protocols and application services [46]. Since it is publicly available under the GNU GPLv2 license, its function and operation have been verified and it has the advantage of being scalable. In this paper, we implement and operate the consensus algorithm of the POA based on NS-3 simulator, which is most widely used in the network field.

The simulation parameters are set as shown in Table 1 to analyse the performance of the POA algorithm, considering the operation and consensus parameters of the POA algorithm, and network characteristics. In addition, performance analysis of the characteristics of the POA blockchain network (e.g., the number of POA blockchain nodes, the connection method and distribution between the nodes, and the block size) is performed.

Table 1 Blockchain Simulation Parameters

Simulation Parameters	Simulation Settings
Number of nodes	100~900
Packet size	1024 bytes
Block size	1MBytes~ 9MBytes
Communication pairs selection	Random selection with uniform probability
Traffic flow pattern	Exponential random distribution
Consensus Algorithm	POA

In detail, based on NS-3.29, GCC 4.9, and Python 2.7 on Ubuntu Linux 18.04, POA consensus algorithm models were designed using C ++ and Python languages.

- POA-configuration.cc : Configure the core switch, edge switches and host nodes and moderator nodes. Connect nodes to create topology and run the POA algorithm.
- Udp-fw-server.cc : In the transaction between nodes, the receiving node delivers the message received from the sending node to the coordinator.
- Udp-bc-server.cc : Implement a coordinator function that verifies messages received from recipients participating in a transaction through all participants and stores them in blocks.
- Udp-l4-protocol.cc : Extension of the existing code to trace and record traces of messages exchanged between POA related nodes.
- Onoff-application.cc : Depending on the model of exponential distribution, the existing code is extended and developed to include the functions of generating transaction messages to any other nodes as well as recording and managing traces thereof.
- Wscript: Register the implemented functions so that the POA implementation can operate in the existing NS-3 package.

4.2. Experimental Process

In Figure 5, transaction occurs after two nodes are randomly selected in POA topology. Traffic between two nodes follows exponential On-Off distribution. The node receiving the transaction forwards it to the coordinator. In this paper, it is assumed that the coordinator has a built-in Miner function. The coordinator propagates the transaction details from all nodes belonging to the POA and receives the response and records the corresponding transaction in the block. The coordinator connects the generated blocks to the chain when it reaches a fixed block size.

Next, we test the confirmation delay to generate blocks according to the node's response delay in the POA agreement process. The coordinator who receives the transaction message delivers the message to all participating nodes. If the node is processing other work, the response may be delayed. The performance result on the block confirmation delay time according to the response delay of the nodes is shown in Figure 6. However, it is assumed that all nodes participate in the response.

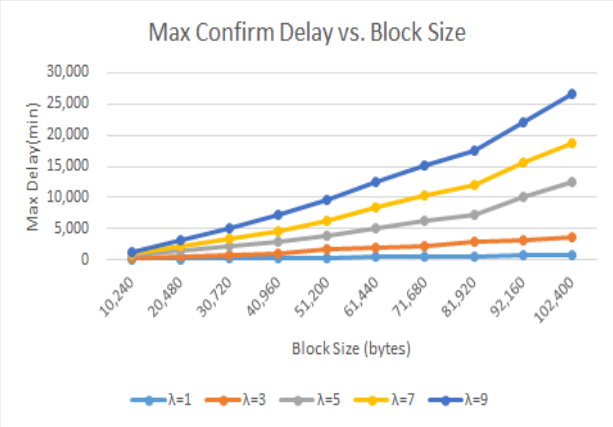

Figure 6 Block confirmation delay according to node's response delay

The time taken for the consensus process between the coordinator node and each participating node is the network propagation delay and the processing time at each node. In this performance analysis, the propagation delay is fixed and the processing delay at each node changes according to the exponential distribution. When consensus is requested for all participating nodes for each transaction, the consensus time is determined according to the node with the longest response delay, and the block confirmation time is also accumulated according to the block size. Figure 6 shows the maximum delay versus block size when the average response delay (λ) in exponential distribution increases to 1, 3, 5, 7, 9 minutes. This performance analysis shows that when the response delay of nodes is too long, it is desirable to limit the maximum response delay time because the entire block confirmation is delayed waiting for a response.

The coordinator delivers a request message for consensus to all nodes participating in the POA but may not receive a response due to node and network errors or intentional denial of participation by the nodes. According to the POA algorithm, if a response is not received from the all current active nodes, the consensus fails, and the message cannot be recorded in the ledger.

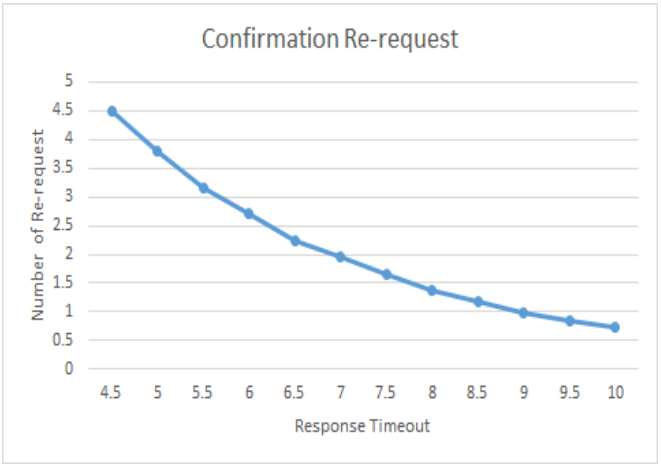

Figure 7 Reconsensus request due to node not responding

The coordinator sends a consensus re-request message to the node that has not responded for a specified time and waits for a response. The performance result according to the number of re-requests is shown in Figure 7. Figure 7 shows the number of re-requests when the average response delay (λ) is set to 3 minutes and the maximum response wait time is set to 4.5 to 10 minutes.

The response or non-response of each node was determined based on whether the response delay time according to exponential distribution exceeds the time limit.

Figure 8 shows the result of average block propagation time with increasing block generation time. Assuming that the number of nodes is 500 and the block size is 1 MBytes, as the time for generating blocks is increased by one minute, it can be seen that the block propagation time is generally low. If the block generation time is short, it takes more time to generate more blocks and propagate them between nodes, while longer block generation time reduces

the average block propagation time because the number of generated blocks is reduced.

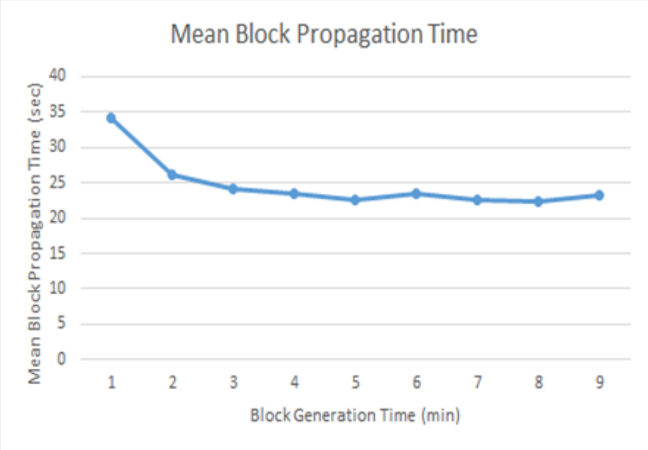

Figure 8 Average block propagation time with increasing block generation time

5. Conclusions

We have enhanced and analysed the PSP-Platform to block unintended sharing of project outcomes in planning, evaluation, task management and performance management as well as to prevent forgery of task information based on the blockchain technology. The PSP-Platform is a platform that shares information over the entire life cycle of the national ICT R&D projects. In particular, it is a platform that adopts the consensus algorithm to solve critical issues occurred in the blockchain operation. The atomic proof (POA) method is a consensus algorithm that complements the existing consensus algorithms and reflects the characteristics of national R&D project management. Especially, a ledger is the most prominent feature to prevent the forgery of national R&D project information. We created a hypothetical scenario for the verification of PSP-Platform and conducted the experiments applied the POA algorithm. In the future, through continuous research on PSP-Platform, we will continue the research to build up an advanced project information sharing platform by improving the performance of the project management platform in terms of efficiency.

Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2020-0-00833, A study on 5G based Intelligent IoT Trust Enabler)

6. REFERENCES

[1] Eunhee Lee, Youngik Yoon, “Project Management Model based on consistency strategy for Blockchain Platform,” SERA 2019.

[2] Karen Fawcett, Jeff Tessler, Claudio Scardovi, Oliver Frischemeier and William Park, “Future of Financial Services in 2030,” Impact of Digitization. 2016.

[3] “2015 National Research and Development Performance Evaluation Plan,” National Science and Technology Review Board, 2014. 4.

[4] “2016 National Research and Development Performance Evaluation Plan,” National Science and Technology Review Board, 2015. 4.

[5] “National Research and Development Standard Guidelines for project Evaluation,” National Science and Technology Review Board, 2015. 3.

[6] “Standard menu for research and management of national R&D projects,” Future Creation Science Department, 2014. 11.

[7] “A Study on the Improvement of R&D Performance in Korea,” Future Creation Science Department, 2013. 8

[8] “Analysis of National R&D Project Survey Results for 2017,” National Science and Technology Advisory Council, 2018

[9] “Implications for IT R&D Policy Evaluation in European FP Assessment, IT R&D Policy Trends (2012- 3),” Information and Communication Industry Promotion Agency, 2012.3

[10] “The Analysis of evaluation systems of the programs by its types and policy recommendations,” Future Creation Science Department, 2013. 8.

[11] Cho Hyun, Yoon Moon-seop, Min Cheol-gu, Ahn Doo-hyun, Seong Tae-kyung, Choi Tae-jin, and Jung Yoon-sung, “Improving the performance evaluation system of fundamental research programs of the Korean government,” Policy Research 2014–02,2014.

[12] Hwang Joon Young, “Improvement of National R&D Project Evaluation”, Korea Science Foundation, 2019. 6.

[13] “3rd Framework Plan for National R&D Performance Evaluation(2016-2020),” National Science and Technology Review Board, 2015. 4.

[14] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] “Distributed ledger,” https://en.wikipedia.org/wiki/ Distributed_ledger

[16] Don Tapscott and Alex Tapscott, “Blockchain Revolution,” Eulyoo Publishing Co., LTD., 2017.

[17] DLP Piper, “The Blockchain Revolution,” Stanford University, 2017.1.

[18] Melanie Swan “Blockchain”, p27-31, 2015

[19] Byeowool kim, Youngik Yoon, “Journalism Model Based on Blockchain with sharing space” Symmetry 11, no 1:19

[20] Hyeon Kwak, “Industrial Trend and Patent Trend of Blockchain Technology,” Korea Knowledge Industry Institute, 2017

[21] Je-young Lee, “Blockchain Technology Trend and Implications,” Science and Technology Policy Institute, 2017

[22] Global Blockchain Technology Market 2017-2021, Technavio, 2017

[23] “Blockchain-based data exchange and sharing for supporting IoT and SC&C”, Technical Specification D3.6, ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities, 2019,

[24] Hyperledger, “Hyperledger,” https://www.hyperledger.org/

[25] Bitcoinwiki, “Block Hasing Algorithm,” https://en.bitcoin.it/ wiki/

[26] “Overview of blockchain for supporting IoT and SC&C in DPM aspects,” Technical Specification D3.5, ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities, 2019,

[27] Y. Sompolinsky and A. Zohar, “Accelerating bitcoin’s transaction processing. fast money grows on trees, not chains,” IACR Cryptology ePrint Archive, vol. 2013, no. 881, 2013.

[28] “The biggest mining pools.” [Online]. Available: https://bitcoinworldwide.com/mining/pools/

[29] K. Nayak, S. Kumar, A. Miller, and E. Shi, “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack,” in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, pp. 305–320, 2016.

[30] N. Szabo, “The idea of smart contracts,” 1997

[31] Choi Jong-seok, Park Jong-kyu, Kim Young-gil, Kim Ho-won, “A Study on the Conformity of the Application of the Blockchain Agreement Algorithm,” Journal of information science, pp 9-16, .2018.

[32] Proceedings of International Conference on Financial Cryptography and data Security, Berlin, Heidelberg, pp. 486–504, 2014.

[33] A. Chepurnoy, M. Larangeira, and A. Ojiganov, “A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability,” arXiv preprint arXiv:1603.07926, 2016.

[34] Jong-cheol Lim, Hyeon-gyeong Yoo, Ji-young Kwak, and Seon-mi Kim, “Blockchain and Consensus Algorithm,” ETRI, 2018.

[35] D. Ongaro and J.K Ousterhout, “In Search of an Understandable Consensus Algorithm,” USENX Annu. Technical Conf, Philadephia PA, pp305-319 USA June 2014,

[36] D. Mazieres, “The stellar consensus protocol: A federated model for internet-level consensus,” Stellar Development Foundation, 2015.

[37] C. Decker, J. Seidel, and R. Wattenhofer, “Bitcoin meets strong consistency,” in Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). Singapore, Singapore: ACM, 2016, p. 13.

[38] D. Kraft, “Difficulty control for blockchain-based consensus systems,” Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[39] CASTRO Miguel, et al, “Practical Byzantine Fault Tolerance,” in OSDI, 1999, p173-186.

[40] Tendermint Wiki, “Byzantine Consensus Algorithm”, Accessed 2017. http://github.com/tendermint/tendernimt/wiki/Byzantine-Consensus-Algorithm

[41] Jakobsson, Markus, and Ari Juels, “Proofs of work and bread pudding protocols.” in Secure Information Network, pp 258-282, 1999

[42] “Proof of stake versus Proof of work,” Bitfury Group Whitepaper, 2015.

[43] Eunhee Lee, Youngik Yoon, “Trusted information project platform based on blockchain for sharing strategy”, Journal of Ambient Intelligence and Humanized Computing 2019

[44] Eunhee Lee, Youngik Yoon, “A Study on the PSP-Platform fot the Atomicity of Distributed Ledger”, Journal of The Korea Society of Computer and Information, Vol. 24 No 5, pp 73-80, 2019

[45] Daniel Larimer, “Delegated Proof-of-Stake (DPoS)”, Bitshare whitepaper, 2014.

[46] Network Simulator ns3, https://www.nsnam.org/

Contact Information:

Eunhee Lee
Department of IT Engineering, Sookmyung Women’s University
Seoul 04310, Korea
eunhee@iitp.kr

Yongik Yoon
Department of IT Engineering, Sookmyung Women’s University
Seoul 04310, Korea
yiyoon@sm.ac.kr

Gyu Myoung Lee
Department of Computer Science, Liverpool John Moores University
Liverpool L3 3AF, UK
g.m.lee@ljmu.ac.uk

Tai-Won Um
(Corresponding author)
Department of Cyber Security, Duksung Women’s University, Seoul 01369, Korea
twum@duksung.ac.kr