Journal of Theoretical and Applied Information Technology
31st August 2022. Vol.100. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# FEDERATED LEARNING DISTRIBUTED CONSENSUS ALGORITHM FOR TELEMEDICINE

**YOUNGBOK CHO**[1]

[1]Deajeon University, Affiliation, Department of Information Security, Korea

E-mail: ybcho@dju.ac.kr

**ABSTRACT**

Recently, as the importance of telemedicine increases due to the COVID-19 pandemic, interest in the safe use of medical data is increasing. The need for safe and effective management of personal information is emerging as the number of hacking cases related to personal information is increasing due to the activation of big data utilization and the activation of telemedicine due to the 4th industrial revolution. In addition, since personal information used in the medical field is classified as sensitive information, it is necessary to focus more on security. However, in order to access one's own medical information in telemedicine and big data environments, it must be provided anytime, anywhere. In Korea, medical information is currently managed in the form of centralization where local hospitals store and manage each patient's data. Therefore, the problem of centralized data management was solved by applying block-chain technology. It provides more free information exchange in cooperative telemedicine and ensures the privacy of patient information while safely reaching mutual agreements

**Keywords:** *Telemedicine, Federated Learning, Distributed Consensus Algorithm, Privacy, Black-chain*

## 1. INTRODUCTION

With the development of IT technology in the era of the 4th industrial revolution, it is a technology that aims to transmit and receive data safely using block-chain technology in various fields such as 5G, SDN, and IoT. The high-speed connection-based intelligent revolution triggered by digital technologies such as artificial intelligence and augmented reality is fundamentally changing our society with the hyper-connection and hyper-share that are being created based on software technology. Block-chain technology was first introduced in 2008 by Satoshi Nakamoto based on cryptocurrency [1-3]. It was proposed as a method to solve the security vulnerabilities of the existing server-client centralized network structure. In a block-chain, all nodes connected in a distributed network are connected, and transaction details are agreed upon and shared through competition. This characteristic of block-chain technology enables accurate management of transaction details. Consensus algorithm is the basis of decentralized trust delivered by blockchain. Block-chain is a technology that guarantees trust without a central authority. The transaction details are stored in blocks and are connected and stored in a chain form. A study was conducted on block-chain technology, a technology that processes data by storing data connected in the form of a chain generated between peers in a distributed environment [3]. Based on Ethereum's distributed consensus algorithm, the block-chain is being utilized to supplement the weaknesses of the centralized networking structure, and the consensus algorithm is one of the key elements in block-chain technology. In a network environment composed of distributed nodes, integrity and it is a very important factor in maintaining security. In this paper, we propose a distributed consensus algorithm to ensure the integrity of medical information in telemedicine systems that are emerging due to the corona pandemic. In the proposed algorithm, the telemedicine platform is a centralized system consisting of connections between multiple nodes centered on a central server, which may cause a problem in which patient information is leaked. Therefore, it is difficult to ensure the safety of patients' personal information, solves the problem of lowering the reliability of transactions, and guarantees safe telemedicine by guaranteeing the integrity of shared medical information. In this paper, the definition and problems of block-chain and telemedicine are presented as related studies. Chapter 3 proposes a consensus algorithm for federated learning proposed in this paper. Chapter 4 concludes the

paper with performance evaluation and conclusion of the proposed algorithm.

## 2. RELATED RESEARCH

### 2.1 Telemedicine

Although it is very difficult to define telemedicine in one word, it includes three common elements of telemedicine. Telemedicine can be defined as (1) the provision of medical information or medical services between (2) remote medical consumers (doctors (medical personnel) or patients) and medical providers (2) using information and communication technology (3) medical information. In other words, telemedicine is an advanced part of medical care that has developed as ICT technology is applied to existing medical practices such as treatment, patient monitoring, reading, advice, surgery, and rehabilitation, based on the doctor's expertise between patients and doctors. And will be defined in the field of healthcare in a broader sense in the future. In Korea, telemedicine is categorized by focusing on the actions performed between telemedicine actors, and in foreign countries, it tends to be categorized according to the telemedicine service provided. However, some scholars in Korea and in Japan are classified according to the subject of telemedicine diagnosis. One thing worth noting here is our society's legal definition of telemedicine, but the current medical law limits it to supporting medical knowledge or technology between medical personnel using information and communication technology. It is true given this reality, the government is currently implementing telemedicine within the regulatory sandbox. In addition, rather than the expressions telemedicine and telemedicine, various related terms such as smart health care (ubiquitous, electrical, mobile-health, etc.), smart treatment, non-face-to-face treatment, and virtual care are used in confusion. At this point, it is necessary to make the broad and diverse definition a little more concrete. It is necessary to define it from the perspective of 'who, who, when, what, and how'. In other words, who (physician in hospital, university hospital doctor, telemedicine qualification holder, AI doctor), to whom (chronic disease patient, infectious disease patient, remote area patient, local patient), when (first visit/revisit, pandemic situation, medical disaster) Situation), what (diagnosis and prescription, education and counseling, visit guidance, simple monitoring), and how (text, voice call, video call, artificial intelligence) can be defined in various ways and concretely[3,4]. It is possible to communicate in more detail within governance composed of stakeholders such as governments and corporations. Although telemedicine has several procedural problems, in the coming future, as the overall platform of society is changing in various ways, the medical field will have to carefully and continuously prepare for telemedicine. Looking at the advantages and disadvantages of telemedicine, what is interesting is that there are a lot of considerations on the advantages in foreign literature and more on the disadvantages in Korea. It can be said that the reality of telemedicine in Korea is well represented. First of all, telemedicine has several advantages for patients, governments medical staff, and related industries. From the patient's point of view, access to medical services is greatly improved, and spatial and temporal constraints can be alleviated to some extent in remote areas, in special areas such as prisons and ships, in patients with difficult mobility, and in emergency situations. From the government's point of view, it will be possible to reduce medical costs, improve medical welfare for medically vulnerable areas and classes, and strengthen disease and health management functions in the population. From the point of view of medical staff, sharing patient information can enhance continuity of treatment and help to share knowledge among medical professionals. In related industries, the possibility of generating profits from the digitization of all data is increasing. However, the disadvantages of telemedicine, which can also be called problems of telemedicine, are as follows. First, the safety of patients is very concerned due to the lack of evidence for telemedicine and the possibility of misdiagnosis. Second, the medical delivery system may collapse due to the concentration of medical care. Third, the risk of medical and health-related personal information leakage. That you have In addition, there are still many institutional challenges related to telemedicine, not the shortcomings of telemedicine itself. For open telemedicine, which is emerging due to the COVID-19 crisis, patient safety should be guaranteed through professionalism and scientific approaches based on ensuring patient privacy.

### 2.2 Block Chain Scheme

There is a limit to sending and receiving a large amount of data between end-to-end nodes centered on a central server. In particular, in the transaction method of the centralized management system, if the central server is hacked, data forgery/falsification becomes possible and the risk of users' personal information leaking increases. For example, in a technology operating in a

network such as IoT, based on periodic data storage and recording in the form of a database, if security and reliability can be guaranteed based on the information possessed by each peer, secure communication will be achieved [5-6]. Block-chain technology is a type of distributed database created to maintain the P2P-based Bitcoin protocol, and transaction details that have been confirmed for a certain period are stored in blocks and connected and stored in a chain form. Although it is used in various forms depending on the place of use, the basic structure is similar. In addition, it guarantees the reliability and integrity of the transaction through the consensus of all nodes participating in the network without a third-party performing authentication.

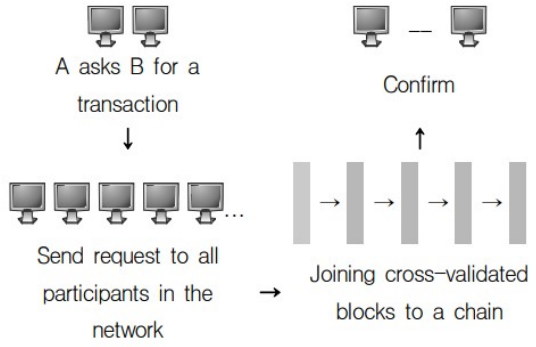


*Figure 1: Block-chain Transaction Process*

As shown in Figure 1, block-chain is managed in a decentralized way, breaking away from the centralized system, which is a representative transaction method. During the block-chain transaction process, the transaction details are encrypted with a hash value, and the data is authenticated by a validator to maintain the accuracy of the data. As such block chains are used in various fields, the problem of double-spending attacks has become an important issue. ***PoW*** (Proof of Work), a distributed consensus algorithm of Bitcoin and Ethereum, had limitations in application to various industries due to resource waste and performance limitations due to the mining method based on computational calculations. Also, with the advent of large mining pools, a small number of people monopolize mining, suggesting a problem of re-centralization. Therefore, in the block-chain environment, various distributed consensus algorithms such as ***PoS*** and ***BFT*** (Byzantine Fault Tolerance) have appeared to solve the excessive resource consumption and performance limitations of ***PoW***. A problem occurred, and although the performance of the BFT-based algorithm improved, scalability problems occurred due to the consensus load. Therefore, efforts were made to solve this problem, and a distributed consensus algorithm was proposed based on decentralization and scalability. This is called a hybrid distributed consensus algorithm. The hybrid-type distributed consensus algorithm distinguishes the process of selecting a consensus and the process of agreeing blocks by the consensus, and uses a different consensus algorithm. The hybrid-type distributed consensus algorithm can be divided into a scalability-oriented consensus algorithm that emphasizes scalability among scalability and decentralization and a decentralized consensus algorithm that emphasizes decentralization. The scalability-oriented consensus algorithm is an algorithm that performs BFT-based consensus after selecting a fixed few nodes as a consensus using ***PoS*** and ***DPoS*** (Delegated Proof of Stake). It has high scalability with a small number of nodes, but has the disadvantages of low decentralization due to a fixed consensus and vulnerability to network attacks. In addition, let's examine the consensus algorithm, one of the major elements of the block chain, closely, understand the principle of the currently adopted consensus algorithm, and analyze its limitations. A new consensus algorithm that can compensate for this limitation is needed.

## 3. FEDRATED LEARNING DISTRIBUTED CONSENSUS ALGORITHM FOR TELEMEDICAINE

In this paper, we propose a federated learning distributed consensus algorithm for telemedicine. In the proposed algorithm, in order to maintain the same value for specific data between systems when the system is decentralized, doctors participating in ECC-based telemedicine create blocks by performing secure signatures. The following is the block generation stage of the proposed algorithm, setup → header generation → signature generation → block generation → chain generation → key update → verification phase. In this paper, many block chain hash functions are performed by generating a signature without performing ***PoW***, unlike the existing block chain method, for blocks to be used for federated learning. The safety of the blockchain proposed in this paper is based on the safety of the signature used in the block verification method. The safety of the block chain is defined as the current shared block chain is $L_t$, and when the secret key $sk_t$ for creating the current block is leaked, forge from the $i^{th}$(i<t) block of $L_t$ to the t-th block, which is the

current block index. $L_t$ is defined as secure when the probability that the $L_t$ block chain created by being recognized by the participants is $\epsilon$ and shared. The following figure 2 shows the block design code.

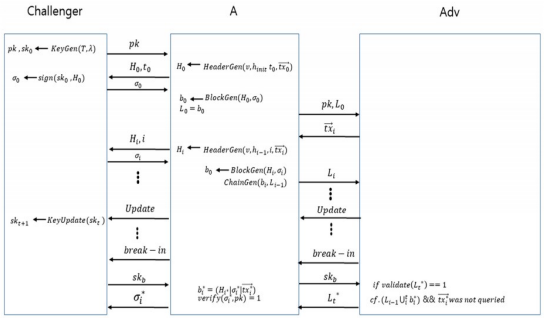


*Figure 2: Proposed Scheme*

Because the proposed algorithm does not apply the update of the secret key in the untrusted environment of the participants and always performs the representative signature generation immediately up to the secret key update, it returns the block hash without performing the secret key update, that is, ***PoW*** in the untrusted environment. Generates a secure signature and returns a block hash containing the signature. The generated signature value is authenticated with a public key so that users accessing the block chain can verify the block, and it generates a block hash of a newly created block through generate Blocks. Calls the ***Fss*** secret key stored in the storage. A block header of a new block is generated by inputting the block chain version information v, current time t, the called ***p-block*** and the transaction information received as input, Transaction Script, and the generated block header is signed with the called ***Fss*** secret key.

After that, the length of the block is increased, and the private key of the signature is updated after one cycle. When the cycle update is completed, hash values for the signature and block header are obtained and returned. By designating shared data among telemedicine data and applying it to a blockchain that stores shared data, personal medical data requesters can safely search for desired data without infringing on personal information, that is, privacy, and request private data accurately using the correct fields. Even when sharing data, processing efficiency is increased by sharing only the data of the appropriate field through re-encryption. The following figure 2 shows the blockchain smart contract system structure for safe telemedicine proposed in this paper.

In addition, doctors participating in telemedicine can verify the block chain created by the block producer. If the signatures of all blocks are verified as correct signatures, before verifying the signatures, the public key ***pk*** of the signature shared with the participants from block to block. It contains the signature value and can verify the block with the signature and public key. The proposed algorithm selects a consensus among nodes participating in telemedicine, and consensus is established on the block based on the selected consensus.

At this time, rather than all nodes participating in the consensus, some nodes selected based on the weight of the nodes proceed with consensus, and the consensus node is replaced at each detailed step of the consensus process so that the consensus node cannot be specified to prevent attacks on the consensus target. In the block agreement, a block producer is selected through VRF-based Cryptographic Sortation, and the selected block producer creates a candidate block. And finally, it was configured to derive a consensus on one block among a plurality of candidate blocks of the selected nodes.

All nodes participating in the consensus have a weight w according to their stake, and the number of selections expected through lottery is $p=l/W$ through the constant $\tau$ and the weighted sum , and the block creator has a selection probability value. Figure 3 schematically shows the block consensus process and shows the formula of the sortation algorithm.

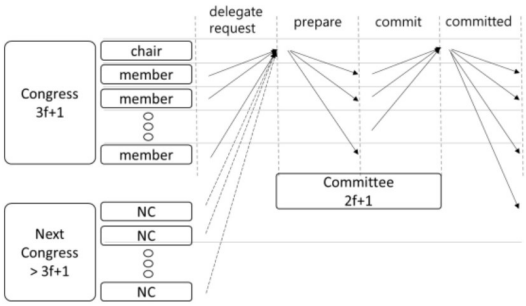


*Figure 3: Block Consensus Process*

$$<\text{hash}, > \quad \text{Net}_j = w_0 + \sum_{i=1}^{n} x_i w_{ij} \quad (1)$$

$$< \text{hash}, \pi > \leftarrow VRF_{sk}(seed||role)$$

$$p \leftarrow \tau/w, j \leftarrow 0 \quad (3.1)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\textbf{while } {}^{hash}/_{2^{hashlen}} \notin \left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p)\right]$$

$$\textbf{do } j++$$

$$\textbf{return } j$$

Each node has its own public key and private key pair to be used for VRF, and discloses the output hash and proof value π of the VRF created using the private key $sk$, and gives the right to vote as much as j through conditional expressions using $hash, p$, and $w$. You will be given the block creation role that you exercise. Thereafter, all nodes that have obtained block producer qualifications through the lottery algorithm generate candidate blocks and deliver them to all nodes. At this time, the generated candidate block and the weight $j$ of the node that generated the block are propagated together. The consensus body selected in this way agrees on a block through the consensus algorithm shown in Figure 3. At this time, the consensus node ($N = 3f + 1$) consists of one chair node and $3f$ member nodes. At this time, at the same time as the consensus algorithm is performed, the message of the consensus selection is transmitted through the following four steps.

• Delegate Request: All $3f + 1$ member nodes (including the chair node) transmit all transactions in their mempool to the chair node. At this time, the mempool is a storage that collects valid transactions received by each node from the client. At the same time, it checks whether it is the Next Congress (NC) of the next block through $\boldsymbol{PoN}$, and then sends the consensus selection message to the chair node if it is correct.

• Prepare: The chair node waits until it receives the Delegate Request message from $2f + 1$ member nodes (including the chair node), then selects a transaction commonly included in $f + 1$ messages among $2f + 1$ messages to create a candidate block. . At the same time, it creates an Evidence indicating which node sent which transaction, piggybacks along with the candidate block, and delivers the Delegate Request to $2f + 1$member nodes. In this case, $2f + 1$ nodes are called Committees.

• Commit: Committee nodes that have received the Prepare message from the chair node verify the received candidate block. By checking the received Evidence for verification, it checks whether the transaction delivered is correct and whether the included transaction is a transaction commonly proposed by $f + 1$ member nodes. When verification is complete, the committee node sends the block signature to the chair node.

• Committed: When the chair node receives a Commit message from 2 $f + 1$ committee nodes, it creates a multi-signature by adding the signatures of all committee nodes to the candidate block created by it, and adds the multi-signature to the block to confirm the block.

The chair node piggybacks the next consensus information to the confirmed block and delivers it to all participating nodes. The participating nodes that have received the Committed message repeat the above 4 steps. The PoW set in the proposed algorithm is generated. At this time, the hash value, data, and nonce value of the previous block are needed to calculate the hash value of the block. By creating it, the data is delivered to all medical staff participating in the federated learning. After receiving the block information, the medical staff calculates the hash value through the SHA256 hash function by adding this value. Since the hash value and data of the previous block cannot be modified when the solution value is obtained in this way, the block creator only changes the nonce value and adds the patient's medical information, and the medical staff participating in the added block verifies it. The medical staff participating in the treatment go through the mutual verification step for their respective treatment contents and confirm the final examination result and diagnosis result, and the consensus algorithm used at this time gives reliability. The proposed block is implemented as a storage, that is, a consensus algorithm between nodes in a way that does not use tokens to form a block chain, thereby providing reliability to medical care in telemedicine.

## 4. EXPERIMENTS AND CONSLUSIONS

The proposed model establishes a medical image data channel so that transactions and smart contracts occurring in the hospital can be shared only in the hospital channel, thereby maintaining the confidentiality of the patient's personal information, and hospitals, image readers, Read-across organizations can safely share medical image data channels with each other. The experimental environment was configured by installing

Hyperledger Fabric and using the default network.sh as shown in Table 1.

Table 1. Experiment environment

| Division | Explanation |
|---|---|
| OS | Ubuntu 20.04.3 LTS |
| Block-chain Platform | Hyperledger Fabric 2.2.3 |
| Language | JavaScript, go, |
| Block Generation Cycle | 15 sec |
| Block Size(MB) | 0.02MB |
| Number of Transactions | 2500, 5000, 75000,10000 |
| Number of Repetitions | 3 rounds |
| Client Program | Calling chaincodes on the block-chain as a shell program |
| Input Processing(Chain code) | A function that store data in the ledger |
| Output Processing(Chain code) | A function that retrieves data form the ledger |

The proposed model establishes a medical image data channel so that transactions and smart contracts occurring in the hospital can be shared only in the hospital channel, thereby maintaining the confidentiality of the patient's personal information, and hospitals, image readers, Read-across organizations can safely share medical image data channels with each other. The experimental environment was performed on the server without considering mobility to the hospital where the subject of blockchain signature creation belongs to the medical staff participating in the joint learning. To evaluate the performance of the proposed algorithm, an experimental environment was established, and the experiment time was measured for each algorithm. In addition, in the existing blockchain, the keygen algorithm is executed the moment a doctor is selected, and there is no need to perform any more after the initial block is created. Therefore, in the case of key generation, 338.5ms is consumed, but this was not taken into account in the design of the proposed blockchain. On the other hand, the update, sign, and verify algorithms are algorithms performed by real-time federated learning where telemedicine is performed, and when the key size is 64, it takes 3.9ms, 5.3ms, and 2.1ms to update. This is because PoW, which was used in the existing blockchain environment, took seconds to minutes, whereas in the case of the proposed algorithm, transactions that ensure real-time were performed through the blockchain. The proposed algorithm proposed a consensus algorithm for federated learning suitable for telemedicine environments by minimizing the time required to run the blockchain while reducing the computation cost of PoW in the blockchain environment. In the case of the proposed algorithm, the security of the signatures of participants participating in telemedicine was strengthened, and personal information and reliability were strengthened compared to the block chain used in the consensus algorithm of the block chain. In addition, even if the signature key is leaked, at least for the currently created block chain, it can be guaranteed that the block cannot be forged through the secure signature, and the safe signature can perform signature generation, signature verification, and secret key update in real time. This could be confirmed through the results. In this paper, since block generators are selected probabilistically, a plurality of block generators can be selected. Therefore, the selection probability of the block producer is important. If the number of block producers is probabilistically small, even a single block may not be generated in the worst case. To this end, the τ value used in the lottery algorithm was set so that the probability that the number of block producers is between 1 and less than 70 is $1 - 10^{-11}$ (τ=26 based on 50,000 nodes). In other words, the proposed method proved that the probability that the ratio of Byzantine nodes among consensus nodes would be 33% or less, that is, the probability of safety guarantee would be $5 \times 10^{-9}$, when 862 consensus nodes were selected from 50,000 nodes, and this probability was 500000 This is an achievable number when 2000 consensus nodes are selected from nodes, which means that when the same number of participating nodes exist, the same level of safety is achieved even if 43% of consensus bodies are selected in the proposed algorithm. The message complexity of the existing BFT-based consensus algorithm is $O(n^2)$ between nodes through block consensus, whereas the proposed algorithm using multiple signatures can lower the message complexity to $O(n)$.

In this paper, the performance of the consensus process was analyzed to test the reliability of block consensus and the stability of nodes through the proposed algorithm. The consensus process performance was measured by transaction processing time (TPS: transaction per seconds). The computer used in the experiment was an Intel Core i7-10510U CPU@1.8GHz processor and 16GB of RAM. For the experiment, the node case was divided into the case where the number of nodes participating for data sharing was less than 2500, more than 2500 and less than 5000, and more than 5000, and the results of the TPS experiment are shown in Figure 4. Case1 is the PoW consensus

algorithm and case2 is the proposed algorithm, and case2 showed 10.5% better performance than case1.

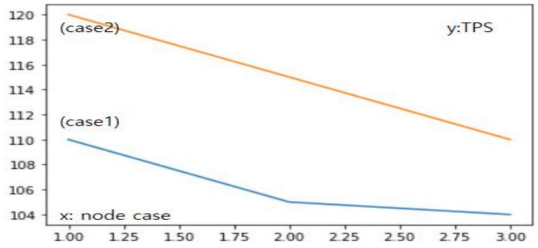


*Figure 1: Description Is Placed Right Below The Figure*

In order for blockchain technology to be successfully used in the medical industry and related social infrastructure, it is necessary to improve the maturity of the technology and secure a verification system through the preemptive introduction of public blockchain, and through this, collaboration with private blockchain and consortium blockchain A diffusion strategy is needed. Currently, most of the medical systems in general in society are highly centralized, so systematic research on the entire blockchain ecosystem such as consciousness, behavior, and institutions as well as technology to replace the existing service model, technology development and infrastructure is necessary, and the most suitable medical care finding applications is also very important. Blockchain-based medical service model development discovers and nurtures fields where blockchain technology is applied to the medical field to innovate the medical system in general. The goal is to discover a completely new medical service model that did not exist before, including areas that improve the system efficiency of the existing society as a whole, such as intelligence, personal health records, and wellness. In building blockchain core platform technology and governance in the medical field, research and development of blockchain core platform technology in the medical field, such as the development of an optimal blockchain architecture and performance improvement algorithm suitable for the medical field, and collaboration between public blockchain and private and consortium blockchain It is necessary to develop an integrated model and should include the establishment of national governance through the blockchain development council in the medical field. The he development of blockchain system and policy in the medical field prepared a national strategy to promote the use of blockchain in the medical field by improving the laws and systems related to the current hospital-centered centralized information infrastructure environment. In addition, rational policies to create a foundation for the spread of blockchain must be followed. The introduction and use of blockchain technology in the form of distributed ledgers in the medical field is inherently likely to cause various legal problems, and in cases where the cause is difficult to identify, the responsibility may be unclear. However, the current law is focused on the centralized management system, which is based on decentralization. It is in conflict with the blockchain technology that has been used, and due to the impossibility of abolition and deletion of retained data, it may be in direct conflict with the Personal Information Protection Act, the Medical Act, and the Act on the Use and Protection of Credit Information. Therefore, it is necessary to prepare a roadmap for establishing a national policy strategy to improve the laws and systems related to the blockchain information infrastructure environment and to promote the use of blockchain as soon as possible. This paper is a private service model of a new concept by linking the security vulnerabilities of telemedicine participants in telemedicine, which is emerging in the context of the corona pandemic, with block chain technology. It can be suggested as an alternative to overcome the anxiety about privacy exposure through information.

## 4. ACKNOWLEDGMENTS

This research was supported by the Daejeon University Research Grants (2020).

## REFERENCES:

[1] IM, H.G., "The Modification of PBFT Algorithm to Increase Network Operations Efficiency in Private Blockchains," *The Journal of the Korea Society of Computer and Information(JKSCI),* 26(2021) 99-104.

[2] Huang, D.Y., Ma, X.I. and Zhang, S., Performance Analysis of the Raft Consensus Algorithm for Private Blockchains," *The Journal of IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(2020) 172-181.

[3] Cho, Y.B., "Block-chain based Medical Image Sharing Protocol," *The Journal of TEST Engineering & Management*, 83(2020) 13059-13068.

[4] Kang, H.B., Jang, H.C.and Jang, C.S., "A Study on the Application Method of Multi-User Encryption Keys for Personal Information Protection in Blockchain," *The Journal of the journal of Korean Institute of Information Technology*,18 (2020) 135-141

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] Cho, Y.B., "Classification Algorithm for Liver Lesions of Ultrasound Images using Ensemble Deep Learning," *The Journal of the Institute of Internet, Broadcasting and Communication (IIBC)*, 20(2020) 101-106.

[6] Kim, K.S, "A study on the legal issues concerning distributed ledger technology based on the characteristics of P2P network and blockchain: Focusing on the Bitcoin network," *The Journal of Science and Technology Law Research*, 26(2020) 3-46.