Design and Implementation of a Personal Health Record Platform Based on Patient-consent Blockchain Technology

Heongkyun Kim[1], Sangmin Lee[2*], Hyunwoo Kwon[3], Eunmin Kim[3]
[1] VTW CSC (Creative Service Center) and Division of Industrial Convergence, Hanyang University
Seoul, Republic of Korea
[2] Department of Business Administration and Data Science, CHA University
Gyeonggi-do, Republic of Korea
[email: slee@cha.ac.kr]
[3] VTW CSC (Creative Service Center)
Seoul, Republic of Korea
[*]Corresponding author: Sangmin Lee

Received September 24, 2021; revised November 9, 2021; accepted November 23, 2021; published December 31, 2021

Abstract

In the 4th Industrial Revolution, the healthcare industry is undergoing a paradigm shift from post-care and management systems based on diagnosis and treatment to disease prevention and management based on personal precision medicine. To optimize medical services for individual patients, an open ecosystem for the healthcare industry that allows the exchange and utilization of personal health records (PHRs) is required. However, under the current system of hospital-centered data management, it is difficult to implement the linking and sharing of PHRs in practice. To address this problem, in this study, we present the design and implementation of a patient-centered PHR platform using blockchain technology. This platform achieved transparency and reliability in information management by eliminating the risk of leakage and tampering/altering personal information, which could occur when using a PHR. In addition, the patient-consent system was applied to a PHR; thus, the patient acted as the user with ownership. The proposed blockchain-based PHR platform enables the integration of personal medical information with scattered distribution across multiple hospitals, and allows patients to freely use their health records in their daily lives and emergencies. The proposed platform is expected to serve as a stepping stone for patient-centered healthcare data management and utilization.

Keywords: Blockchain, Hyperledger Fabric, On-Chain/Off-Chain, Personal Health Record, Patient Consent.

This paper was written based on the contents of the research project (HI19C0552) titled “Channel-type personal health record platform based on blockchain” of the Korea Health Industry Development Institute (KHIDI).

http://doi.org/10.3837/tiis.2021.12.008 **ISSN : 1976-7277**

1. Introduction

Under the current system, there are limitations to the exchange and utilization of personal health records (PHRs) owing to the centralized data management system used in medical institutions [1-3]. In particular, there are limitations to conflicting legal positions, in terms of changing, deleting, or destroying PHRs with the incorporation of blockchain technology [4]. Additionally, the inherent possibility of information loss and leakage when using PHRs is another drawback. Damaged information may compromise the credibility of the information, and there is also the possibility of information requests under identity fraud. Furthermore, it is difficult for patients to check when their medical information may be used, and if they consented to that act [1,5,6].

In general, PHRs can be managed with on-chain data of patient-consent information, and off-chain data for hospital treatment records [7,8]. With regard to consenting the use of personal information of PHRs, according to the provisions in the Personal Information Protection Act, the conditions of the consent require dynamic consent, in which the following applies: the consent should be "freely given," for which the individual data subject has the actual right of choice and can control and alter their consent choices in real-time [1,4,9-11].

In line with the need for a platform in which patient-centered medical data can be securely collected, stored, modified, and shared, a PHR platform based on the personal consent system using blockchain has emerged. The adoption of blockchain technology prevents the tampering/altering of data and ensures the autonomy of the patient in terms of PHR utilization as well as information transparency, thereby enabling the secure management and utilization of sensitive PHRs, for which high levels of reliability and security are critical [6,14]. Moreover, it allows patients to take ownership of the use of personal medical data by allowing them to manage their personal data with their own initiative, and conveniently view and check the history of the information usage. With the PHR platform, a groundbreaking shift to a data-driven healthcare system centered on prediction/prevention can be expected, and individual patient-centered precision medicine will be implemented in practice [2,3,11-13].

The goal of the proposed PHR platform is to present a secure and convenient method that utilizes PHR in the healthcare field through the research, development, and implementation of a patient-centered PHR platform that employs blockchain technology [4,14]. The information used in the proposed PHR platform is divided into patient-consent information and hospital treatment information; the structure of which is a blockchain network in which the platform, users, and medical institutions share a ledger [11]. The main contributions of this study regarding personal health management, application of blockchain technology, and usability by users are outlined as follows.

- The proposed patient-centered PHR platform based on a consent system using blockchain empowers the patients to have ownership over their health records and manage them accordingly.
- Our blockchain technology compensates for the defects of the conventional Hyperledger Fabric blockchain by allowing only users to have access to their data through the authentication process in the chaincode.
- The utilization of on/off-chain data enables us to overcome the limitations of using PHR in terms of privacy issues, insufficient storage space, network speed decrease, and security vulnerabilities.
- The health status of individuals can be viewed at a glance, and the provision of personalized medical services and treatment is possible based on the integrated medical records in emergency situations.

- With the participation of general hospitals, universities, and healthcare-related enterprises, this study showcases the feasibility of using the proposed patient-centered PHR platform as a standardized healthcare data distribution method and a technical reference model.

Based on the goals and expected effects described above, this paper consists of seven chapters. Chapter 2 presents a literature review of the blockchain concept and the related prior research. Chapter 3 describes the technologies used for platform development and its goals. Chapter 4 describes the structure and operation of the implemented platform, and Chapter 5 presents the platform configuration and implemented functions. Chapter 6 presents the results of the performance analysis with respect to the block generation time and block data size. Finally, Chapter 7 presents the conclusion and the limitations of the study based on the results, which could fuel future works.

2. Literature Review

2.1 Blockchain

In a blockchain, members in a distributed network record digital transactions into a shared ledger that can be viewed by all members, and the recorded transactions are copied to multiple computers and stored. The structure comprises blocks that contain data and are generated at a set period; these blocks are connected to prior blocks, similar to a chain [11,15]. Unlike conventional methods, in which transaction records are stored in a central server during data transactions, the transaction data in a blockchain are stored in a distributed network structured in blocks by all nodes (participants) participating in the transaction; the blockchain is referred to as a “public transaction ledger” [6]. With these characteristics, arbitrary modification or the tampering/altering of data is not possible; however, the changes in the transaction data can be viewed and shared by all participants in this distributed computing network [17].

The distinct merits of blockchain, when compared with the conventional database, include transparency (through the use of a shared ledger), security (by the authentication process), trust (formed by data validation), and immutable characteristics. In addition, the inherent properties of blockchain, such as cryptographic public/private key access, proof of work, and distributed data create a new level of integrity for healthcare information [31]. If a malicious adversary attempts to access a blockchain with personal information, such access can be blocked through public/private key matching. In the case of data manipulation, the data integrity can be validated, and the risk of hacking can be minimized through proof of work, in which any change in the data is compared and verified with other participants [1,19-21].

However, there are several limitations to the direct application of blockchain-based PHR platforms in PHR management. First, the PHR must be destroyed after a certain period of time; however, since data recorded in the blockchain cannot be changed or deleted, it indicates a conflict with the current legislative framework [4]. Second, participating nodes (participants) can view all data, which violates the provisions of the Personal Information Protection Act. Third, there is an exponential increase in the volume of medical data, such as the patient-generated health data, because of the development of wearable technology; however, owing to the reduced network speed and limitations in computing power, it is not realistic to store all data in unit blocks. In addition, in the case of technical errors or requirements for upgrades, prompt responsive actions may be relatively difficult [7].

In this study, a storage mechanism called the on/off-chain is employed for the implementation of the proposed system, in which an index called hash and address is stored on-chain, and the index is used to access the medical data in off-chain storage [5,11,22,23].

2.2 Dynamic Consent

Prior studies on the medical information consent system were conducted in 2019 and 2020. The consent system is divided into pre-consent (opt-in) and post-consent (opt-out) depending on the timing of consent of the data subject. Pre-consent (opt-in) refers to the case in which the personal information controller obtains consent from the data subject before collecting and using the personal information. Post-consent (opt-out) refers to the case in which the use of personal information is discontinued when the data subject expresses their unwillingness to use the information [23,24].

In the United States and Europe, regulations have been relaxed so that non-personally identifiable information can be used in an opt-out manner when the non-personally identifiable information is used for public interest/academic purposes. The General Data Protection Regulation (GDPR) of Europe stipulates the following as valid consent: 1) freely given consent, 2) individually specified consent, 3) informed consent, and 4) consent with an unambiguous indication of the wishes of the data subject [24-26]. “Freely given consent” refers to dynamic consent, in which data subjects have actual rights of choice and control over the processing of personal information, to freely give or withdraw their consent, and alter their consent choices in real-time [9,10,24]. However, since only the pre-consent method is recognized under domestic laws, such as the Personal Information Protection Act, in order to use sensitive information such as PHR, it is necessary to notify the data subject in advance and obtain their consent [24].

2.3 KOREN-based Healthcare Blockchain Demonstration Project

This is a project for verifying the feasibility of distributing standardized healthcare data using the Korea Advanced Research Network (KOREN) software-defined infrastructure. Based on anonymized medical data, the project aims to build a blockchain server in several physically separated spaces and examine the results by assuming the reliable operation and distribution of PHRs. This study is a large-scale demonstration project involving the participation of multiple organizations such as large hospitals, universities, and companies in the healthcare sector, and presents the feasibility of the distribution of standardized healthcare data and the technical method.

2.4 MedRec: Project for Sharing Electronic Health Records and Medical Research Data Using Blockchain

MedRec is an open-source project for the development of a decentralized PHR platform through a blockchain smart contract. It aims to provide medical researchers with a rich source of medical data while allowing patients to freely choose whether to disclose medical metadata as active participants [1,10,28]. This model enables authentication, confidentiality, accountability, and data sharing using the private Ethereum blockchain and allows organizations to have different levels of permission to read/write for each participant. In addition, the patients can check the person, content of the information, time (when the information was viewed), use of the information, and where their PHR was exposed.

3. Platform Model

In this chapter, the models used in the platform and types of blockchain are examined, and the design goals of the PHR platform are presented.

3.1 On/Off-Chain

As discussed in Chapter 2, there are some limitations in the direct application of blockchain to PHR management; to overcome these limitations, a storage mechanism called on/off-chain was used. Blockchain can store two types of information: (1) “on-chain” data, which verifies the reliability and security of the data, is directly stored on the blockchain and (2) “off-chain” data is the large amount of data stored in separate external databases [7,8].

Using the on/off-chain method, expansive detailed health records are stored off-chain so that the stored data can be altered and deleted while protecting information privacy and small-sized data, such as hash, which is stored on-chain, thus presenting a solution for computer overload.

3.2 Public/Private Blockchain

The various types of blockchain can be largely divided into public blockchain, which can be accessed by the general public, such as Ethereum and Bitcoin, and permissioned and private blockchain, which can be used only by the users registered in the membership service provider (MSP) authentication management platform [19,20]. In this study, a private blockchain concept was used to develop a platform that could maintain confidentiality between the blockchain participants in a private channel; the Hyperledger Fabric, which provides the MSP-based access control function and is most actively updated as an open-source form for the development and implementation of the platform, was used among the different types of Hyperledger frameworks [19,20,29,30]. **Table 1** outlines the types and characteristics of the different Hyperledger frameworks, including the Hyperledger Fabric [32,33].

Table 1. The types and main features of a Hyperledger framework

Types	Description
Hyperledger Fabric	• Applied to the most active Hyperledger projects • A method that provides MSP-based access control and forms consensus after arranging transactions in blocks
Hyperledger Sawtooth	• Built based on the Intel distributed ledger • Uses the Proof of Elapsed Time consensus algorithm, which is implemented using the Secure Guard Extension
Hyperledger Iroha	• Based on the Yet Another Consensus algorithm, in which the consensus is formed by voting on block hashes • Provides infrastructure for mobile and web environments such as iOS, Android, and JavaScript
Hyperledger Indy	• The development was led by the Sovrin Foundation • Purpose-built for providing digital identities without intermediaries in the Internet environment

3.3 Design Goals

In this study, we developed a patient-centered PHR platform that focused on the following challenges: 1) improving the ease of information sharing and utilization through PHR integration, 2) enhancing data security and transparency using blockchain, and 3) utilization of patient-centered PHRs through a consent system. To manage and use the PHR of a patient as a data controller, the PHR platform should achieve the following goals.

- **Reliability:** Since all ledgers are shared by blockchain, the risk of data tampering/altering is reduced, and only the user themself can use/verify their data through the authentication process [31].
- **Autonomy:** Based on the dynamic consent system that allows the consent and withdrawal of consent for use of PHR in real-time, the patient manages the data with ownership over that data.
- **Data integration:** By integrating PHRs with a scattered distribution across the databases of individual hospitals into the platform, data can be freely used; this is especially useful in cases where detailed patient records are required in urgent situations such as emergencies.

4. Blockchain Model

This chapter describes the internal structure and operation mechanism of the blockchain, which is the core technology of the platform, and presents the operation procedure of various functions implemented in the platform.

4.1 Blockchain Structure

A blockchain network consists of multiple components (peers, ledgers, smart contracts, orderers, policies, channels, applications, organizations, identities, and membership). Among these various components, a peer node, or peer for short, refers to each server participating in a transaction in a blockchain network, and because it has a ledger with transaction records and a smart contract (referred to as the chaincode in a Hyperledger Fabric), it is the most important component in the network [34].

4.1.1 Participants of Blockchain Platform

Blockchain platform participants are classified into four categories, as shown in **Fig. 1**. 1) A patient or user who is the owner of PHR data; 2) a platform that manages the blockchain ledger and information with the delegated authority from the patient; 3) an institution, such as a hospital, visited by a patient that creates and provides PHRs (Organization A), and 4) an organization, such as an insurance company or other hospitals, that requests and uses the PHRs (Organization B).

The user (the patient) delegates the authority to store their PHR on the platform, and the platform receives, stores, and manages the PHR of a patient from institutions (such as multiple hospitals) upon obtaining consent from the patient. In addition, Organization A (the producer and provider of PHR) creates the PHR for each visit by the patient, and when another hospital (Organization B) requests the data of that patient, the information is sent through the platform upon obtaining prior consent from that patient.

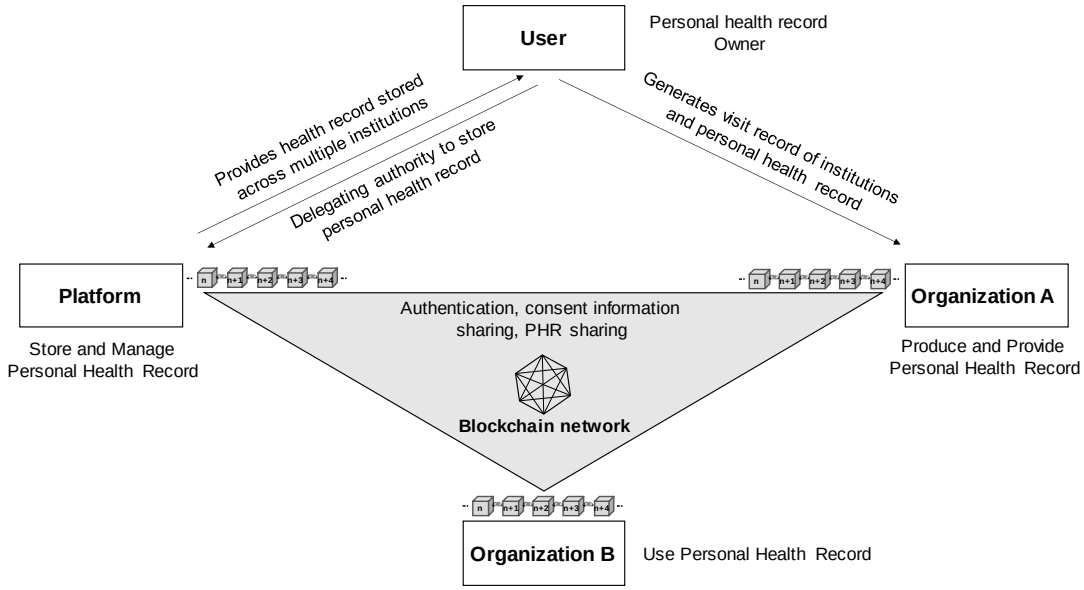


Fig. 1. Participants and their roles

4.1.2 Peer Nodes on Blockchain Network

As shown in **Fig. 2**, peers directly participating in the blockchain network are the platform operators that share the ledger: Organization A, which produces and provides the PHR, and Organization B, which requests and uses the PHR; they all have a network key.

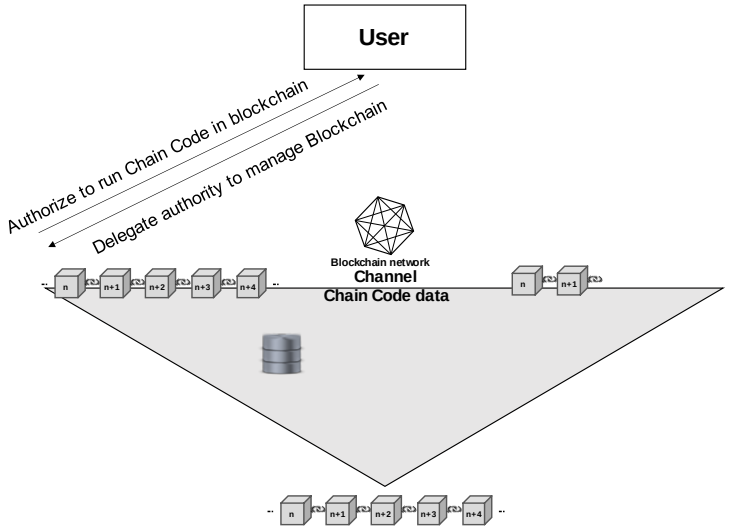


Fig. 2. Peer nodes on the blockchain network and identification key by role

It is not feasible in practice for users to create a platform and run it in real-time to share the blockchain ledger; hence, the users are not direct participants in the blockchain channel. Thus, because the users are not subscribed to the channel in the blockchain network, they

cannot view the data of the ledger or input data through the chaincode. Instead, the users delegate authority to the platform operator and gain access to the blockchain network through a platform.

4.1.3 Authentication Key

A conventional Hyperledger Fabric system confirms network participants using the Membership Service Provider (MSP) component, but cannot identify users in chaincode. Furthermore, as described in the sections on blockchain participants and peer nodes, if a participant is subscribed to a channel, the participants can read the any content of the ledger and create a new block using the chaincode. However, if all channel subscribers can read all data in the blockchain and create content, one of the participating organizations can view the data of a user and change it at will, which could prove to be malicious. To overcome these defects of the conventional Hyperledger Fabric framework, the blockchain chaincode presented in this paper uses an authentication key to grant different authorities according to the role classification of each node. The types of authentication keys that can be registered in the chaincode correspond to the data key in **Fig. 2**, and the role of each key is outlined as follows.

- **Platform Administrator Key**: With chaincode, only one administrator key can be created, and the platform, which is a blockchain network administrator, has that administrator key. The platform administrator can use this key to view most records, such as the user identity data stored in the blockchain, user consent history, and PHR sharing history; however, unlike the users, the administrator cannot give consent to the consent form or request PHR sharing.
- **Organization key**: A node with an organization key is an organization, including hospitals and public health centers. They can generate consent forms and send data when users request PHR sharing with the chaincode.
- **User key**: A node with a user key is a patient, and the patient can create consent information in the consent form created by the organization, as described above. They can also request data sharing to the organization that has the PHR of that patient.

4.2 Blockchain Algorithms

The implementation of blockchain algorithms to use the functions of the PHR platform consists of three steps. 1) In the key registration process, users and organizations register keys on the channel through identity registration. 2) In the consent process, the organization registers the consent form in the chaincode, and the patient can provide their consent for that consent form registered in the chaincode. 3) The sharing health record procedure includes the process of requesting PHR sharing to sending PHR, and validation. **Table 2** outlines the main notations used in the blockchain algorithm schematics.

Table 2. Notation and description

Notation	Description
$U_{()}$	User () => ex) U_A U_B User A, User B
P	Platform
$O_{()}$	Organization ( ) => O_A O_B Organization A, Organization B
PK	Private Key => ex) U_APK O_APK, Private key to user A, Private key to Organization A
AR	Address => ex) U_AAR U_BAR Address to user A, Address to user B

$DT_{( )}$	Data => ex) $U_ADT_{(name)}$ $U_ADT_{(name,\ birth)}$ Name data for User A, Name and birth data for user A
$TX( )$	Transaction(parameter) || On-chain Transaction(parameter) ex) $TX(U_APK,\ U_ADT_{(name)})$ Transaction with user A's private key and name data
$OTX( )$	Outer Transection(parameter) || Off-chain Transaction(parameter) ex) $OTX(DT_{(consent)})$ Sending consent data to our platform
$RT( )$	Return(data) => ex) $RT(O_APK)$
$( )^{hash}$	Convert data to hash => ex) $(U_ADT_{(name,\ birth)})^{hash}$ Hashed name and birth data of User A
$( )==( )$	Compare the two data => ex) $(U_ADT_{(name,\ birth)})^{hash}==$
IDG	Chaincode identification data group
CFG	Chaincode consent form data group
CDG	Chaincode consent data group
MIG	Chaincode Medical information usage record data group
$( )SQ_{( )}$	Data group unique sequence => ex) U_ASQ_{IDG} O_ASQ, ID to user A, ID to organization A
$( )SL_{( )}$	Search the data => ex) $(U_AID)SL_{IDG}$ Search U_AID in the IDG
$( )IN_{( )}$	Insert the data => ex) $(U_AAR,\ SQ_{CFG},\ DT_{(agree\ Y/N)})IN_{CDG}$
$( )@Q$	"Select" Query => ex) $MIG@Q$
$( )UP_{( )}$	Update the data => ex) $Q(DT_{(status\ code\ :\ success)})UP_{MIG@Q}$
$*()$	All data => ex) *ID
>>	Generate data from a key => ex) $O_APK >> O_AAR$

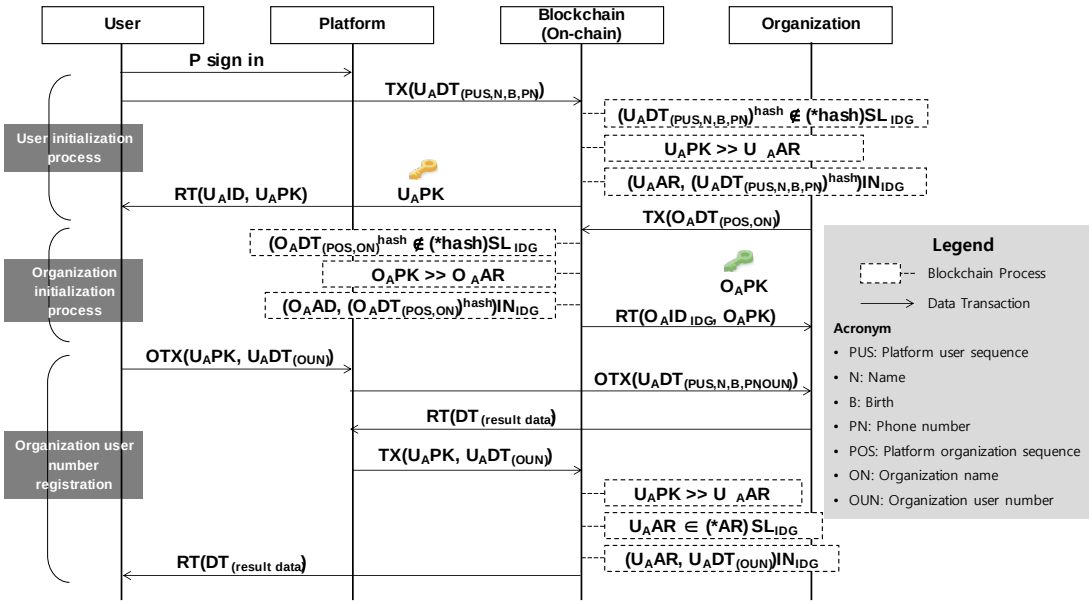


Fig. 3. Key Registration Process

4.2.1 Key Registration Process (Initialization)

Fig. 3 illustrates the process of identity registration in the blockchain. Process consists of three parts: user key registration, organization key registration and organization user number registration. For authentication, the hash of user A (U_A) and a key set are required. A key set consists of a private key (PK), an address (AR), and a public key. In this study, we use PK and AR for authentication. To generate a key set, an arbitrary private key is first generated,

followed by a conversion into address with the private key ($U_APK >> U_AAR$), and the generated address is stored and managed in the chaincode authentication data. Hence, authentication can be performed by converting the private key to an address and comparing it with the address on the chaincode.

4.2.1.1 Registration of user identity information

This process authenticates a user in the blockchain chaincode when giving consent to the consent form created by the organization or requesting PHR sharing to the organization. In the process of registration, a transaction (*TX*) is requested with a blockchain chaincode, and for the transaction data, the platform user classification value (*platform user sequence*), name (*name*), date of birth (*birth*), and cell phone number (*phone number*) of the user (U_A) are sent ($TX(U_ADT_{(platform\ user\ sequence,\ name,\ birth,\ phone\ number)}$). The data received from the chaincode ($U_ADT_{(platform\ user\ sequence,\ name,\ birth,\ phone\ number)}$) are converted to a hash (($U_ADT_{(platform\ user\ sequence,\ name,\ birth,\ phone\ number)})hash$), and the hash of the user and the total hash ($(*hash)SL_{IDG}$) stored in the identification data group (IDG) are compared to check the agreement between the values.

4.2.1.2 Registration of the organization identity information

This process authenticates an organization in the blockchain chaincode when creating the consent form required for the organization, or when confirming the request of the PHR sharing from the user and processing that request. In the registration process, a transaction (*TX*) is requested with a blockchain chaincode, and for the transaction data, the platform organization classification value (*platform organization sequence)* of the organization (O_A) and the organization name (*organization name*) are sent ($TX(O_ADT_{(platform\ organization\ sequence,\ organization\ name)})$). The process of converting the data received from the chaincode and storing the hash is similar to the process of the user identity information registration described above.

4.2.1.3 Registration of the organization user information

This process is to get confirmation of user(U_A)'s organization user number by organization(O_A). When the user sends the private key (U_APK) and the unique sequence number of the user for the organization ($U_ADT_{(user's\ organization\ number)}$) to the platform ($P$) by off-chain ($OTX$) ($OTX(U_APK, U_ADT_{(user's\ organization\ number)})$), the platform sends the name (*name*), date of birth (*birth*), and cell phone number (*phone number*) of the user and the unique sequence number of the user for the organization (*organization user number*) to the hospital off-chain, and requests to confirm whether the user is registered in the organization. An organization verifies the off-chain received user data (($U_ADT_{(platform\ user\ sequence,\ name,\ birth,\ phone\ number,\ user's\ organization\ number)}$)) and returns the result ($RT_{(result\ data)}$)) to the platform. When the user authentication is complete in the chaincode, chaincode generates AR from PK ($U_APK >> U_AAR$). Finally the unique sequence number of the organization and sequence number of organization user (*user's organization number*) are stored in the user data($U_AAR,U_ADT_{(organization\ user\ number)}IN_{IDG}$), as shown in **Fig. 3**.

4.2.2 Consent Process

The process of registering the consent form information of the organization and the consent information of the user with the chaincode is shown in **Fig. 4**.

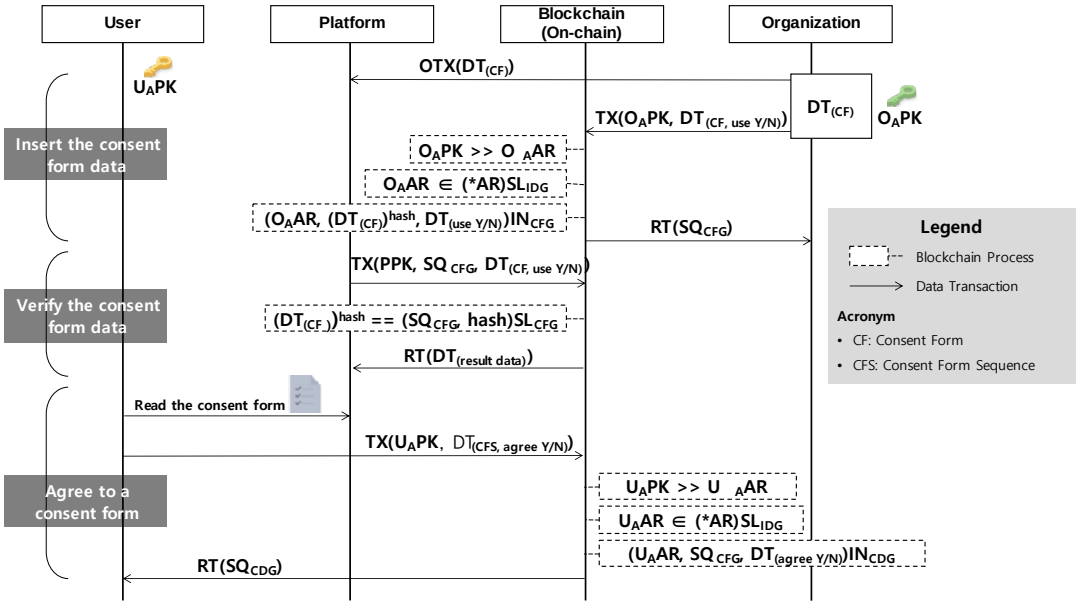


Fig. 4. Consent process

An organization (O_A) that has completed the identity registration process can upload the consent form of the organization to the blockchain. In general, hospitals can create various forms of consent, such as consent forms for personal information inquiry, or treatment and operation consent for surgery. In this paper, the identity authentication process is described by assuming that the consent form to share the PHR is registered. For authentication using on-chain data in the consent and PHR sharing process, the private key (PK) of the user (U_A) or organization (O_A) is sent. The private key that has been sent is converted to an address, and it is checked whether the converted value corresponds to the user or organization registered in that identification data group (IDG).

4.2.2.1 Consent form data registration

The organization (O_A) sends the data with the content of consent form to the platform via *Off-chain* $OTX(DT_{(consent\ form)})$ and sends private key of the organization (O_APK), content of consent form and use status of the consent form to chaincode via *On-chain* $TX(O_APK, DT_{(consent\ form,\ use\ Y/N)})$.When the authentication of the organization is completed in the chaincode, data with the content of the consent form is converted into a hash, and then the address, the hash, and use status is saved in the consent form data $((O_AAR, (DT_{(consent\ form)})^{hash}, DT_{(use\ Y/N)})IN_{CFG})$. Chaincode sends the unique sequence number of the consent form, and the platform stores the sequence number and the consent form data $(DT_{(consent\ form)})$ sent off-chain from the organization. To verify data manipulation of the consent form sent to platform, the platform sends its consent form to the blockchain and compares the hash values of both sides. The sequence number is used to allow users to give their consent to the consent form and to change the use status of the consent form.

4.2.2.2 Giving consent to the consent form

A user (U_A) who has completed identity registration and an organization user number registration, can proceed to give their consent to the consent form prepared by the relevant organization (O_A). In this section, the process of the user giving consent to the consent form is

described assuming a consent form (SQ_{CFG}) for sharing the PHR is registered. To give consent to the consent form, user private key (U_APK), sequence number of the consent form, and the consent status is sent to chaincode ($TX(U_APK,\ DT_{(consent\ form\ sequence,\ agree\ Y/N)})$). After user authentication with AR ($U_AAR \in (*AR)SL_{IDG}$), the AR, the sequence number and the status of consent are saved in consent form data group (CFG) by chaincode($((U_AAR,\ SQ_{CFG},\ DT_{(agree\ Y/N)})IN_{CDG}$).

4.2.3 Procedure of Sharing Personal Health Record

Fig. 5 shows the PHR sharing procedure, which consists of a PHR sharing request and verification, and the PHR data sending and validation processes. The PHR sharing data consist of a unique sequence number, the sequence number of user requesting the PHR sharing, a share request confirmation value, and status of a request.

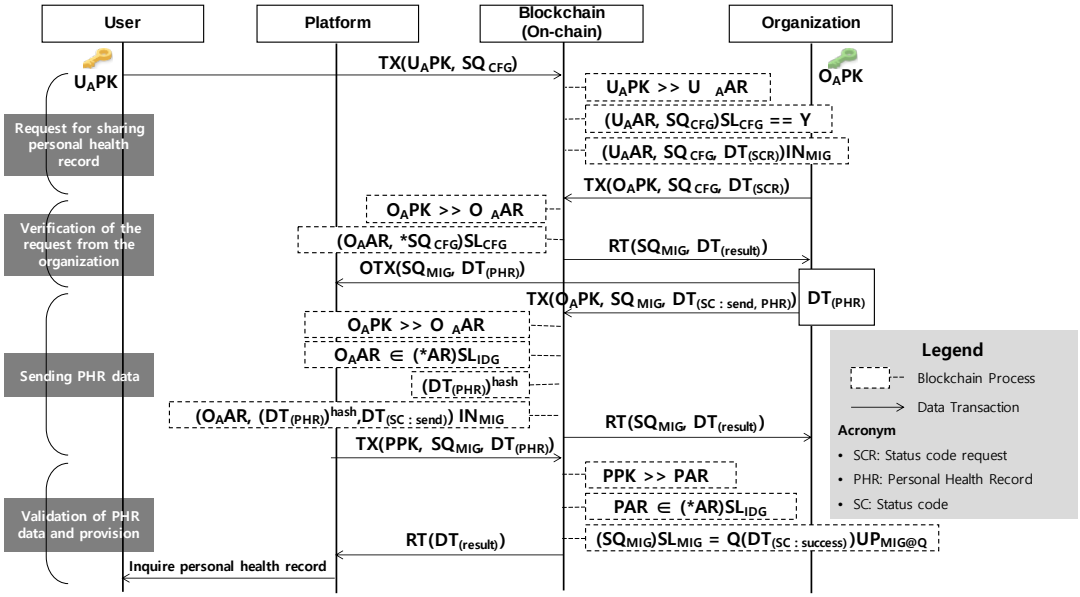


Fig. 5. Health Record Sharing Procedure

4.2.3.1 PHR data-sharing request

The user (U_A) requests PHR data from the organization based on the consent data (SQ_{CDG}) of the consent form (SQ_{CFG}) registered by the organization (O_A). When the authentication process of the user is complete on the chaincode, and the status of consent ($(U_AAR,\ SQ_{CFG})SL_{CFG} == Y$) has been confirmed, a transaction is requested with the sequence number for user authentication (SQ_{IDG}) and the consent data (SQ_{CDG}), and the code of requested status ($DT_{(status\ code:\ request)}$) by chaincode for sharing request ($(SQ_{IDG},\ SQ_{CDG},\ DT_{(status\ code:\ request)}IN_{MIG})$).

4.2.3.2 Verification the organization request

The organization (O_A) requests a transaction (TX) via the blockchain chaincode to view the status data (*request*) of the consent form with the consent form sequence (SQ_{CFG}) prepared by the organization. As for the data, the private key (O_APK) and consent form sequence (SQ_{CFG}) of the organization are transmitted; the identity authentication process of the organization is

completed in the chaincode, and the status is checked and verified by searching ($((O_AAR, *SQ_{CFG})SL_{CFG}$) the consent form that is using the organization address (O_AAR).

4.2.3.3 Sending PHR data

After the organization (O_A) verifies the PHR sharing request by the user (U_A) through the organization request verification process, the PHR data ($DT(personal\ health\ record)$) and the PHR data sequence (SQ_{MIG}) are sent to the platform via the off-chain (OTX). When the data transmission is completed, the sending success status data and PHR data ($DT_{(status\ code:\ send,\ personal\ health\ record)}$) are sent to the blockchain ($TX(O_APK, SQ_{MIG}, DT_{(status\ code:\ send,\ personal\ health\ record)})$), and the PHR data are converted to hash ($(DT_{(personal\ health\ record)})^{hash}$) and stored.

4.2.3.4 Validation and provision of PHR data

In the last stage of sharing the PHR, the platform (P) sends the private key of the platform (PPK), PHR data sequence (SQ_{MIG}), and the PHR data received by the off-chain from the organization ($DT_{(personal\ health\ record)}$) via the blockchain chaincode. When the identity authentication process is complete in chaincode, the transmitted PHR data are converted to hash ($(DT_{(personal\ health\ record)})^{hash}$), and the data are compared and validated. From the comparison, if the hash matches with one that stored in the blockchain, the success status is updated ($(DT_{(status\ code:\ success)})UP_{MIG@Q}$) and the result data are sent to the platform ($DT_{(result)}$). Through this process, it is possible to validate whether the information currently held by the platform is correct or has been manipulated by a third party.

5. System Implementation

In this chapter, the implementation environment of the platform is described, and the screen of the actual implementation is presented.

5.1 Configuration

In this study, the configuration of three virtual servers of blockchain is based on Ubuntu. They are composed of two orders and two organizations, and each organization comprises two peer nodes. The one who issues the order uses validated transactions to ensure the secure delivery of transactions to peer nodes. The peer node is the most basic node in the Hyperledger Fabric with chain (ledger); the chaincode (smart contract) developed in this study is also included in the peer node. The peer validates the requested transaction and shares it with other peers by updating the chain (ledger).

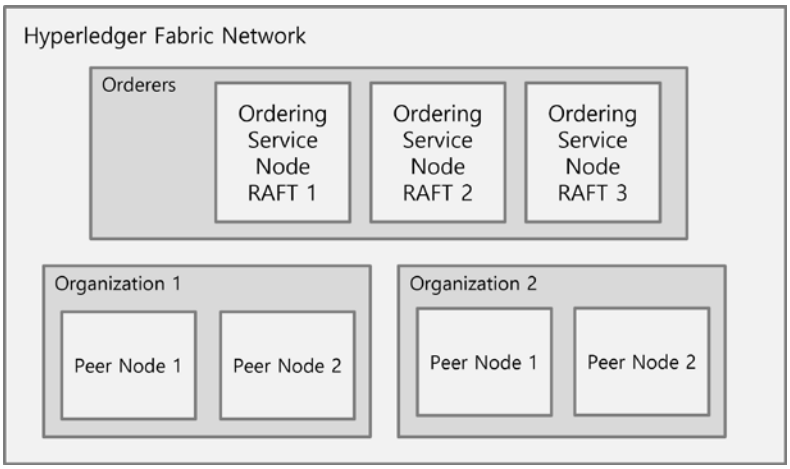


Fig. 6. Hyperledger Fabric network configuration

In our Hyperledger Fabric network, orderers use the Raft algorithm as presented in **Fig. 6**. Raft is a distributed consensus algorithm of the Hyperledger Fabric [35], which selects a leader and followers to provide a stable ordering service even when errors occur in some nodes. Raft was used among the other algorithms such as Kafka because Hyperledger Fabric officially supports only Raft consensus from version 2.0, and our network was built with version 2.2. Ordering service nodes are connected and operate as a single system with Raft, similar to the configuration of a cluster.

5.2 Implementation

Among the functions of the blockchain-based PHR platform presented in this paper, the identity registration function, consent form registration function, consent function, and PHR sharing function are described, and a screen with the direct implementation of the platform is presented.

5.2.1 Key Registration Function

For user key registration, after entering the name, date of birth, and gender information in the unique sequence number (*Key*) of the user in the platform, as shown in **Fig. 7**, the authentication sequence number (*userSeq*) completed with registration in the blockchain and the response data of the private key is provided, as shown in **Fig. 8**. The user can proceed with the consent, registration, and PHR data request with the received private key. The key registration function of the organization proceeds similarly to that of the user.

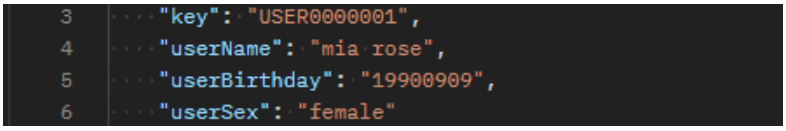


Fig. 7. Requesting the user key registration

Fig. 8. Response to the user key registration

5.2.2 Consent Form Registration Function

In **Fig. 9**, for the registration request, the private key of the organization that has completed the key registration, a JSON-format document containing the contents of the consent form, and the status data for the use of the consent form (*useYn*), are sent. When the converted hash value is stored, as can be seen in **Fig. 10**, the unique sequence (*adSeq*) is sent to the consent form to proceed with the user consent.

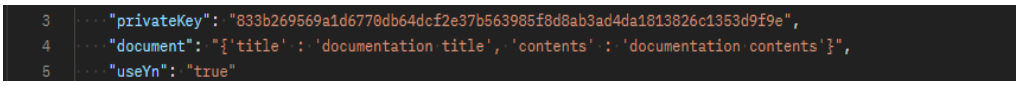


Fig. 9. Requesting the registration of the consent form

Fig. 10. Response to the registration of the consent form

5.2.3 Consent Function

As for the private key of the requested data shown in **Fig. 11**, the private key completed with key registration as shown in **Fig. 8**, the consent form sequence responded as shown in **Fig. 10** (adSeq), and the agreement status data (*agreeYn*) are sent to the consent form, as shown in **Fig. 12**.

Fig. 11. The consent request

Fig. 12. The response to the consent request

5.2.4 PHR Data-sharing Function

The PHR data-sharing request and response proceed in a similar way to the key registration and consent function. The response result only shows a sequence number of the PHR data; however, from the internal blockchain data, the status is changed to a request status as shown in **Fig. 13**, which allows the organization to view the data request of the user.

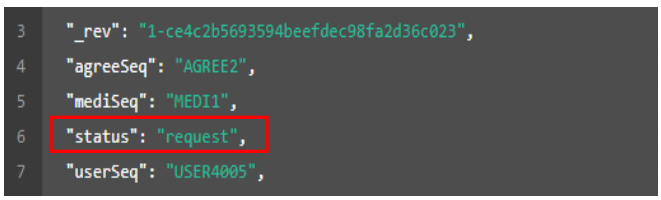


Fig. 13. Verification of the PHR data (request)

The last process validates the PHR data in the blockchain received from the off-chain organization in the platform. With the chaincode, the private key of the platform, PHR data sequence (*MEDI1*), consent data sequence (*AGREE2*), and PHR data (*mediInfo*) are transmitted. In the chaincode, the received PHR data is converted to a hash and checked, and if the value matches the information registered by the organization, the status data is “success”,

as shown in **Fig. 14**.

```
"_id": "MEDIDETAIL2756",
"_rev": "2-3d463a8fc98ac27bcc99213d7f141833",
"address": "9cA3f331a6e2d606996B37Da082d1D3c7EC5F7F5",
"agreeSeq": "AGREE2",
"mediDetailSeq": "MEDIDETAIL2756",
"mediInfo": "ea481ec8e2c3fa4472bbc85347c6d88fc20266fc209ff54252b9890c56860819",
"mediSeq": "MEDI1",
"status": "success",
"~version": "CgQCIKoA"
```


Fig. 14. Verification of the PHR data (Success)

Through the processes described above, the user can give their consent to the consent form only with their authentication key (*private key*), and can request the PHR based on the consent form. Even for a platform administrator or a hacker, without the proper private key, they cannot access the consent or the PHR through the blockchain.

6. Performance Analysis

In this chapter, the performance assessment of our proposed model was based on the block generation time test, and measurement of the maximum data storage ~~amount~~ of the blockchain by measuring the size of block data. The block generation time affects the overall processing time of all of the chaincode functions; thus, it was important to check whether the network exhibited an appropriate block generation speed by measuring the transactions per second. Moreover, we performed data size measurement because the block data size affects the process speed of the chaincode. The test results were compared with data from the national statistics office and hospitals to conduct an appropriate performance assessment.

6.1 Block Generation Time (TPS: Transaction per Second)

The response time from requesting a transaction from the Hyperledger Fabric-based blockchain to stacking one block in the blockchain network was analyzed, as shown in **Fig. 15**. When 1000 blocks were stacked, the fastest and slowest response times were 33 ms and 95 ms, respectively; the average response time was 50.608ms, and the number of transactions per second was 19.759 TPS. This is the rate of generating 5.66 cases per second based on a total of 178,341,437 cases of outpatient examinations at tertiary general hospitals, general hospitals, and hospitals presented in the data of Statistics Korea in 2019. This can be regarded as a suitable TPS for tertiary general hospitals, general hospitals, and local hospitals.

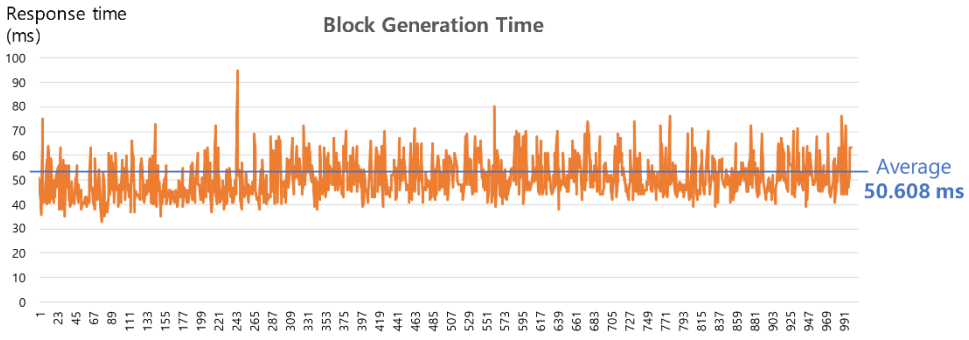


Fig. 15. The block generation time

6.2 Size of Block Data

In addition to the block generation time (TPS), an important performance indicator in a blockchain is the size of the data accumulated in the block. Many firms construct databases that store blockchain data and blockchain index data or hash values, and then use a combination of these data.

In consideration of personal information leakage and blockchain scalability, the design of the PHR platform proposed in this paper also includes a hash that validates the PHR data in the block data, which is the on-chain data; the decrypted PHR can be managed as off-chain data in this design. Among the currently developed blockchain systems, PHR data has the largest data size, and as a result of checking the blockchain data size, an average data size of 312 bytes is required per PHR sharing data.

Based on the total number of outpatient examinations at tertiary general hospitals, general hospitals, and hospitals derived from the data of Statistics Korea in 2019 [36], when the measured average data size (312 bytes) is multiplied, the size of the PHR blockchain data proposed in this study recorded over one year in Korea can be estimated to be 55,642,528,344 bytes (51.821143 GB). In general, the block data size of Ethereum accumulated for about six years from 2015 to the present is 900 GB; thus, it is recorded at an annual average of 150 GB, which is far bigger than the blockchain data size presented in this paper.

7. Conclusion and Future Research

In this study, to utilize patient-centered PHRs, a process from user identity information registration to patient-consent procedure and PHR sharing was established, and a blockchain-based PHR platform was implemented. The distinct effects of this platform include: 1) preventing data tampering/altering by comparing hash values, 2) ensuring transparency by sharing transactions, and 3) improving security through an identity authentication process. In particular, by adding an authentication process to the chaincode of the private blockchain of the Hyperledger Fabric, only registered users can participate in the network, and only the user themselves can gain access to their personal information. Users were able to exercise independent ownership of their PHR and the platform presented an opportunity to raise awareness of the use of personal information. In addition, the feasibility and validity of the PHR platform were confirmed through performance analysis. Should the proposed platform be used in the future, PHRs scattered around individual hospitals can be integrated into one system, and PHR consent can be obtained in advance to facilitate the safe and convenient use of the data.

The contribution of this study is that it presented a systematic direction for how blockchain technology could be employed to implement a patient-centered data utilization platform.

The blockchain-based PHR platform presented herein is expected to enable improved confidence on the part of patients and doctors owing to increased data sharing, which will lead patients to become more active in writing daily health records on the platform. In consequence, PHR big data systems will shape the future of medical science by facilitating preventive and predictive methods designed to provide personalized and participatory medical service.

However, our study has a limitation in that the beta test of the platform and the feedback from user demonstration were omitted due to the COVID-19 situation.

In future studies, further investigation on data standardization, which is an essential step for the integration of data in various organizations, and validation of the adequacy of actual PHR exchange between patients in a cloud-based PHR platform, is needed. However, different

views and opinions of various stakeholders such as hospitals and government agency, can cause the conflicts in data standardization which can be a limitation of the future study. Additionally, further studies on the interoperability of blockchain-based IoT devices between the proposed PHR platform and various medical devices is necessary [37]. This will facilitate the evolution of the proposed platform into a channel-type PHR platform linked with various healthcare stakeholders, such as hospitals, insurance companies, pharmacies, and medical device manufacturers.

References

[1] H. Kim, "Blockchain, Protection and Application of Medical Information," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 38 no. 7, pp. 25–31, Jul., 2020. Article (CrossRef Link)

[2] S. Woo, Y. Lee, and Y. Cho, "Issues in the Blockchain-Based Health Care Industry," in *Proc. of the Korean Institute of Information and Communication Sciences Conference*, Busan, Republic of Korea, pp. 363–366, 2019. Article (CrossRef Link)

[3] Y. Choi, W. Jeong, and C. Park, "A Blockchain-Based Access Control Method for Medical Data Sharing," *Journal of the Korean Institute of Industrial Engineers*, vol. 45, no. 6, pp. 503–513, Dec., 2019. Article (CrossRef Link)

[4] S. W. Oh, S. M. Park, and S. P. Hong, "A Case Study for the Safe Implementation of Blockchain: Focused on Hospital Information System," in *Proc. of Symposium of the Korean Institute of communications and Information Sciences*, Seoul, Republic of Korea, pp. 131–132, 2017. Article (CrossRef Link)

[5] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A Blockchain-Based Approach to Health Information Exchange Networks," *Computer Science*, 2016. Article (CrossRef Link)

[6] H. Kwon, H. Kim, and J. Choi, "A Blockchain Application for Personal health information: Focusing on Private Block Scheme," *Knowledge Management Research*, vol.19, no.4, pp.119–131, 2018. Article (CrossRef Link).

[7] J. Eberhardt and S. Tai, "On or Off the Blockchain? Insights on Off-Chaining Computation and Data," *Service-Oriented and Cloud Computing*, pp. 3-15, 2017. Article (CrossRef Link).

[8] Deloitte, "Blockchain: Opportunities for Health Care," 2016. Article (CrossRef Link)

[9] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. Teare, and K. Melham, "Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks," *European Journal of Human Genetics*, vol. 23, pp. 141–146, 2015. Article (CrossRef Link).

[10] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data," *MIT Media Lab publication*, August, 2016. Article (CrossRef Link)

[11] J. Moon and D. Kim, "Design of a Personal-Led Health Data Management Framework Based on Distributed Ledger," *The Journal of Society for e-Business Studies*, vol. 24, no. 3, pp.73–86, August 2019. Article (CrossRef Link).

[12] S. Y. Lee, K. H. Lee, and Y. B. Jeon, "A method of Improving Medical Data Management Protection Using Metadata and Blockchain," in *Proc. of Korea Information Processing Society Conference*, Seoul, Republic of Korea, pp.161–163, 2018. Article (CrossRef Link)

[13] L. A. Linn and M. B. Koo, "Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research," *Journal of Medical Internet Research*, March, 2019. Article (CrossRef Link)

[14] R. E. Choi, S. Y. Kim, S. J. Jang, J. H. Jeong, K. J. Won, A. R. Lee, and I. K. Kim, "Patient-centered Consent System for Using Healthcare Data Based on Blockchain Technology," in *Proc. of the Korea Software Congress 2020*, Seoul, Republic of Korea, pp. 1309–1311, 2020. Article (CrossRef Link)

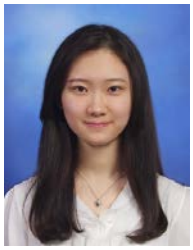
[15] K. H. Lee, "A Study on the type of BlockChain (Ethereum, Hyperledger Fabric)," in *Proc. of Symposium of the Korean Institute of communications and Information Sciences*, Seoul, Republic of Korea, pp. 442–443, 2018. Article (CrossRef Link)
[16] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008. Article (CrossRef Link)
[17] Z. Sukhbat and J. Choi, "Blockchain Technology Usage on Health Equity: Is Blockchain Technology a Panacea for Global Health Equity Issues?," *Knowledge Management Research*, vol.19, no.4, pp. 187–201, 2018. Article (CrossRef Link).
[18] https://101blockchains.com/blockchain-vs-database-the-difference/
[19] S. T. Manion and Y. Bizouati-Kennedy, *Blockchain for Medical Research: Accelerating Trust in Healthcare*, CA, USA: Productivity Press, 2020.
[20] V. Dhillon, J. Bass, M. Hooper, D. Metcalf, and A. Cahana, *Blockchain in Healthcare: Innovations that Empower Patients, Connect Professionals and Improve Care*, NJ, USA: Productivity Press, 2021.
[21] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk control," *Journal of Medical Systems*, 40(10), 218, 2016. Article (CrossRef Link).
[22] Y. Cho and S. Woo, "Block Chain Algorithm to Ensure Patient Anonymity," in *Proc. of Information and Communication Convergence Engineering Conference*, Busan, Republic of Korea, pp. 358-362, 2019. Article (CrossRef Link)
[23] T. Son, "Under the Revised Personal Information Protection Act, Whether Blockchain-Related Information are Personal Information," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 38, no. 7, pp. 40–43, July, 2020. Article (CrossRef Link)
[24] J. Lee, J. Kim, C. Kim, and J. Yang, "Research and Implementation of Mutual Trust System for Consent to Use Personal Information Based on Blockchain," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 45, no. 8, pp. 1342–1354, August, 2018. Article (CrossRef Link).
[25] R. Layton and S. Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices," in *Proc. of 2019 12th CMI IEEE, Copenhagen*, Denmark, pp. 1–6, 2019. Article (CrossRef Link).
[26] G. Kennedy, *Data Privacy Law: A Practical Guide to the GDPR*, NJ, USA: Bowker, 2019.
[27] H. W. Yu, E. Lee, W. Kho, H. Han, and H. W. Han, "Blockchain Technology for Healthcare Big Data," *The Journal of Bigdata*, vol. 3, no. 1, pp. 73–82, August, 2018. Article (CrossRef Link)
[28] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *Proc. of 2016 2nd International Conference on Open and Big Data, Vienna*, Austria, August, pp. 25–30, 2016. Article (CrossRef Link)
[29] M. Kwon, R. Myung, and H. Yu, "Performance Analysis of Execution and Ordering Phases of Hyperledger Fabric," in *Proc. of the Korea Information Processing Society Conference*, Seoul, Republic of Korea, pp. 62–64, 2019. Article (CrossRef Link)
[30] Y. Choi and K. Kim, "Secure Healthcare Data Management and Sharing Platform Based on Hyperledger Fabric," *Journal of Internet Computing and Services*, vol. 21 no. 1, pp. 95–102, 2020. Article (CrossRef Link)
[31] H. H. Han, "Authentication for Blockchain Service," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 38, no. 7, pp.19–24, July, 2020. Article (CrossRef Link).
[32] N. Gaur, A. O'Dowd, P. Novotny, L. Desrosiers, V. Ramakrishna, and S. A. Baset, *Blockchain with Hyperledger Fabric: Build decentralized applications using Hyperledger Fabric 2*, Birmingham, UK: Packt Publishing, 2020.
[33] M. Zand, X. B. Wu, M. A. Morris, *Hands-On Smart Contract Development with Hyperledger Fabric V2: Building Enterprise Blockchain Applications*, CA. USA: O'Reilly Media, 2021.
[34] https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html
[35] B. Min, "An Improvement of Hyperledger Fabric Raft Algorithm toward Enhancing Availability," *The Journal of KING Computing*, vol. 17, no. 2, pp. 80–91, Apr., 2021. Article (CrossRef Link)
[36] https://kosis.kr/statHtml/statHtml.do?orgId=117&tblId=DT_117030_001

[37] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park, "Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks," *Human-centric Computing and Information Sciences*, vol. 11, no. 21, May, 2021. Article (CrossRef Link)

Heongkyun Kim received M.S. in Electronic Engineering from Yonsei University, Republic of Korea, in 1995. He is currently working as executive director and head of the research center of VTW and an adjunct professor in the Graduate school of Engineering at the Hanyang University since 2009 and the Division of Industrial Convergence since 2016. He has about 30 years of IT and business strategy consulting experience in public and private sectors such as government-industry, public institutions, finance, medical health care, manufacturing, logistics, and university. His research interests are Information System Architecture, Software Engineering Consulting, and the application of CRM/SCM solutions.

Sangmin Lee received a Ph.D. in Engineering Management, a M.S. in Computer Science from the George Washington University, and a B.S. in Computer Science from Indiana State University. He is an assistant professor of School of Business Administration and Data Science at CHA University, Pocheon, Korea. Prior to joining CHA University, he served as an assistant professor at the School of Business at Soongsil University, Seoul, Korea. His current research interest includes big data analysis, business intelligence, fintech, and application of blockchain technology.

Hyunwoo Kwon received A.E. in Information and Communication from Inha Technical College in 2013 and B.E. in Information and Communication Engineering from Academic Credit Bank System in 2016, both in the Republic of Korea. He is currently working in VTW with his research interests in Software Engineering, Medical Information Management, and Blockchain Technology.



Eunmin Kim received B.E. in Data Analytics from Kangwon National University, Republic of Korea, in 2019. She is currently working as a web developer in the research center of VTW with her research interests in Software Engineering, Medical Information Management, and Computer/System Architecture.