Blockchain-based Medical Information Sharing Service Architecture

Sang Young Lee

Namseoul University, South Korea
sylee@nau.ac.kr

Abstract

Blockchain technology is a distributed database, which is a Ledger technology that records changes, for example, adding information, revising, and deleting in the unit of blocks and share. Here, the ledger means a list of transactions, but Blockchain technology can be applied to all data if it is interpreted as shared information. This paper proposed a method of applying Blockchain technology in the medical field and using it in PHR applications. That is, architecture is proposed for a gateway application of healthcare data for easy and safe control and sharing of PHR data. If Blockchain technology is applied to PHR service in this way, it may affect a distributed database that provides saving and backup/restore functions for medical information by transmitting/saving medical information to each existing base medical institution. Through this, the Blockchain Server for each participating base of the Blockchain Network can serve as an Interface for utilizing medical information along with medical information saving.

Keywords: Blockchain, Medical, Information sharing

1. Introduction

As interest in the medical environment is increasing, the demand for medical services is also increasing. Therefore, the establishment of a foundation for the development of medical services became the center of attention, and the medical information sharing business has started. Since medical information system has been converted into EMR, health information has been created and distributed by non-medical personnel because interest in health care is increasing and the expansion of Smart Device [1].

Generally, Blockchain technology is a distributed database, which is a Ledger technology that records changes, for example, adding information, revising, and deleting in the unit of blocks and share. Here, the ledger means a list of transactions, but Blockchain technology can be applied to all data if it is interpreted as shared information [2][3].

In general, security becomes a great concern when using cloud computing. Especially medical institutions use a remote cloud base to manage and protect sensitive and confidential data related to personal medical care on basis of cloud services. Therefore, the stability of companies that manage hospital data is very important in terms of security. Not only that, patients may feel uncomfortable giving their medical data to third parties. This means medical institutions are obliged to protect data from unauthorized users by selecting a reliable cloud service provider. The verification of security and proven performance analysis is more important than efficiency in a cloud computing environment [4][5].

With the platform centrally managed PHR, a patient can retrieve medical information and share it with his/her doctor. In addition, the patient can edit and store medical information, insurance-related information, medical records, etc. with the computer at his home. To be specific, it can be used to input user's PHR, provide health information relating to PHR (symptoms, causes, and treatments), upload PHR information via medical institutes, check drug interactions, search doctors/hospitals, and so on [8][9][10].
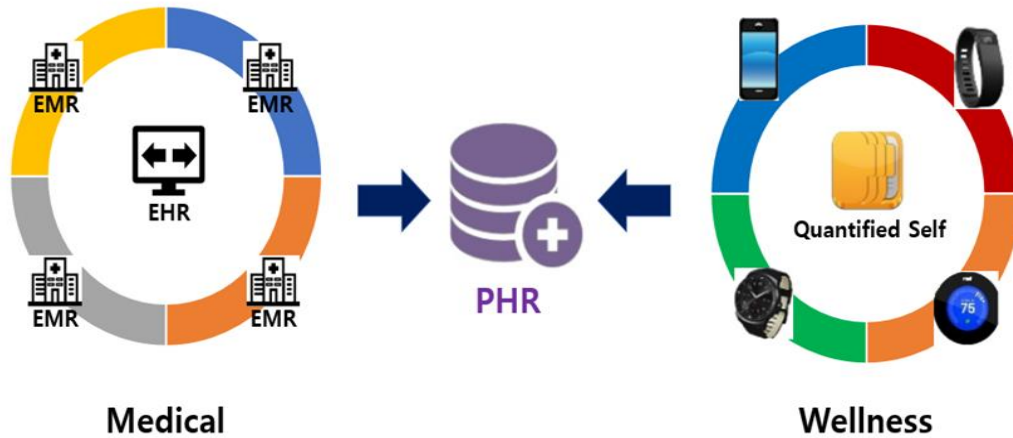

Figure 1. Structures of PHR

PHR covers all information related to personal health. And it is a concept that includes personal health care services, personal health information, and personal health management platform overall. EMR is a medical information system created and used within a single medical institution, and EHR is a medical information system that complies with national standards for interoperability and is used by multiple medical institutions. The personal medical information saved in the EMR and EHR becomes the important basis of PHR. PHR has developed from an early model which confirms easily personal health information scattered across various institutions and devices that are integrated, and sharing [6][7].

And now, it is developing into a model that provides useful services such as self-health care, disease, medical institutions, disease prevention related to insurance companies, and follow-up management. Soon, specialized information such as social networking, behavior habits, and extra will be added not only genetic information, analyzing a new health indicator, and offering personalized disease prevention health care. This paper is to offer how-to apply Blockchain technology in the medical site and how to use it in PHR applications. We provided an architecture for a gateway application of healthcare data for easy and safe control and sharing of PHR data.

2. Related works

Medical information that was recorded by the hand of medical personnel in the past has been converted to EMR (Electronic Medical Record) with the introduction of an information system. As interest in personal health increased, the concept of medical information is changed into EHR (Electronic Health Record), and recently, its scope has expanded to PHR (Personal Health Record) with the spread of Wearable Devices, IoT, and Smart Devices [8, 9]. As the number of the population increased, medical personnel and the amount of medical

information is increased naturally. The data quality of medical information is demanded to increase the use of medical information that has been greatly increased, and international standards for medical information such as DICOM (Digital Imaging and Communications in Medicine) and HL7 (Health Level 7) have been applied accordingly [10][11].

Now it became possible to exchange and share medical information among various institutions such as hospitals, medical research institutions, and legal institutions. As interest in such a medical environment increases, the demand for the development of medical services is soaring. Therefore, the establishment of a foundation for the development of medical services is emphasized and various studies on medical information have been conducted [12].

Blockchain is a data structure, which is composed of blocklists connected with chains. Such blockchain is distributed through peer-to-peer (P2P) networks with the latest version of all nodes. The block is a record of transaction data. Blockchain-based on Bitcoin is one of the distributed ledger technologies, which is a distributed, shared, and encrypted database that serves as an "irreversible and incorruptible repository of information". The block includes the header and body.

Blockchain is a data structure, which is composed of blacklists connected with chains. Such blockchain is distributed through peer-to-peer (P2P) networks with the latest version of all nodes. The block is a record of transaction data. Blockchain-based on Bitcoin is one of the distributed ledger technologies, which is a distributed, shared, and encrypted database that serves as an "irreversible and incorruptible repository of information". The block includes the header and body [11][12].

3. Medical information sharing

Personal Health Record (PHR) has been introduced as a patient-centered health information model. Through these PHR services, patients can create, manage and control their health data in one place. This means they can manage data through efficient tools for saving, retrieving, and sharing medical information.

The PHR allows patients to control their medical records and share their health data with various users.

In recent years, various IoT devices such as wearable devices, for example, activity tracker or heart rate measurement, and sleep motoring device or smart home devices have been introduced, and it is expected that IoT personal's will be actively discussing PHR-related health care standard in the future. Unlike the current system that uses EHR for management centered on providers, PHR can manage data centered on patients. In other words, it is an application that patients use. The concept that data owners access and manage their health information.

(a) Data access control.

(b) Know the source of the collected data.

(c) Notify when a provider accesses data.

(d) It is always transparent to the patient through the data log.

(e) Patients can search for health information anytime, anywhere.

In other words, PHR is defined as an Internet-based tool that allows individuals to access their lifelong health information, and people who need specific information can use it. Medical service users can make better decisions, access information necessary for treatment,

and effectively communicate between patients and medical personals through PHR, thereby it can improve the quality of medical care.

The order of sharing medical information based on Blockchain is as follows. Creating Block, transmission, receiving block verification, and saving for the medical information to be shared. In the case of applying Blockchain to a specific information service, the subject which created or changed information makes Block that the information to be shared. It is transmitted to all nodes that participated in the Blockchain Network. And the node on the Blockchain Network verifies the transmitted information block.

After that, a normal block shares information transmitted by senders in the way of registering and saving in Chain. Chain information saved in a specific node on the Blockchain Network can be forged by an attack of an unauthorized person. However, Blockchain Network applies the principles of PoS (Proof of Stake, Proof of Ownership) and PoW (Proof of Work, Proof of Work), Forged Blocks or Chains in one Node are rejected. To apply forgery of specific information to the entire Blockchain Network, chain information saved in all nodes must be simultaneously forged but this is practically impossible.

It is evaluated that Blockchain technology can satisfy the integrity of shared information through the mechanism, The method of modifying and processing information on the Blockchain is continuously added without deleting or modifying Block. These features allow for information-specific Life-Cycle tracking with Chain Management technology alone, without the need to implement Version management.
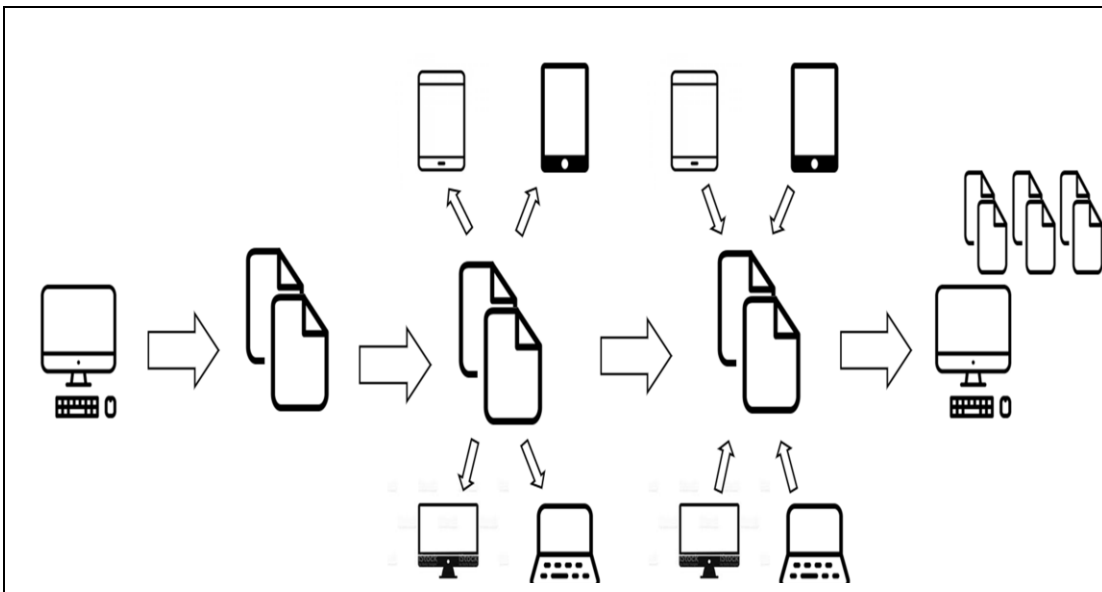

Figure 3. Medical information sharing

4. Architecture with blockchain platform

As medical information includes personal information, there are many kinds of security requirements, not only patient records. Reliability, integrity, and traceability should be guaranteed along with confidentiality to prevent leakage of personal information.

Currently, HL7 and DICOM present security requirements as shown in the table below. It is a security measures standard for each layer of medical information. The security threats and security requirements for medical information written above are as follows. Shortly, medical

information should have the reliability of medical information for the entire life-cycle of its creation, saving, transmission, and shredding.

And medical information requires comprehensive security features such as user certification, rights to management, confidentiality, integrity, traceability, and non-repudiation. A medical information sharing service that is used in various fields should satisfy all of the previously identified security requirements as a basis for medical service development. This study suggests Private Blockchain to the current medical information sharing service including Life-Cycle of medical information, security requirements, the current medical information sharing technology, and the research and efforts.

The blockchain-based medical information sharing service structure is shown in the [Figure 4].
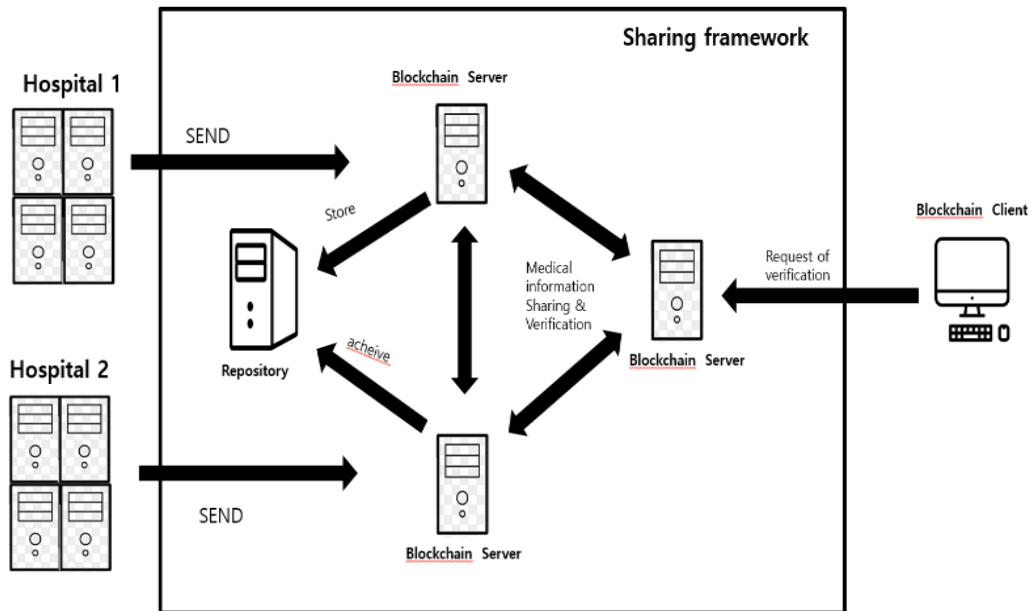

Figure 4. Blockchain-based medical information sharing service

5. Conclusions

This paper proposed a method of applying Blockchain technology in the medical field and using it in PHR applications. That is, an architecture is proposed for a gateway application of healthcare data for easy and safe control and sharing of PHR data.

If Blockchain technology is applied to PHR service in this way, it may affect a distributed database that provides saving and backup/restore functions for medical information by transmitting/saving medical information to each existing base medical institution. Through this, the Blockchain Server for each participating base of the Blockchain Network can serve as an Interface for utilizing medical information along with medical information saving. The chain also manages access, processing, and disposal regarding medical information, providing verification and inspection of medical information along with maintaining the integrity of medical information and satisfying the previously recorded security requirements

Acknowledgments

References

[1] Information Security Reference Model for u-Health Service, TTA Standards, Dec., **(2010)**

[2] M. Kratz, P. Humenn, M. Tucker, M. Nolte, S. Wagner, G. Seppala, G. Shadrow, W. Wilson, and S. Auton, "Health level seven security services framework," HL7 Security Group, July

[3] National Electrical Manufacturers Association, Part 8: Network Communication Support for Message Exchange, DICOM PS3.8 2015b, Mar., pp.23, **(2007)**

[4] HIPAA, Security Series, HIPAA, Mar., **(2007)**

[5] A. J. Van Dierendonck and B. Arbesser-Rastburg, "Measuring ionospheric scintillation in the equatorial Region over Africa, including measurements from SBAS geostationary satellite signals," Proc. ION GNSS, Long Beach, CA, Sept., **(2004)**

[6] W. Pelgrum, Y. Morton, F. van Graas, P. Vikram, and S. Peng, "Multi-domain analysis of the impact on natural and man-made ionosphere scintillations on GNSS signal propagation," Proc. ION GNSS, Portland, OR, Sept., **(2011)**

[7] S. Gunawardena, Z. Zhu, F. van Graas, "Triple frequency RF front-end for GNSS Instrumentation Receiver Applications," Proc. ION GNSS, Savana, GA, Sept., **(2008)**

[8] S. Peng and Y. Morton, "A USRP2-based multi-constellation and multi-frequency GNSS software receiver for ionosphere scintillation studies," Proc. ION ITM, San Diego, CA, Jan., **(2010)**

[9] P. Vikram, "Event driven data collection system for studying ionosphere scintillation," MS thesis, Miami University, **(2011)**

[10] T. Humphreys, M. Psiaki, P. Kintner, and B. Ledvina, "GPS carrier tracking loop performance in the presence of ionospheric scintillations", ION GNSS Long Beach CA, pp.156-167, Sept., **(2005)**

[11] D. Xu and Y. T. Morton, "A semi-open loop GNSS carrier tracking algorithm for monitoring strong equatorial scintillation", IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 2, pp.722-738, Apr., **(2018)**

[12] C. L. Rino, "The theory of scintillation with applications in remote sensing," Hoboken, NJ: IEEE and Wiley, **(2011)**

Authors

Sang Young Lee

Professor (Namseoul University)