International Journal of Advanced Research in Big Data Management System
Vol.3, No.2 (2019), pp.31-36
http://dx.doi.org/10.21742/ ijarbms.2019.3.2.05

# Blockchain-based Framework for Medical Data Management

Sang Young Lee

*Namseoul University, Korea*
*sylee@nsu.ac.kr*

## *Abstract*

*The advantage of introducing blockchain is that it can deliver data to members while maintaining the security of medical data sensitive to personal privacy. That is, by using a blockchain in the ecosystem of medical information, it is possible to connect the insurer, the health care organization, and the patient. The blockchain provides health data efficiently and increases accuracy and efficiency when changing patient data through the health system. In addition, it improves the efficiency and control of medical environment paradigm and health services. This paper suggested the framework with functions to support clinical decision making more efficiently using blockchain technology and FHIR data standards. This framework is built on the FHIR, which is designed to be provided to patients. In addition, it complements and uses open key encryption technology and meets the key requirements required in interoperability functions, such as user identification/authentication, secure data exchange, and authorized data. In particular, it provides further secure data exchange method aiming access guarantee, consistent data format and system modularity.*

***Keywords:*** *blockchain, framework, Medical data, Management*

## 1. Introduction

The application of technologies that can be specialized in the medical field, such as blockchains, is being studied. In other words, multiple peers validate and store each other's data over the network [1][2]. Therefore, it is a storage platform designed to make it difficult for other people to manipulate their data. One block that makes up this blockchain consists of a Header and a Body [3].

Where the header consists of the Hash value that connects the previous block to the next block and Nonce, a random number, associated with encryption. The body also records transactions by trade, and peers in the blockchain can verify the data using the hash values here. This is named blockchain because of the structural shape in which the blocks are linked between the previous block's hash value and the current block's hash value [4].

The biggest advantage of introducing blockchain is that it can deliver data to members while maintaining the security of medical data sensitive to personal privacy. That is, by using a blockchain in the ecosystem of medical information, it is possible to connect the insurer, the health care organization, and the patient. The blockchain provides health data efficiently and increases accuracy and efficiency when changing patient data through the health system. In

**Article history:**
Received (July 29, 2019), Review Result (September 16, 2019), Accepted (November 3, 2019)

Print ISSN: 2208-1674, eISSN: 2208-1682 IJARBMS

addition, it improves the efficiency and control of patients' personal health data and increases the price transparency of pharmaceuticals and health services.

## 2. Related works

Blockchain technology is a standard that enables personalized health in health care systems and has the potential to address the problem of interoperability that enable health providers and medical researchers to securely share health data electronically [5][6]. Meantime, several studies have been carried out in this respect. These studies have been proposed to solve the ownership problem of individual medical and health information by using the blockchain technology [7]. In particular, blockchain technology has been recognized as one of the various ICT technologies for the transition of medical environment paradigm to personal customized health care. That is, the blockchain technology is being used as an effective alternative to protect the patient's data in the medical field. In addition, several researchers have studying to be used to support the data management in various medical applications.

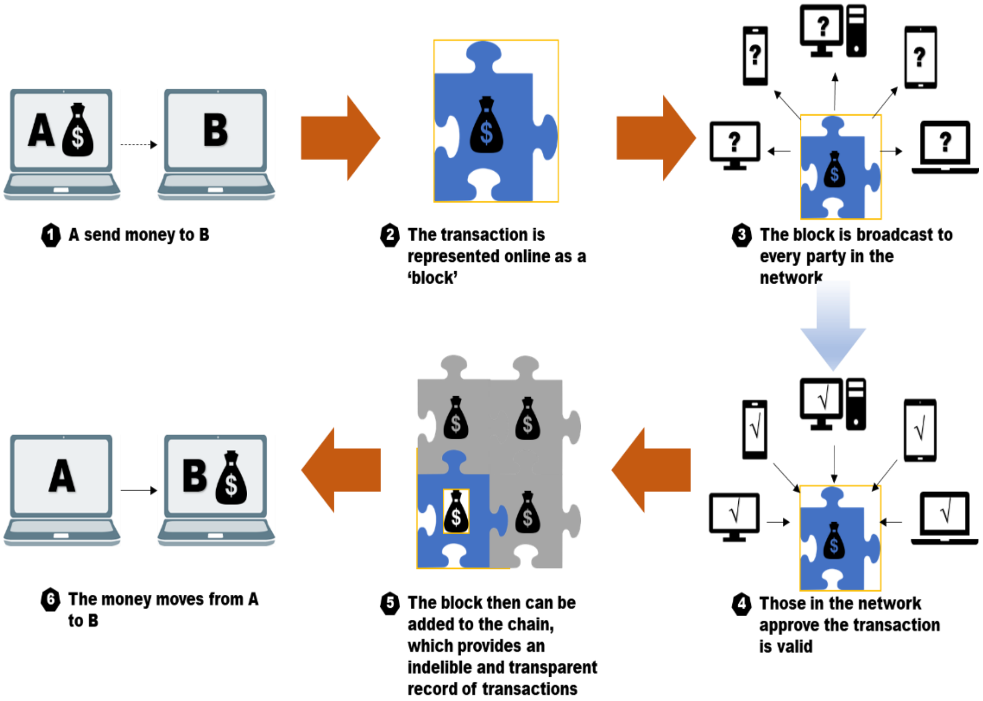
A
B
❶ A send money to B
❷ The transaction is represented online as a 'block'
❸ The block is broadcast to every party in the network
❹ Those in the network approve the transaction is valid
❺ The block then can be added to the chain, which provides an indelible and transparent record of transactions
❻ The money moves from A to B

Figure 1. Blockchain of medical environment.

## 3. Healthcare interoperability

In particular, FHIR is a standard framework that defines common methods for addressing problem of healthcare information sharing and defines resources that can be used in various environments. In other words, it was developed to support paths that could interact with existing standard transmission models.

FHIR provides improved functions compared to v2, v3, and CDA which are existing standard transport models. These improved functions include: First, since FHIR is focused on implementation, the developers can use it easily and simple. Second, the FHIR supports an execution library and numerous available cases to speed up development. Third, FHIR utilizes resource-based interoperability. For example, for the management of patients with hypertension, a chronic disease, only three resources are available for exchange and treatment: blood pressure measurement information (Observation), patient information (Patient), and blood pressure system information (Device). Fourth, since they are doing mapping work with the data types of the existing reference standard HL7 v2 and the reference information model, they can coexist in the same environment. Fifth, it expresses the clinical documents received by the medical worker to facilitate understand through summary of patient information. And the resources of the FHIR are available at any time as an open source. The environment for sharing and exchanging health information is extensive, including Social Media on Mobile phones, Cloud Communications, Electronic Health Record System, and Personal Health records. Social Media can identify patients by external identification and patients' records connections or logins through Google, Facebook and open IDs, and logins restrict access to security and patient records through standardized authentication methods. One general method to integrate medical information from various resources is to create space to store patient records.

These standards are prepared and managed by Health Level Seven International (HL7 by the Health Standards Organization). The FHIR is licensed without restrictions or royalty requirements, which serves to promote broader adoption. In particular, FHIR users provide the improved mobile and cloud-based application utilization, integration of medical devices, and flexible/customized opportunities for healthcare workers. Using the FHIR can separate HER data elements. It also has two kinds of resource types; identifiers (suppliers and patients) and general clinical activities. These partitioned resource configurations of FHIR facilitates the transmission of EHR data in appropriate. In addition, the FHIR resource follows the Representational State Transfer (ReST) principle and allows for verification of the structural suitability of the standard and can be added by an additional conformity declaration called a profile.

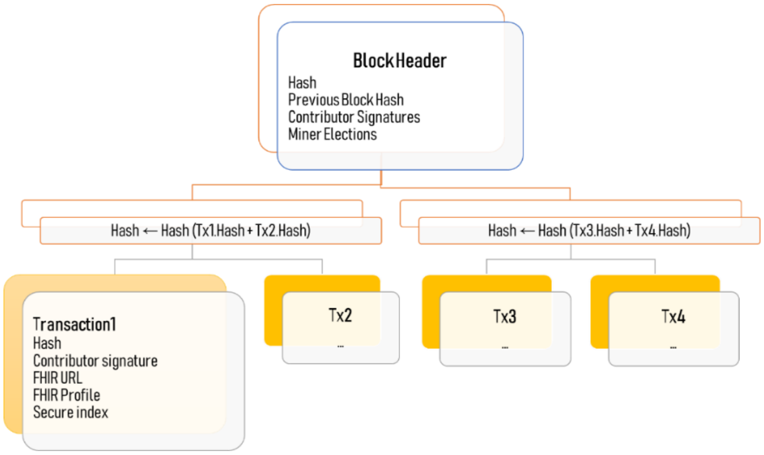

Figure 2. Example of a healthcare blockchain structure reflecting FHIR

In this paper, blockchain technology applied can be used as an alternative to meet the requirements of existing standards, while supplementing rather than replacing the FHIR system. Because blockchain is not yet sufficient to store and distribute all medical and health-related information. Because it is difficult to store large image information, such as X-rays and MRIs directly, and it is also dangerous if Personal Identification Information (PII) is publicly exposed. In order to address these problems, two types of information storage methods are used: 'On-Chain' data that stores information directly in the blockchain and 'Off-Chain' data that uses links stored in the blockchain as a pointer for information stored in a separate traditional database.

## 4. Blockchain-based architecture for clinical data sharing

The following [Figure 3] shows the architecture presented to address the needs of the medical sector. This architecture enables application in a wide range of health IT systems. In addition, it can be applied to distributed mobile systems that support decision making on joint treatment (cooperative treatment) in remote health care.

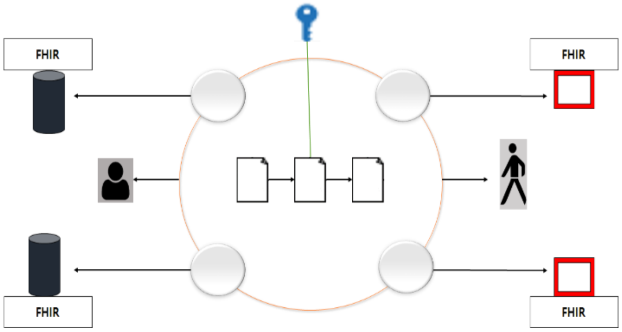

Figure 3. Architectural components in healthcare blockchain

In [Figure 3], the central ellipse represents a blockchain that supports data sharing among collaborative health care professionals. Clinical data used here can be linked and operated with different types of databases. The architecture also utilizes the FHIR standard and use the common structure that shared data has. In this structure, a secure database connector is connected to the blockchain. Here, it has a blocked data source that only authorized entities can be obtained. And the secure tokens are recorded in the smart contract document (display as linked document) for distributed access and traceability. This smart access allows to store/exchanges secure access tokens and maintain transaction logs of events that use tokens. These logs record specific information about what access right was granted to the user, which token was used to access the resource, and so on. In other words, this architecture ensures that all shared data is approved by authorized clinicians and health care organization only to ensure the validity of all shared data [5][6].

This architecture has the following technical requirements;

First, it is the requirements for authenticating. In here, the verifying identity and all peer's contexts are authenticated. That is, the blockchain provides an anonymous personal account (an open address consisting of random hash values) for the user to process the cryptogram. However, these unique IDs do not address all peer's identifiability or requirements for authenticating. Basically, the blockchain can be accessed by anyone who can access the Internet. Since users can have multiple blockchain accounts, minimizing the identifiability of the account owner. However, these requirements should be able to identify all health care person concerned and require traceable users that are completely different from the unique ID of the blockchain. That is, these functions define the identity of the medical user involved in the sharing of clinical data and protect important personal information in the blockchain.

Second, it is the requirements for storing and exchaing. In here, data is stored and exchanged safely. The key function provided by blockchain is that it also supports transactions between parties that do not have trust relationships. Since the blockchains are peer-to-peer in nature, they support the ubiquitous of digital assets traded. Third, it has access right. It is a right that is accessible to data source context. Data references are performed by blockchains for access to multiple paths. However, access rights should only be granted to providers authorized to view data.

to another supplier. In this architecture, they make a digital sign on the sharing content. And encrypt the document with the provider's private signature key and the public encryption key. And then, after obtaining an encrypted token, make a smart contract for access to the document. This digital signature process ensures that the provider actually shares the resources and does not tamper. It protects documents from unauthorized access. These authorities can be implemented by connecting in the same way as a traditional centralized system. In this case, a meta-encryption key pair is created for the properties and stored securely in the system database. Users who meet certain authority criteria allow to use the key when accessing data while protecting users from non-critical details.

Forth, it is a consistent data formats/context. Clinical data may exist in a various formats and structures, but may or may not be meaningful when shared with other providers. Fifth, it is a maintenance of module method. In here, design patterns apply to MVC (Model-View-Controller) model.

MVC patterns divide the system into three components: (1) Models: Manage the behavior and data of the system and respond to requests (2) View: Information on status and status change instructions, (3) Controller: Manage information displays, and deliver user input to view or model.

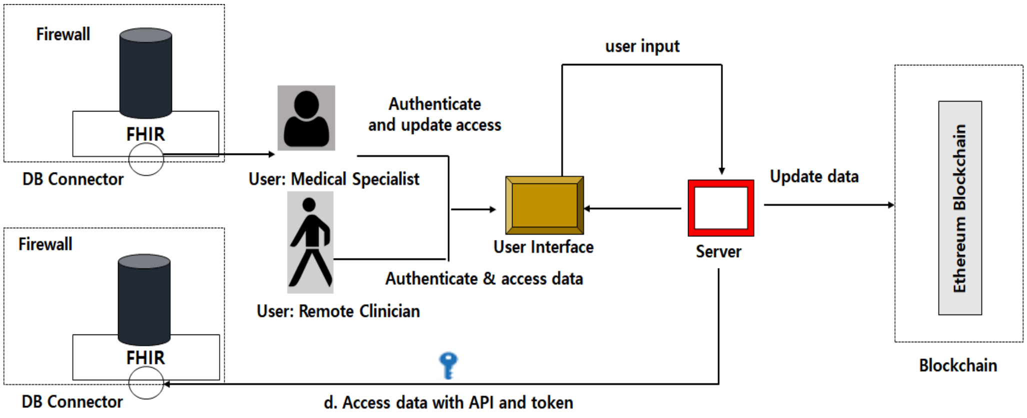

Figure 4. Extended framework

This architecture applies these MVC patterns to individual context. (1) Allow to store the required metadata through a model in the form of non-changeable blockchain components. (2) Views provide a front-end user interface that accepts user input and provides data. (3) The controller facilitates interaction with the data between the user interface and the blockchain components. (4) The Controller Call Data Connector Service is used to verify the implementation of the FHIR standard and to create a reference pointer for the data source upon request from the server.

This architecture separates the rest parts of the system and the data store by storing healthcare-related information in smart contracts. This decoupling has the advantage of enabling future upgrades to other components without losing access right to existing users or authority information. Figure 4 shows the form of this extended framework

## 5. Conclusion

This paper has suggested the framework with functions to support clinical decision making more efficiently using blockchain technology and FHIR data standards. This framework is built on the FHIR, which is designed to be provided to patients. In addition, it complements and uses open key encryption technology and meets the key requirements required in interoperability functions, such as user identification/authentication, secure data exchange, and authorized data. In particular, it provides further secure data exchange method aiming access guarantee, consistent data format and system modularity.

## Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (2017R1D1A1B03027873)

## References

[1] Zapata B. C., Fernández-alemán J. L., Toval A., and Idri A., “Reusable software usability specifications for mHealth applications,” J. Med. Syst, vol.42, pp.1-9, **(2017)** DOI: 10.1007/s10916-018-0902-0

[2] Imtiaz S. A., Krishnaiah S., Yadav S. K., Bharath B., and Ramani R. V., “Benefits of an android based tablet application in primary screening for eye diseases in a rural population,” India J. Med. Syst. vol.41, no.4, pp.49, **(2017)** DOI: 10.1007/s10916-017-0695-6

[3] Elhoseny M., Abdelaziz A., Salama A. S., Riad A. M., Muhammad K., and Sangaiah A. K., “A hybrid model of internet of things and cloud computing to manage big data in health services applications,” Futur. Gener. Comput. Syst., vol.86, pp.1383-1394, **(2018)** DOI: 10.1016/j.future.2018.03.005

[4] Puthal D., Malik N., Mohanty S. P., Kougianos E., and Yang C., “The blockchain as a decentralized security framework,” IEEE Consumer Electronics Magazine, vol.7, no.2, pp.18-21, **(2018)** DOI: 10.1109/MCE.2017.2776459

[5] Ma Y.and Sharbaf M. S., “Investigation of static and dynamic android anti-virus strategies,” In: 10th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, pp.398-403, **(2013)** DOI: 10.1109/ITNG.2013.62

[6] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and IoT integration: A systematic survey,” Sensors, vol.18, no.8, pp.2575, **(2018)** DOI: 10.3390/s18082575

[7] T. Neudecker and H. Hartenstein, “Network layer aspects of permissionless blockchains,” IEEE Communications Surveys & Tutorials, **(2018)** DOI: 10.1109/COMST.2018.2852480

## Authors

**Sang Young Lee**
Professor (Namseoul University)