International Journal of Innovative
Computing, Information and Control
Volume **16**, Number **3**, June **2020**

 ISSN 1349-4198
pp. 1117–1124

DESIGN AND IMPLEMENTATION OF DISTRIBUTED LEDGER BASED HEALTH DATA MANAGEMENT SYSTEM

Junho Moon and Dongsoo Kim*

Department of Industrial and Information Systems Engineering
Soongsil University
369 Sangdo-ro, Dongjak-gu, Seoul 06978, Korea
jhmoon@soongsil.ac.kr; *Corresponding author: dskim@ssu.ac.kr

Received December 2019; revised March 2020

Abstract. *In this paper, we propose a new health data management system based on distributed ledger. The Personal Health Record (PHR) systems are the most developed technology for a person to manage his or her own health data. The PHR systems have technical and legal problems despite rapid technological advances. It is technically very difficult to integrate and standardize dispersed data. In addition, there are many legal limitations because health data is very sensitive. Therefore, the PHR systems have attempted to solve these problems using blockchain. However, these attempts do not solve all problems. Personal health data is still dispersed, and in some countries it is not legally permitted to record health data in a blockchain. In most countries, individuals have a right to store their own health data. The proposed system stores health data in the device of each information subject participating in health data generation processes. The proposed system also makes the individual user's device a member of the network. Users can utilize the data as if they were using the data on a single system.*
Keywords: Personal health record, Blockchain, R3 Corda, Distributed ledger

1. **Introduction.** The Personal Health Record (PHR) systems have been developed as a core technology for personal health care for many years [1,2]. In recent years, the PHR systems have evolved into interconnected-PHR forms that integrate and manage various types of health data. In addition, they not only store data, but also analyze the collected health data to provide health services [3]. However, the PHR systems using a centralized database have some problems, such as the difficulty in collecting scattered health information, standard mismatch between groups, risk of data forgery and modulation, risk of data security, and lack of data utilization [4].

Therefore, companies such as MedRec, GemHealth, Health Bank and MediBloc have adopted blockchain technology to solve problems in their PHR systems. There are two ways to apply blockchain technology to information systems: On-chain and Off-chain. Most companies and researchers are applying blockchains in Off-chain type to PHR systems. Off-chain type PHR systems do not store data directly in the blockchain. They store the access path, authority, and access history of data in the blockchain. Blockchain based PHR systems enable health data from distributed medical institutions to act as a single system [5,6].

However, blockchain based PHR systems have problems. First, the use of Off-chain method can detect forgery and modulation of data. However, it cannot restore the original value. Second, security issues of the blockchain are constantly being raised. Blockchain security issues can cause a large amount of data leakage. Third, block mining costs are

DOI: 10.24507/ijicic.16.03.1117

high. The proof of work of the blockchain requires a large amount of computer equipment and electric power. Fourth, personal health data is not wholly owned by the data subject. The data of blockchain system is not stored on the device of the data subject. Fifth, blockchain based PHR systems have the risk of losing user data due to loss of private key. Finally, storing health information in a blockchain network can be a legal issue in many countries. Health data is very sensitive data. Therefore, many countries have strict legal control. In Korea, health data cannot be kept outside of owners, medical institutions, and authorized government agencies.

Therefore, in this paper, we propose a new health data management system based on distributed ledger. This system allows health data subjects and medical institutions to store and manage the same data together. In addition, this system promotes user participation by distributing the profits of using health data to users.

The remainder of this paper is organized as follows. Section 2 describes the techniques used to implement the proposed system. Section 3 presents the design goals and the conceptual design model of the proposed system. Section 4 shows the implemented system, and finally Section 5 offers conclusions of this study.

2. Related Work.

2.1. R3 Corda.

R3 Corda is one of the consortium blockchains. Figure 1 shows some of the key concepts of R3 Corda. As shown in Figure 1(b), Corda does not store data in all nodes, unlike other blockchain techniques. It stores data only on nodes participating in data generation. Figure 1(c) shows Corda's data consensus process. The consensus of the data is made by agreement between participants in data generation. In addition, the Notary function in Figure 1(d) verifies the data [7].

These features are suitable for development of the proposed systems. However, the proposed system cannot be fully implemented in Corda. First, all nodes in the Corda must have static IP as shown in Figure 1(a). The nodes of proposed system cannot have a static IP, because they work on personal mobile devices. Second, the Web Application

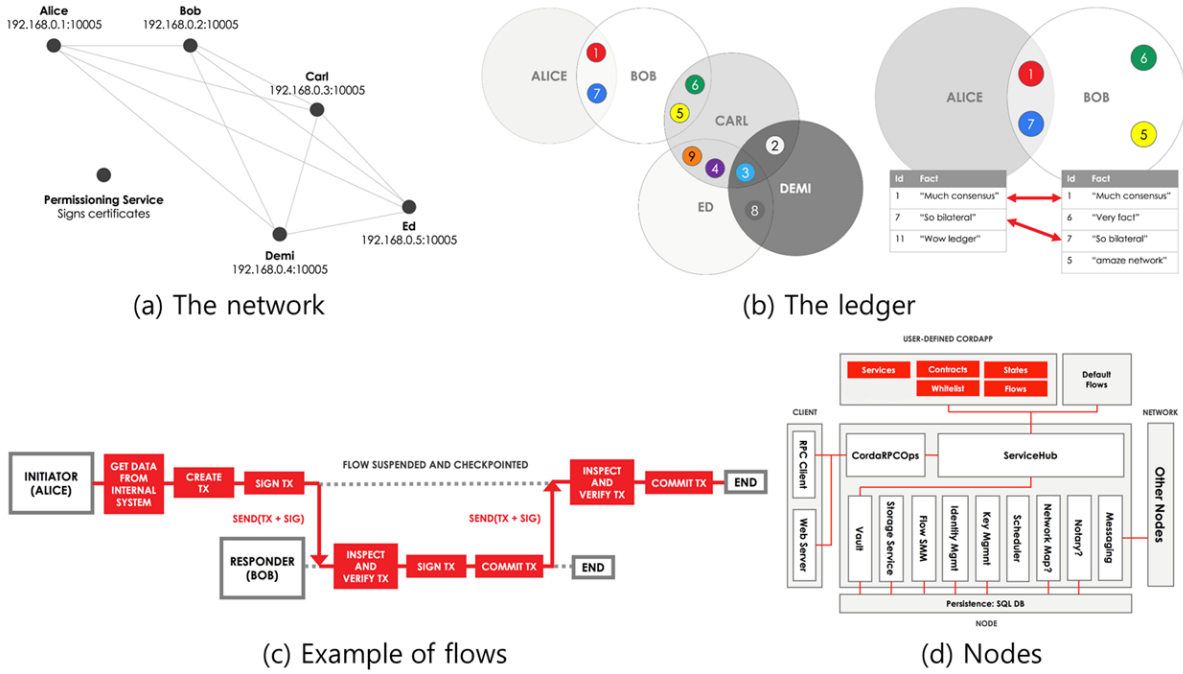


FIGURE 1. Key concepts of R3 Corda

Server must be installed on all nodes for Corda to work. It also cannot be installed on personal mobile devices. Third, the Corda is a system developed for the financial industry. Therefore, all nodes are in the format of Figure 1(d). However, in the proposed system, it is necessary to delete unnecessary functions or add new functions. Therefore, in this study, we designed a new framework that can achieve the goal of the proposed system by referring to the basic structure of Corda.

The existing blockchain based PHR systems store the health data on the devices of medical institution or PHR provider. However, the proposed system is designed to work with personal mobile devices based on the Corda architecture. This allows the data subject to store the data directly. The existing systems share data (Health data access path, authority, history) stored in a blockchain by all participants. Although this data is encrypted, there is a risk that a large amount of data will be leaked due to system failure or hacking. The proposed system minimizes data leakage because the data is distributed across multiple devices and the data is shared only with members participating in the state data generation process.

2.2. **Firebase cloud messaging.** The proposed system works on personal mobile devices. The typical information systems are a form of communication between a web server using static IP and a client application of many users. The client accesses the logical location (Static IP) of the server and requests information. However, it is difficult for the server to call the client. Most clients do not have a static IP, so the client must continue to detect the server. This is an inefficient way. In addition, this does not allow direct communication between clients. Therefore, a typical messenger program uses a separate messaging server.

We refer to the messaging program as a communication method for using a personal mobile device as a node in the network. Firebase Cloud Messaging (FCM) is a messaging service provided by Google. This allows users to communicate directly between clients without having to build a separate messaging server. The FCM issues an instance token to the device and it identifies individual devices based on this token. The issued token becomes the path to access the mobile device, such as the logical address of the server [8].

One of the key concepts of this study is to store and share data on the devices of personal users. To do this, it should be based on an easy and frequently used device by the personal user. Therefore, we designed this system based on a personal user's smartphone. However, a smartphone cannot work like a server. Therefore, this system uses the FCM function. FCM allows smart phones to receive external messages like a server. This allows personal users' smartphones to be used as participants in the distributed ledger network.

3. Architecture of Health Data Management System.

3.1. **Goals of framework.** The goals of the proposed framework are as follows. First, it allows the data subject to store health data directly. Second, it ensures the reliability and integrity of the information. Third, it creates a network between information subjects and health data control institute. Fourth, it enables secure data transmission among network members. Fifth, it prevents data forgery and modulation and it enables recovery of lost data. Sixth, it is possible to search among network members to improve health information utilization.

3.2. **Design of the framework.** Figure 2 shows the structure of the proposed system. The Distributed Ledger-based Health Data Management System (DL-based HDMS) is designed with reference to the architecture of Corda.

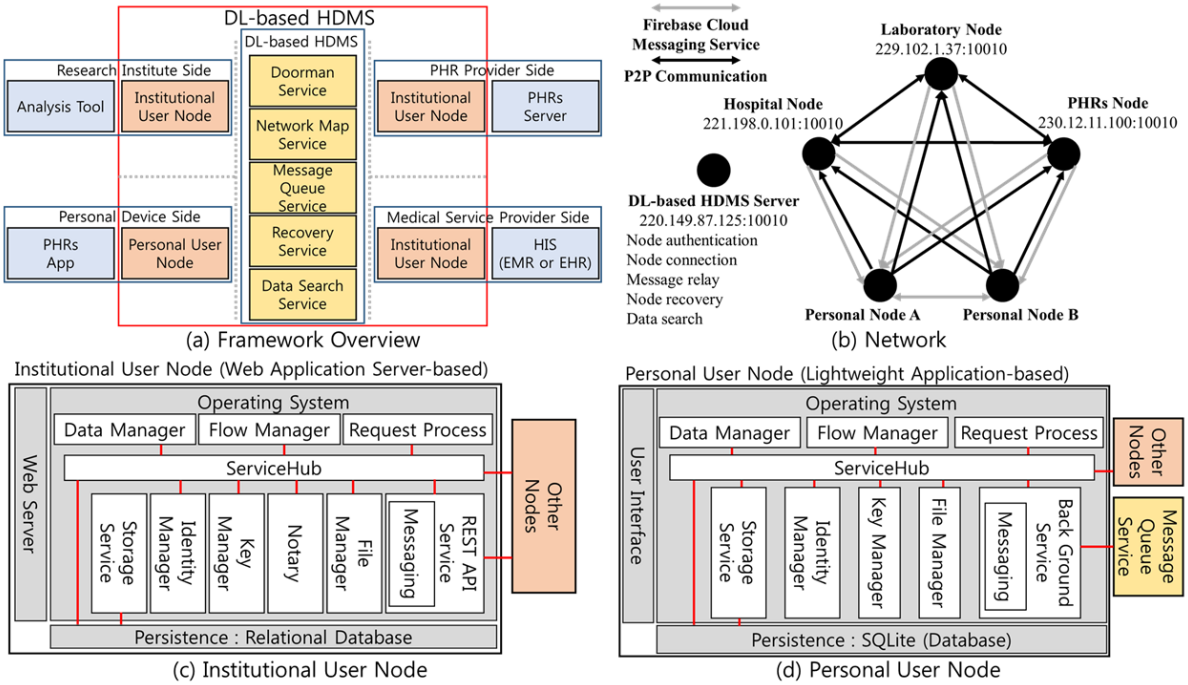


FIGURE 2. System architecture

The overall structure of the DL-based HDMS is shown in Figure 2(a). The DL-based HDMS consists of three components: the DL-based HDMS server for maintaining the network, the personal user node for personal users, and the institutional user node for institutional users. The Corda also has a control server that maintains the network. However, it only performed node-to-node access paths, and nodes authentication. The DL-based HDMS server has a function of storing a message of a missing node, and it has a function of recovering a damaged node, and it has a function of inquiring data between nodes. The DL-based HDMS has a network structure as shown in Figure 2(b). The Corda has static IP on all nodes, and it communicates directly between the nodes. However, the personal user node does not have static IP. The FCM is used as a way to access personal user nodes in the DL-based HDMS. The node structure of the DL-based HDMS is shown in Figures 2(c) and 2(d). The DL-based HDMS uses two types of node. The structure of the institutional user node is very similar to Corda. It removes unnecessary parts from the Corda structure, and it adds the ability to handle large data files, and it adds the REST API for improving communication. The personal user node has a simple function to operate on a personal mobile device, and it has added Back Ground Service for receiving FCM messages.

The primary purpose of the DL-based HDMS is for personal users to store and manage their own health data directly. Traditional PHR systems provide personal health promotion services by analyzing health data. However, the DL-based HDMS is not designed to provide such functionality. Therefore, it is possible to link the DL-based HDMS node with an external program as shown in Figure 3. External programs can use the data on the DL-based HDMS as if they had their own data.

4. **Implementation of Health Data Management System.** We implemented the system based on the proposed system framework. Figure 4 shows the UIs of the proposed system. We implemented the proposed system in the environment shown in Table 1. To achieve the first goal of the proposed system, the personal user node used SQLite on the

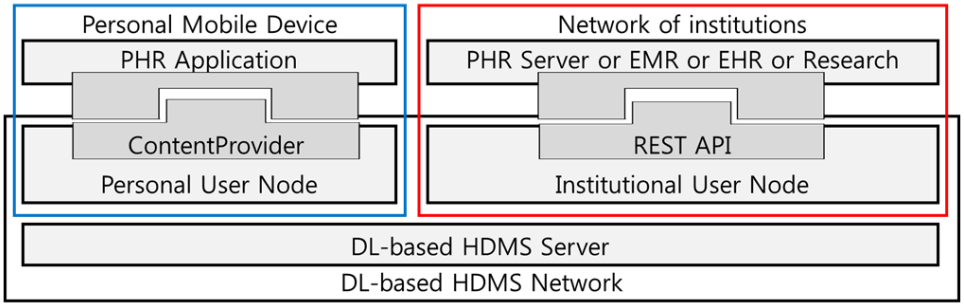


FIGURE 3. Links between the proposed system and external systems

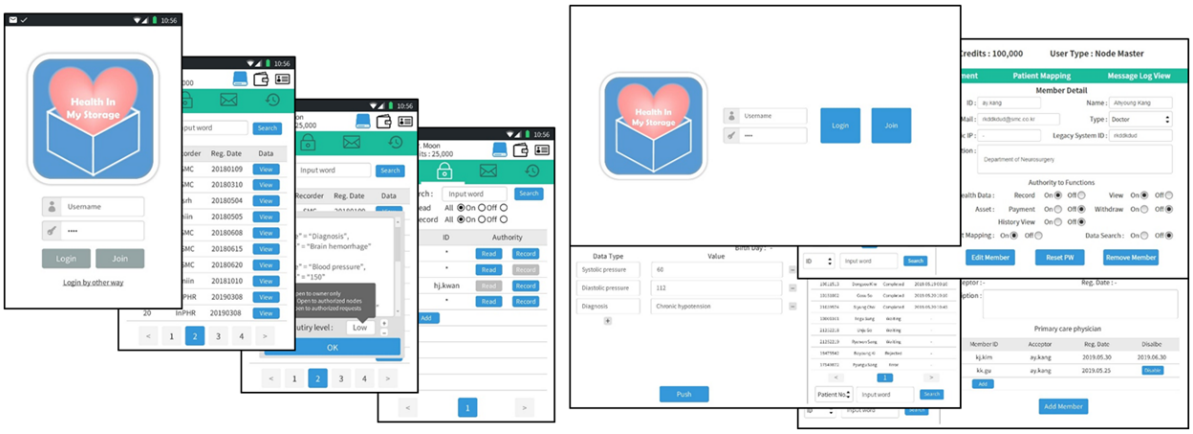


FIGURE 4. UIs of the DL-based HDMS

TABLE 1. Implementation environment of the DL-based HDMS

Personal User Node	DL-based HDMS Server	Institutional User Node
Platform: Android Database: SQLite Persistent: Room Language: Kotlin Communication: Retrofit2 & Firebase Cloud Messaging Key Management: Android Key Store	Framework: Spring Build tool: Gradle Database: Oracle 11g XE Persistent: JPA Language: Kotlin Communication: REST & Firebase Cloud Messaging Key Management: Java Key Generator & Database	Framework: Spring Build tool: Gradle Database: Oracle 11g XE Persistent: JPA Language: Kotlin Communication: REST Key Management: Java Key Generator & Database

Android platform. This allows users to store data directly on their device. In addition, we set up a node-to-node communication network using REST, Retrofit and FCM for our third goal. For the fourth goal, all data communication is encrypted with RSA and AES algorithms. We explain how to achieve the remainder goals along with usage scenarios. We present two scenarios for storing health data and trading health data.

4.1. **Scenarios of storing health data.** Health data storage is one of the main purposes of the proposed system. It consists of 4 steps. The first step is that the institutional user node creates and encrypts the data. The second step is that the personal user node decrypts and verifies the data and it stores the verification key in any notary node. The third step is to send the encrypted personal user node signature and notary information to

the institutional user node. The fourth step is to save and commit the personal user node signature and notary information received by the institutional user node. Figure 5 shows the overall process of this scenario. It has a complex flow for secure data transmission. However, the user's operation is simple as shown in Figure 6. Most of the work is done automatically by the machine.

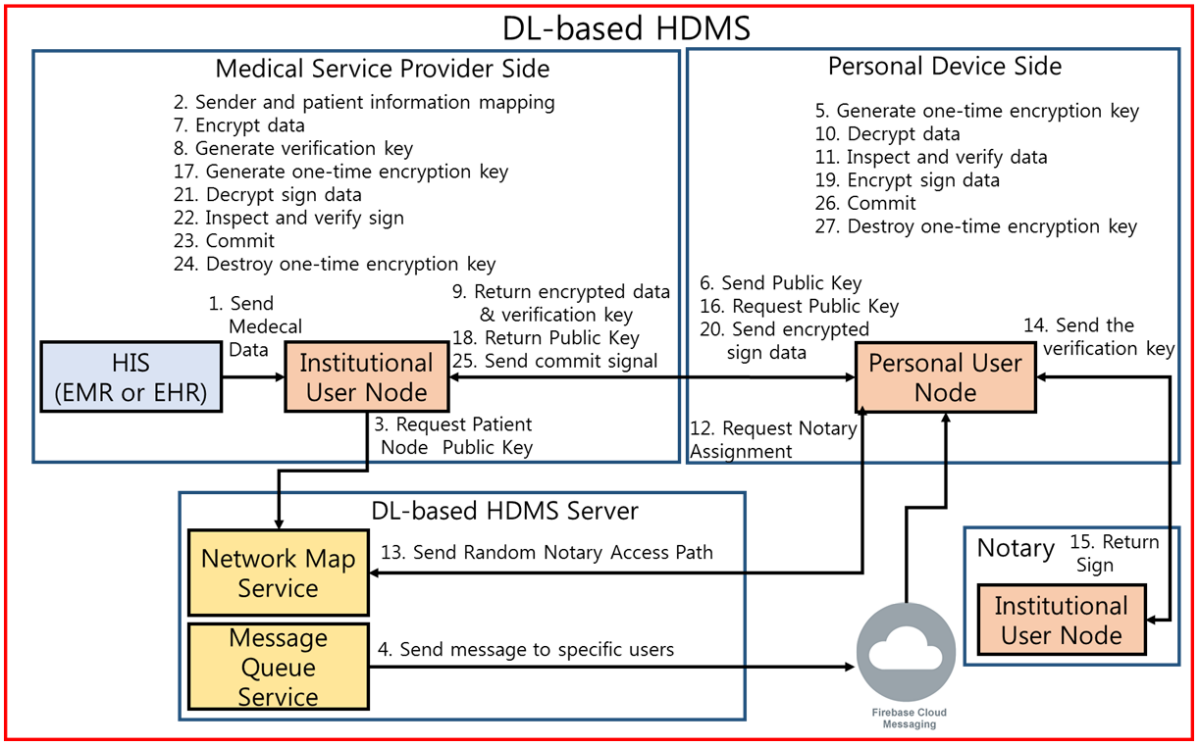
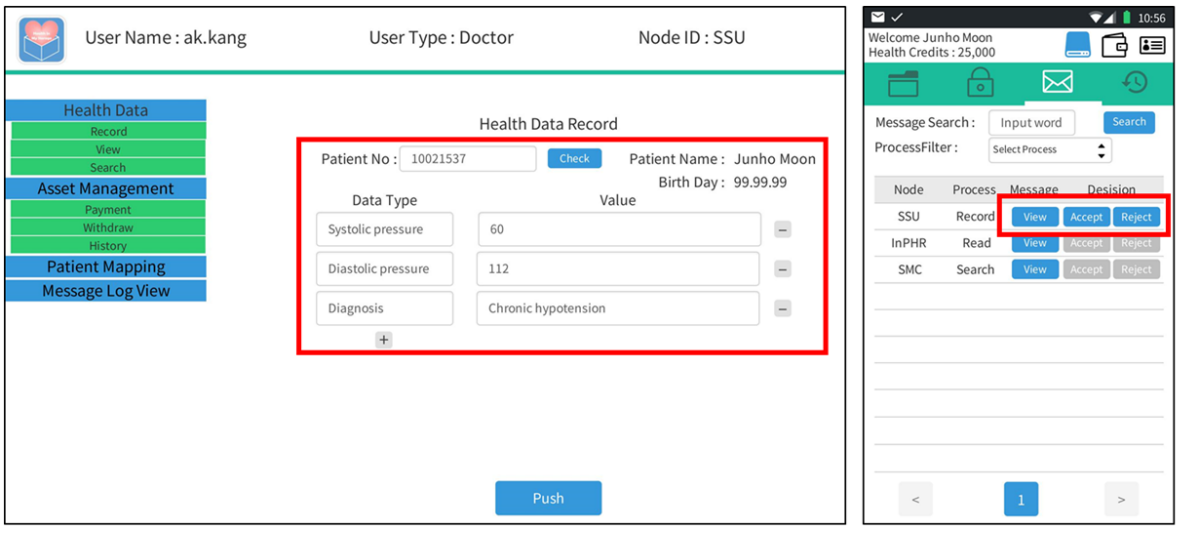


FIGURE 5. Scenarios of storing health data



1. The doctor enters health data.

2. The personal user check health data messages and make decisions.

FIGURE 6. User interfaces for storing health data

In the second step of health data storage, the proposed second goal is achieved by storing the verification key of the data in random notary node. It is also a reference for detecting data forgery and modulation of the fifth goal. The lost data can be recovered by storing it on the institutional user node and the personal user node respectively.

4.2. **Scenarios of health data trading.** The trading of health data is a major function of using the sixth goal of the proposed system. This function also has a complex flow, as shown in Figure 7. This is technically easy using the broadcast function of FCM. This also minimizes the user's work and it is mostly done mechanically.

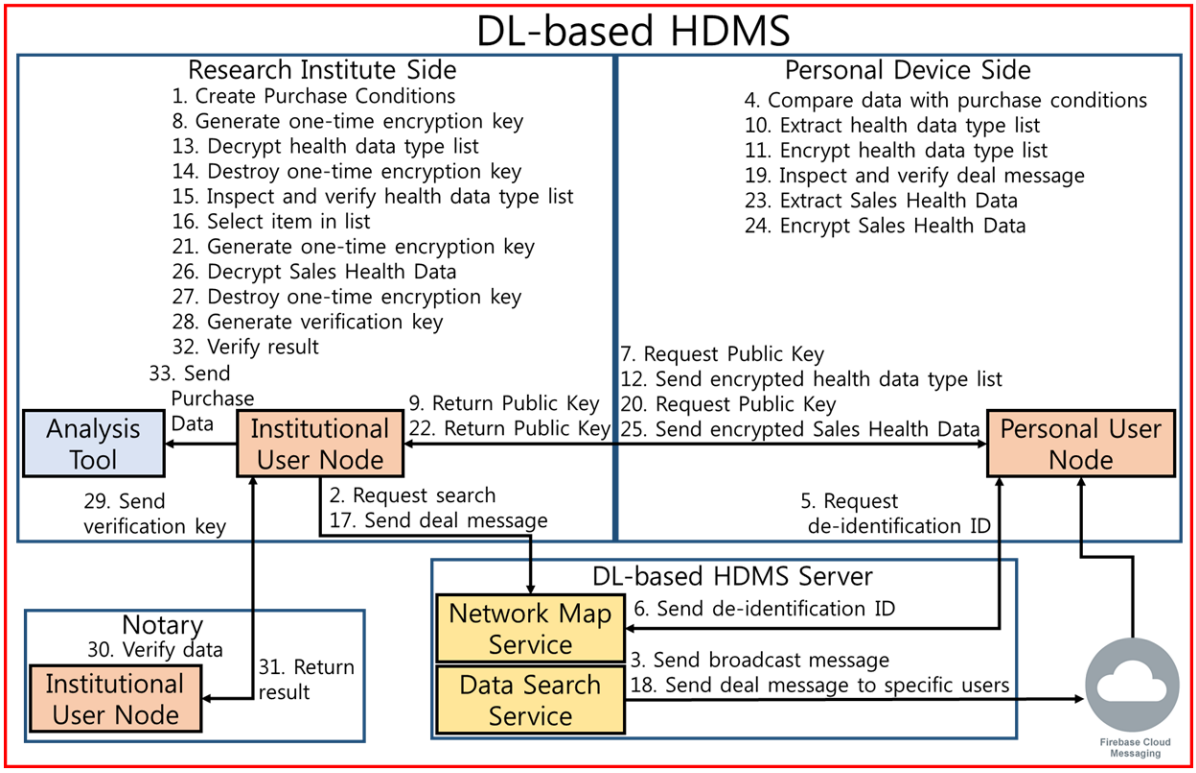


FIGURE 7. Scenarios of health data trading

5. **Conclusions.** In this paper, we proposed an innovative health data management method. It allows information subjects to directly manage and store their health data. The proposed system is the use of lightweight structural node. Therefore, personal users can be direct participants in the network. This proposed system can solve legal disputes in most countries by managing information by information subjects. It also encourages users to actively participate in the system by sharing the benefits of utilizing health data. This will improve data utilization in the healthcare market.

There are concerns about the security problems of the mobile device itself, as the personal user node of the proposed system operates on a personal mobile device. However, mobile devices continue to evolve, and this problem will be solved someday. The proposed system cannot be used independently. It should be combined with existing systems such as PHR systems, EMR, EHR and research tools. It requires an industrial infrastructure. And for that many companies need to be together.

There is no health data standardization function in the currently proposed system. Therefore, we will do additional research on how to standardize health data.

Acknowledgment. This work was supported by the Basic Science Research Program with the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B05029080).

REFERENCES

[1] AHIMA, *Role of the Personal Health Record in the EHR (2010 update) – Retired*, https://library.ahima.org/doc?oid=103209#.Xolg_6gzaUk, 2010.

[2] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage and D. Z. Sands, Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption, *Journal of the American Medical Informatics Association*, vol.13, no.2, pp.121-126, 2006.

[3] J. Moon, S. Lee, J. Byun, J. S. Choi and D. Kim, A case study of interconnected PHR system implementation, *ICIC Express Letters, Part B: Applications*, vol.10, no.6, pp.501-508, 2019.

[4] R. J. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, A. Nesbitt, K. Fedosova, J. Killmeyer, A. Israel and L. Tsai, Blockchain: Opportunities for health care, *Proc. of NIST Workshop Blockchain Healthcare*, pp.1-16, 2016.

[5] J. Jeon and Y. Kim, Case study of medical record management platform using blockchain, *Proc. of Korea Software Congress 2018*, pp.1976-1978, 2018.

[6] L. A. Linn and M. B. Koo, Blockchain for health data and its potential use in health IT and health care related research, *Proc. of ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States, pp.1-10, 2016.

[7] R3, *R3 Corda Development Documentation Version 4*, https://docs.corda.net/releases/release-V4.0/, 2019.

[8] L. Moroney, *The Definitive Guide to Firebase*, Apress, Berkeley, CA, 2017.