


Review

DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System

Tong Min Kim ¹ , Seo-Joon Lee ², Dong-Jin Chang ³, Jawook Koo ⁴, Taenam Kim ⁴, Kun-Ho Yoon ^{5,*} and In-Young Choi ^{2,*}

¹ Department of Biomedicine & Health Sciences, College of Medicine, The Catholic University of Korea, Seoul 06591, Korea; dianakim@catholic.ac.kr

² Department of Medical Informatics, College of Medicine, The Catholic University of Korea, Seoul 06591, Korea; 22001362@cmcnu.or.kr

³ Department of Ophthalmology and Visual Science, College of Medicine, The Catholic University of Korea, Seoul 06591, Korea; hpalways@catholic.ac.kr

⁴ WeHealed Inc., a Corporation Duly Established under the Laws of Korea, Seoul 08786, Korea; jasonkoo@wehealed.com (J.K.); tom@wehealed.com (T.K.)

⁵ Department of Internal Medicine, Division of Endocrinology and Metabolism, Seoul St. Mary's Hospital, College of Medicine, The Catholic University of Korea, Seoul 06591, Korea

* Correspondence: yoonk@catholic.ac.kr (K.-H.Y.); iychoi@catholic.ac.kr (I.-Y.C.)

Abstract: Although blockchain is acknowledged as one of the most important technologies to lead the fourth industrial revolution, major technical challenges regarding security breach and privacy issues remain. This issue is particularly sensitive in applied medical fields where personal health information is handled within the network. In addition, contemporary blockchain-converged solutions do not consider restricted medical data regulations that are still obstacles in many countries worldwide. This implies a crucial need for a system or solution that is suitable for the healthcare sector. Therefore, this article proposes the development of a dynamic consent medical blockchain system called DynamiChain, based on a ruleset management algorithm for handling health examination data. Moreover, medical blockchain-related studies were systematically reviewed to prove the novelty of DynamiChain. The proposed system was implemented in a scenario where the exercise management healthcare company provided health management services based on data obtained from the data provider's hospital. The proposed research is envisioned to provide a widely compatible blockchain medical system that could be applied in future healthcare fields.

Keywords: medical data; blockchain; security management; dynamic consent; smart contract



Citation: Kim, T.M.; Lee, S.-J.; Chang, D.-J.; Koo, J.; Kim, T.; Yoon, K.-H.; Choi, I.-Y. DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. *Appl. Sci.* **2021**, *11*, 1612. <https://doi.org/10.3390/app11041612>

Academic Editor: Jae Kwon Kim

Received: 27 January 2021

Accepted: 9 February 2021

Published: 10 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

As part of the fourth industrial revolution in recent years, the advancement in blockchain technology has brought back the original theorem regarding smart contracts. Such algorithms based on computer protocols were designed to automatically facilitate, verify, and enforce the negotiation and implementation of digital contracts within an authority distributed architecture [1–3]. Smart contracts are being applied to a wide range of fields, mainly from the digital economy to healthcare, and the Internet of Things (IoT) [4]. To date, there is still a trend to use mainstream blockchain platforms, such as Bitcoin and Ethereum, when developing such platforms [5,6].

However, smart contract-related core technology is still in its infancy, and major technical challenges regarding security breach and privacy issues still exist. For example, blockchain cannot guarantee transactional privacy, since the values of all transactions and balances for each public key are publicly visible [7,8]. Moreover, a user's Bitcoin transactions can be linked to reveal user's information [9]. Similarly, each client can be uniquely identified by a set of nodes it connects [10]. "DAO Attack" that occurred in June 2016 [11–13] might be one of the most well-known blockchain targeted attacks. It

was a severe incident that resulted in a loss amounting to more than \$50 million Ether (approximately worth more than 8.5 billion dollars at that time) being transferred to an unauthorized account. This type of security breach is particularly sensitive in the medical industry, where personal health or medical information is being transferred within the network. In addition, contemporary blockchain-converged solutions do not consider restricted medical data regulations that are still obstacles in many countries worldwide.

In addition, current medical systems lack evidence-based data sharing policy, making it difficult for data providers to control their data based on their desired settings or policies. Some of the core values that blockchain technology aims to achieve, which are distributed authority, and consensus-based security, could play a vital role in providing these data providers with the rights they have over their own health data. This implies a crucial need for a system or solution that is suitable for the healthcare sector.

This paper, therefore, proposes the development of a medical blockchain ecosystem based on a dynamic consent system. The proposed solution not only solves security issues by using blockchain technology, but also tackles the problem of privacy piracy by adopting a dynamic consent algorithm original to this research. Our developed system was applied in a practical healthcare business application scenario focusing on actual physical examination of big data being used for health services. Moreover, a medical blockchain-related studies were reviewed to prove the novelty of the system in terms of dynamic applicability and expandability. The proposed solution is envisioned to provide a successful example for future blockchain applied medical systems to be extended to other disease areas or medical databases.

The rest of this paper is organized as follows. Section 2 gives a brief review of the state-of-the-art approaches for blockchain technology. Section 3 provides comprehensive details of the whole DynamiChain. Section 4 describes the specific implementation of DynamiChain. Section 5 highlights the novelty of DynamiChain, and finally, the Section 6 concludes the discussion with the extension of DynamiChain in the future.

2. Related Works

2.1. Related Concept

The algorithm of proof of work (PoW)-based cryptocurrencies, such as Bitcoin, is focused on solving the computationally intensive puzzle to validate transactions and create new blocks. That is, the best computational performance mining node is prioritized when it is selected as the next creator of the new block. The concept was invented by Cynthia Dwork and Moni Naor, as presented in a 1993 journal article [14]. The term “proof of work” was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels [15], and today it is the most widely applied algorithm in all blockchains. However, the PoW method has the disadvantage of wasting resources by consuming a huge amount of electricity and is heavily influenced by computing resources, such as graphics cards and ASIC chips, resulting in the formation of large mining pools that are approaching centralization. A new consensus mechanism that compensates for the PoW limitation is Proof of Stake (PoS), which is based on on-chain currency pricing. PoS is the concept of randomly selecting who will create the next block among the participants of the blockchain network, and several studies have begun to develop this concept further. Song et al. proposed PoS based on competition (CPoS) based on forging committee mechanism to solve the problem of rich people getting richer easily in traditional PoS mechanism and improve the productivity and liquidity of the system [16]. Zhao et al. applied Delegated PoS (DpoS), which is more effective, more decentralized, and more flexible consensus mechanism, in the blockchain network and reduced the number of recording nodes in the block and increased the recording efficiency of the block [17].

The smart contracts have trigger conditions and the corresponding response actions on the terms of the contract. These terms are preset using trigger condition statements, such as “If-Then” statements. Smart contracts are agreed upon and signed by all parties (consensus) and submitted in transactions to the blockchain network. Such transactions are

broadcast to the blockchain network, verified by mining nodes. In a blockchain network, synergy occurs when attack vectors of various IoT devices are analyzed and categorized, and combined with the classify results based on hardware, network, and software [18].

Miners' verification activities are motivated by the system's incentive policies (usually cryptocurrencies) and will contribute their computing resources to verify as much transaction as their capacity allows. When a transaction is finally validated, it is packaged into a new block. The new block is chained as one of the infinite series of blockchains once the entire network reaches a consensus. The creation and execution of a smart contract are fundamentally enforced among anonymous, decentralized individual nodes. These smart contracts are verified on the blockchain, making them resistant to malignant tampering that is not based on participants' pre-agreed consent [19,20].

2.2. Related Research

Despite heavy regulations and bureaucratic inefficiency in the medical field, some prior studies have attempted to innovate the converging blockchain and medicine. Azaria et al. proposed MedRec [21], a novel, decentralized record management system to handle electronic medical records (EMR) using blockchain technology. Their proposed system can be summarized as a system that provides data providers with a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. MedRec mainly ensures authentication, confidentiality, accountability, and data sharing crucial considerations when handling sensitive information. Their system also provides mining rewards in return for sustaining and securing the PoW-based network. The system provides a sustainable system powered by the big data economy, which fundamentally rewards data providers and providers in their choice to release metadata.

Similarly, Fan et al. proposed a blockchain-based information management system, MedBlock, to handle information from data providers [22]. In their proposed scheme, the distributed ledger of MedBlock allows efficient EMRs access and retrieval. MedBlock's consensus mechanism achieves a consensus of EMRs without high energy consumption and network congestion. In addition, MedBlock exhibits a high level of information security by combining customized access control protocols and symmetric cryptography, providing a secure platform for sharing of sensitive medical information.

In addition, although blockchain is not applied to the medical field, there are many studies using blockchain. Jiang et al. proposed a new blockchain-based authentication protocol for WLAN mesh security access, to reduce the deployment costs and resolve the issues of requiring key delivery and central server during authentication [23]. Borja et al. defined a theoretical framework for trust in IoT scenarios, and practically implemented the solution based on the blockchain technology as it meets both, the mathematical formalization and the usual requirements for trust provision systems [24]. Singh et al. detailed the discussion of several key factors for the convergence of Blockchain and AI technologies that will help form a sustainable smart society by blockchain security enhancement solutions, summarizing the key points that can be used for developing various blockchain-AI based intelligent transportation systems [25]. Yan et al. puts forward a blockchain framework based on mobile edge computing, in which the blockchain mining tasks can be offloaded to nearby the edge computing service providers, and the encrypted hashes of blocks can be cached in the edge computing service providers. Moreover, they model the process of offloading and caching to ensure that both edge nodes and edge computing service providers obtain the maximum profit [26]. Nguyen et al. presents a new privacy-preserving Secure Ant Colony optimization with multi-kernel support vector machine with elliptical curve cryptosystem for secure and reliable IoT data sharing based on blockchain to ensure protection and integrity of data [27]. Wang et al. analyses the security requirements of electronic records. Then, based on the characteristics of blockchain decentralization with coding theory, a distributed secure provenance guarantees technology of electronic records is constructed ensuring the authenticity, integrity, confidentiality, and reliability of the provenance information [28]. Cheng et al. presents a highly effective and secure lightweight

mobile client privacy protection system that utilizes the trusted execution environment to provide a new method for privacy protection based on blockchain. They design the authentication mechanism and privacy protection strategy based on Intel software guard extensions to achieve hardware-enhanced data protection, and the blockchain network is to store the hash memory table, which uniquely identifies the data from SGX [29].

Moreover, there are many studies that can safely and effectively manage medical data. Ali et al. proposes the designed to resolve challenges in regression testing in component-based healthcare cloud-enable systems while supporting continuous dynamic change decision and implementation activities in modern software development organizations [30]. Singh et al. works on some public cloud and private cloud authorities, as well as related security concerns. Additionally, it encompasses the requirements for better security management and suggests 3-tier security architecture [31]. Naresh et al. provides a review of IoT in the healthcare domain by first describing the enabling technologies for delivering smart healthcare. In addition, a fog-based architecture consisting of three layers for IoT-based healthcare applications is proposed [32]. Parvathavarthini et al. modifies crow search algorithm by introducing the genetic operators like cloning and mutation operators. In addition to that, the study creates an archive of memory to store the best solutions of the iterations, and these values are used for updating the position when the acquired solutions are not feasible [33].

3. Proposed System

3.1. Overall System Architecture

The overall system architecture of DynamiChain is shown in Figure 1. As mentioned previously, the proposed medical blockchain network was specialized to handle health examination big data, which consists of Inbody [34] tested, blood test, and functional test datasets. The specific data specifications are explained in Section 4.1.

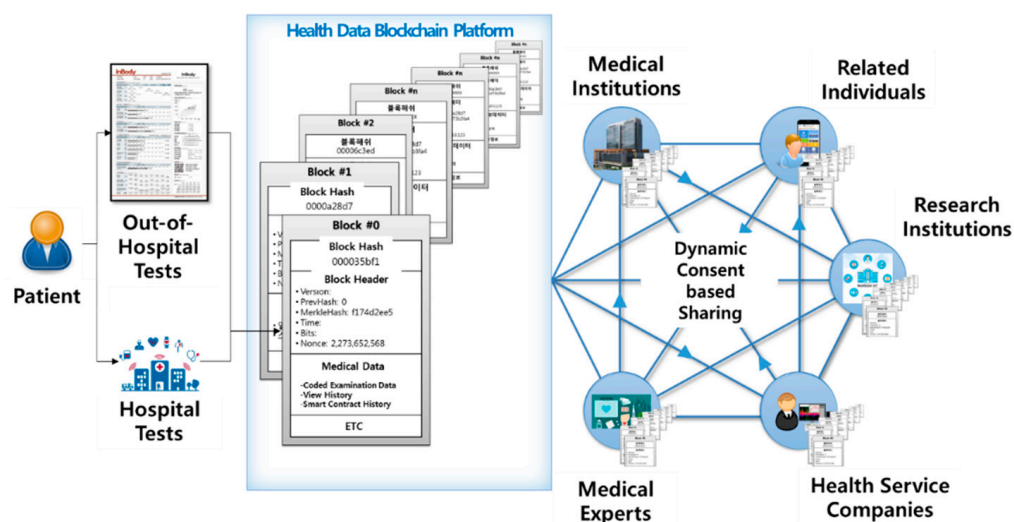


Figure 1. DynamiChain network service based on blockchain and health examination of big data.

Participants include various parties, such as data providers (e.g., patents, holders of health examination data) and data utilizers (e.g., medical professionals, medical institutions, insurance companies, research institutions, and health service companies). Data providers, which are the main party of this network, have established a dynamic consent rule in three main parts: Consent level, approval duration, and approval target. Data utilizers can only participate under dynamic conditions set by the data providers in charge of their own medical data. Data utilizers use this hyperledger-based network under a dynamically set consent. The specifications for the three main dynamic rules are explained in the Section 3.2.

3.2. Specific System Functions

The functions that comprise the overall system mentioned in the previous section are explained in this Section. The list of the function contents is shown in Table 1.

Table 1. Specific system function list.

Function Classification	Function Contents
Data Provider's App	Basic account functions (log in, create account, etc.) My examination history ledger My examination data (raw data and statistical data) Dynamic consent rule settings
Data Utilizer's App	Basic account functions Input health examination results data function Data provider list management Data providers' examination history management ledger Data providers' examination data sharing usage history management ledger Request for data provider data function Data provider data request management function (applicable and non-applicable)
Blockchain System	Health examination data hash storage function Sync smart contract with real-time dynamic consent function settings Smart contract and blockchain ledger
Blockchain Admin Web	Channel management Peer node management User account management Blockchain data sharing history ledger management

Through the data provider's app, data providers may not only view their own health data, but also change dynamic consent rule settings. They have full access to the ledger, which includes the history of which data utilizer viewed or used their data.

By using the data utilizer's app, any data utilizers may access data providers' health examination data based on set rules. They may also act as a "mining node" (mining, in terms of blockchain), to be rewarded for checking if the transmitted data are real. Since hospitals are the main provider for the hospital examination data provider data, numerous data management functions can be enforced with this app. Even if the requested data meet the settings set by the data provider, the hospital finally confirms whether or not the transaction should be made. This function may be disabled in countries that do not have restricted medical data policies. Explanation of restricted medical data policies will be further explained in Section 3.4.

The hash function of the blockchain system is created and matched to each health data. In addition, this function is automatically synced with real-time changing consent settings by each data provider. Most importantly, all transaction history is stored for data integrity and security in each blockchain. Finally, the blockchain admin web functions enable the super administrator to monitor the status of the entire channel, participating peer nodes, and participating users (i.e., data provider and data utilizer) within the blockchain network.

3.3. Dynamic Consent Algorithm

Medical data is an intangible asset that requires time and effort from a medical institution or individual. It is intertwined with users, service providers, data carriers, etc., requiring a consent system algorithm that all participants can intuitively understand and agree on. To meet these needs, this paper applied the dynamic consent concept on a new customized consent system, called "dynamic consent algorithm". The system is tailored to the individual user's taste, minimizing the user's resistance to data disclosure. Furthermore, by implementing this dynamic consent algorithm in the chaincode mentioned in Section 4, this paper developed a consent system algorithm that is transparent and integrated to all

participants in the consensus operation of the blockchain. Our proposed dynamic consent algorithm includes data type, approval duration, and objectives (Figure 2).

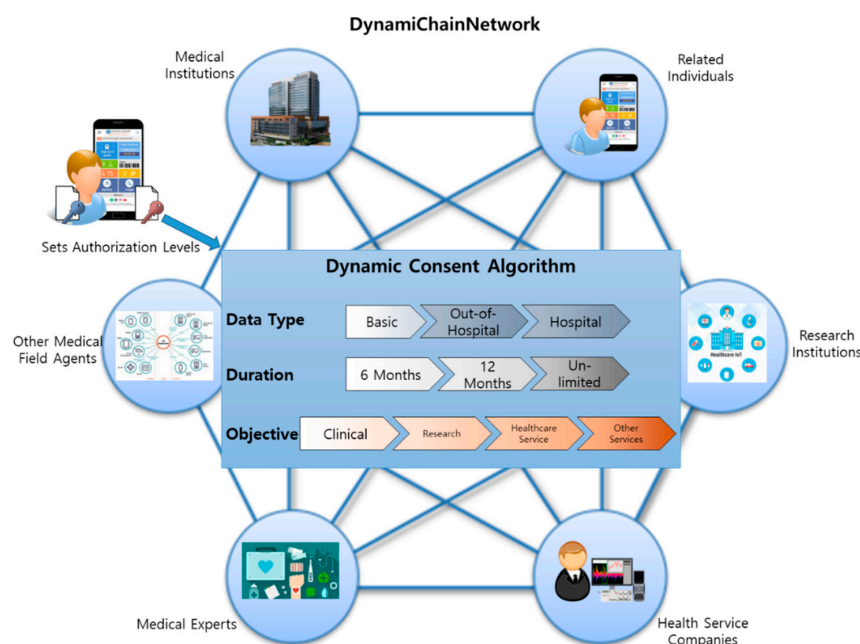


Figure 2. Three main functions of the proposed dynamic consent algorithm.

The term data type refers to data providers setting the type of data they wish to provide to other data utilizers. Data providers can choose from three data types: Data derived basically, out-of-hospital-level tests, and data derived from hospital-level tests. For example, basic data refer to social demographic data, such as age, sex, and address. Out-of-hospital tests refer to basic health tests that data providers can easily achieve through home healthcare devices, such as thermometers, InBody tests, or other healthcare-related devices. On the other hand, data obtained from hospital-level tests are more in-depth because data providers can only achieve such data when they visit the hospital. The specific contents of these three classifications are shown in Table 2.

Table 2. Contents of the three-level classifications of consent data types.

Classification	Contents
Basic	Serial number, Sex, Age, Smoking Status, Drinking Status, Height, Weight, Waist
Out-of-hospital-level tests	Body Water, Protein, Minerals, Body Fat Amount, Weight, Bones and Muscle Amount, BMI, Body Fat Ratio, InBody Score, Abdomen Fat Ratio, Internal Organ Fat Level, Fat-free Mass, Basal Metabolism, Obesity Index, Recommended Calorie Amount, Body Parts' Muscle Analysis (Right Arm, Left Arm, Body, Right Leg, Left Leg), Body Parts' Fat Analysis (Right Arm, Left Arm, Body, Right Leg, Left Leg), Body Parts' Body Water Analysis (Right Arm, Left Arm, Body, Right Leg, Left Leg), Body Parts' Cell Water Analysis (Right Arm, Left Arm, Body, Right Leg, Left Leg), Body Parts' Cell-free Water Analysis (Right Arm, Left Arm, Body, Right Leg, Left Leg), Cell-free Water Ratio, Phase Angle
Hospital-level tests	Cholesterol, Triglycerides, HDL Cholesterol, LDL Cholesterol, Diastatic Hemoglobin, Diastatic Hemoglobin Before Meal, Protein in Urine, Serum Creatinine, AST, ALT, Gamma GTP, Serial Number, Examination Date, Examined Institution, Sight (Left, Right), Blood Pressure (Systolic, Diastolic)

Approval duration refers to data providers setting the exposure duration of their personal medical data to other data utilizers. By default, data providers can simply select 6 months, 12 months, or unlimited duration. This can always be changed by accessing the system settings.

The third objective refers to data providers selecting which data utilizer they desire to provide their personal medical data according to the usage objective. With this function, data providers can, by default, select any group based on these four classifications: Clinical, research, healthcare service, and other services. Any data utilizers (mainly hospitals) that registered into our proposed system with the objective of using physical examination data for clinical matters are classified as “Clinical.” Similarly, all groups (mainly universities or research institutions) whose data usage objective is for research are classified as “Research.” Most health insurance companies are classified as “Healthcare services,” and other data utilizers with other needs are classified as “Other services.”

3.4. Restricted Medical Data Policy Applied Work Flow Specifications

Some countries worldwide, including South Korea, still prohibit healthcare data to be stored outside certified medical institutions. Considering this, the proposed system only saves hash values of the health examination data and stores actual medical data separately in another database. Medical data’s multiple hash values are stored in the blockchain ledger so that data utilizers could read the data providers’ data based on set rules. Encoding–decoding access key to the actual medical data is, by default, managed by the data provider, unless the data provider delegates his or her authority to medical institutions where the actual database is stored. Using this mechanism, we balanced the data co-ownership ecosystem while preserving data integrity in a practical situation. This service process is shown in Figure 3. The hospital generates health examination data of a data provider than the hash management system encrypts the data with the data provider’s public key and stores them with the hash value of the data. The data provider then confirms the data itself and dynamic consent rule in real-time and modifies the setting of the rules if necessary. The data utilizer requests for the data of the data provider, and the hospital confirms the request. The hospital allows access to actual data transmission after the endorsement process. Finally, data utilizer read the requested data through hash value comparison.

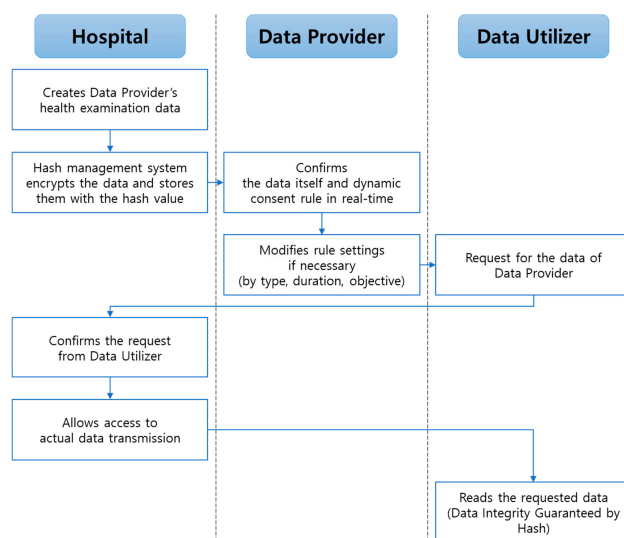


Figure 3. Proposed specific blockchain service process.

Hospital type data are created when data providers visit the hospital for a health examination. For each data, our proposed system stores encoded data, and accordingly, it has the data provider public key. Data providers have access to their own physical data and can set or change their dynamic consent rule in real-time. When other data utilizers (e.g., companies and research institutions) request for the allowed data providers’ medical data, the data source hospital confirms this request before transmitting the actual medical data to the requested data utilizer. Thereafter, the data utilizers could read the requested data.

This is the key process that not only overcomes the issue of restricted health data sharing policies for some countries, but also guarantees data integrity. Note that out-hospital-data types are free from this scenario.

4. Implementation

4.1. DynamiChain Network Based on Hyperledger Fabric

Because of the sensitivity of healthcare data, DynamiChain was implemented using Hyperledger Fabric Blockchain technology (version 2.2.0), one of the permissioned and private blockchains that enhanced privacy [35]. It was established as a network that allows data utilizers to operate peer nodes. A hyperledger chaincode-based smart contract was implemented to store data in the blockchain and to distribute it to peer nodes. The original medical data from the data provider are implemented in the off-chain of the blockchain system, and the hash values of the medical data are stored on-chain, where dynamic consent system rules are applied to control the data provider's medical data.

Three organizations, such as data providers, data utilizers, and hospital, form a consortium in DynamiChain (Figure 4). Mainly, data providers can set their dynamic consent rules, and we updated the chaincode according to the rules. Hospitals can store medical data transmission records and manage overall health examination data transmission. Data utilizers can compare health examination data hashes and read health examination data, respectively. The consortium is joined by all three organizations through one channel (Channel1). Additional participation on the consortium can be established through the configuration block stored in the ordering service, including peer, channel, client, network policy, and channel policy, after establishing the ordering service node, Orderer1, under consultation between organizations. Channel1 is created through Orderer1, and Channel1 provides the ability to share data only between organizations that share interests among consortiums. Organization1–3 will install their own peer in their data center and then participate in Channel1. Every peer has the role of communing/reader/anchor peer, and only the Peer3 has the role of endorsing peer additionally. The peers participating in Channel1 can store Distributed Ledger1 used on Channel1 in their local repository and share data. Chaincode1 has a smart contract function for the purpose of the Channel1 participants and is installed on every peer. Every participant on Channel1 must use our newly developed Dapp to participate in the network and send a transaction to the peers where the Chaincode1 is installed. Dapp commonly consists of a UI front end, REST API [36] backend, and Fabric Software Development Kit [37] (SDK, based on node.js).

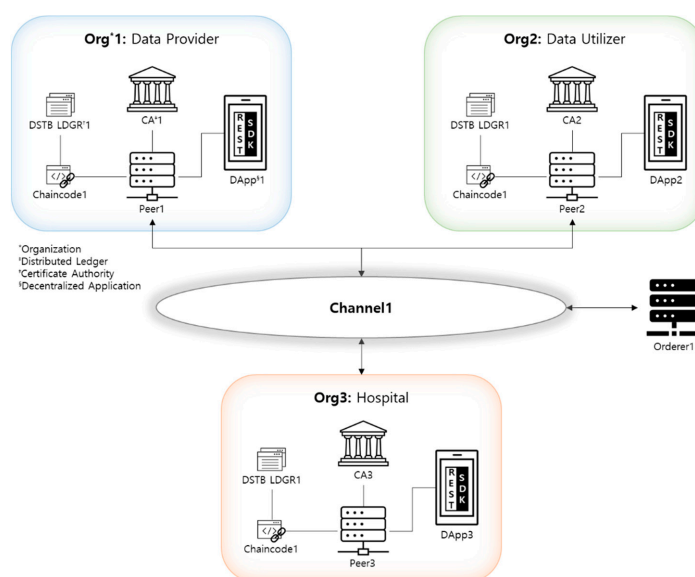


Figure 4. DynamiChain Network based on Hyperledger Fabric.

4.2. Dynamic Consent System

Dynamic consent algorithm is implemented in the Chaincode1, and blocks are generated throughout the following process (Figure 5). In this process, the participant called Data Provider1 in Org1 tries to send their data to the hospital in Org3 according to the dynamic consent system through the Dapp1. First, Data Provider1 requests transaction generation to send the data to the hospital via Dapp1 (Figure 5a). After receiving the transaction generation request, Dapp1 generates a transaction that contains the message of sending data and sends the transaction to the endorsing peer, Peer3. Peer3 can be connected to Dapp1 after passing the certification process using the certificate of Data Provider1. After connection, Dapp1 calls up the update function of the chaincode installed in Peer3 and requests the chaincode execution (Figure 5b). Upon receipt of the transaction from Dapp1, Peer3 simulates the chaincode by referring to the World State DB and checks the results of read/write set to determine whether it is endorsed or not (Figure 5c). If the transaction execution result is valid and the endorsement of Peer3 is passed, Peer3 sends the results and the digital certificate of Peer3 to Dapp1 (Figure 5d). Receiving the simulation results from Peer3, Dapp1 checks to see if the value of the read/write set is the same as its expected value and checks whether the digital certificate of Peer3 has been received. After verification, Dapp1 broadcasts the transaction containing the digital certificate of Peer3 and the results of read/write set to the Orderer1 node to create the block (Figure 5e). The Orderer1 identifies the time stamp fields, which is required to order the transactions, and then orders the transactions to be included in the block to create the latest blocks (Figure 5f). After that, Orderer1 delivers the created blocks to all the peers on the network (Figure 5g). Every peer who receives the latest block performs verification by running a Validation System ChainCode (VSCC) system chain code to verify the results and certificates of all transactions contained in the block. If the validation process is passed, all the peers update the distributed ledger stored in their local repository (Figure 5h). Peers complete the distributed ledger update process by sending the results of the updated distributed ledger to Dapp1 (Figure 5i).

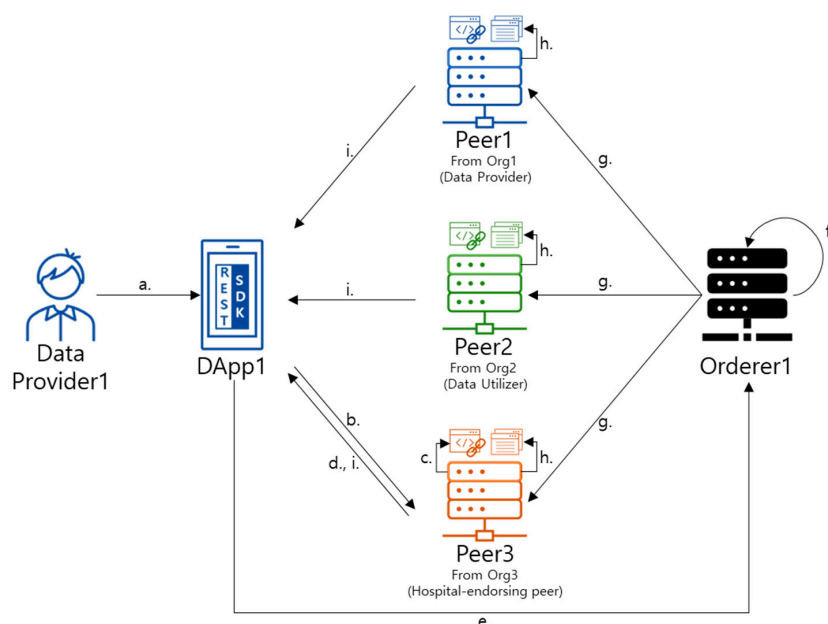


Figure 5. Blockchain generation flowchart of DynamiChain. (a) Request transaction creation. (b) Connect endorsing peer (peer3), and request chaincode execution. (c) Execute chaincode (d) Return endorsed transactions and certificate of endorsing peer. (e) Forward endorsed transactions and certificate of endorsing peer. (f) Order transactions and create a block, (g) send a new block, (h) commit transaction and update distributed ledger, and (i) send the result of the updated distributed ledger.

4.3. Security Management System

Blockchain security comprises mainly confidentiality, integrity, availability (CIA) [38]. DynamiChain also meets the CIA by complementing the existing public blockchain model.

Since information is open and cannot be restricted from participating in the traditional public blockchain, it is very difficult to meet consistency. DynamiChain uses private blockchain's channel to meet confidentiality by only allowing pre-selected participants to join the network. Moreover, not only are digital certificates safely managed by applying Fabric-CA, but also sensitive data are encrypted by implementing Private Data Collection (PDC).

In the existing public blockchain, Public Key Infrastructure (PKI) based on hash algorithms is used to prevent the manipulation of the block, and each block stores the information of not only the current block, but also the previous block. DynamiChain also take advantage of the existing public blockchain's attribute. In addition, DynamiChain increases its integrity by requiring all the peers to periodically verify the current block state before adding a new block, therefore, reducing the possibility of peer hacking.

In the traditional blockchain, as well as DynamiChain, data are accessible from the rest of the nodes even if one node is not working. All nodes are kept and decentralized with the same contents, preventing a single point of failure to gain availability. Furthermore, from the generation of transactions process to the consensus process, it can be processed individually in stages, which improves the performance by allowing parallel processing to perform more than one task at the same time.

A user management system and a key management system are the two main components of the security management system.

The user management system (Figure 6) manages the actual users for creating, blocking, and deleting (Figure 6a) data providers and data utilizers. Data providers can create additional accounts under a dynamic consent framework by requesting the super administrator. Data utilizers can also create additional accounts by requesting the super administrator (Figure 6b) by specifying the purpose of data usage information (e.g., clinical, research, and healthcare). Figure 6c shows the DynamiChain interface of the user management system implementation screen showing the management list according to the user type. The functions for managing the permissions of data providers and data utilizers were implemented in the super administrator account. A super administrator can create, block, and disable accounts of the data provider and user. If a user is created, a key in the blockchain is also generated. If a user is blocked, it is impossible to login to the system. The data provider sets the access permissions of the data according to the dynamic consent system. The data utilizer manages and utilizes the data according to the access permission set by the data provider.

The key management system requires a key to sign the blockchain for each user. The key to the data provider is generated when he or she joins the web service (Figure 7a). The ECDSA algorithm was used to generate private and public keys. The generated keys are stored in a key-store-only wallet within the server (Figure 7b). The keys of the super administrator and the user are distinguished. For security purposes, each user maintains the key in a separate wallet.

In Table 3, medical blockchain-related studies (2016 to 2020) were reviewed to prove the novelty of the system in terms of dynamic applicability and expandability.

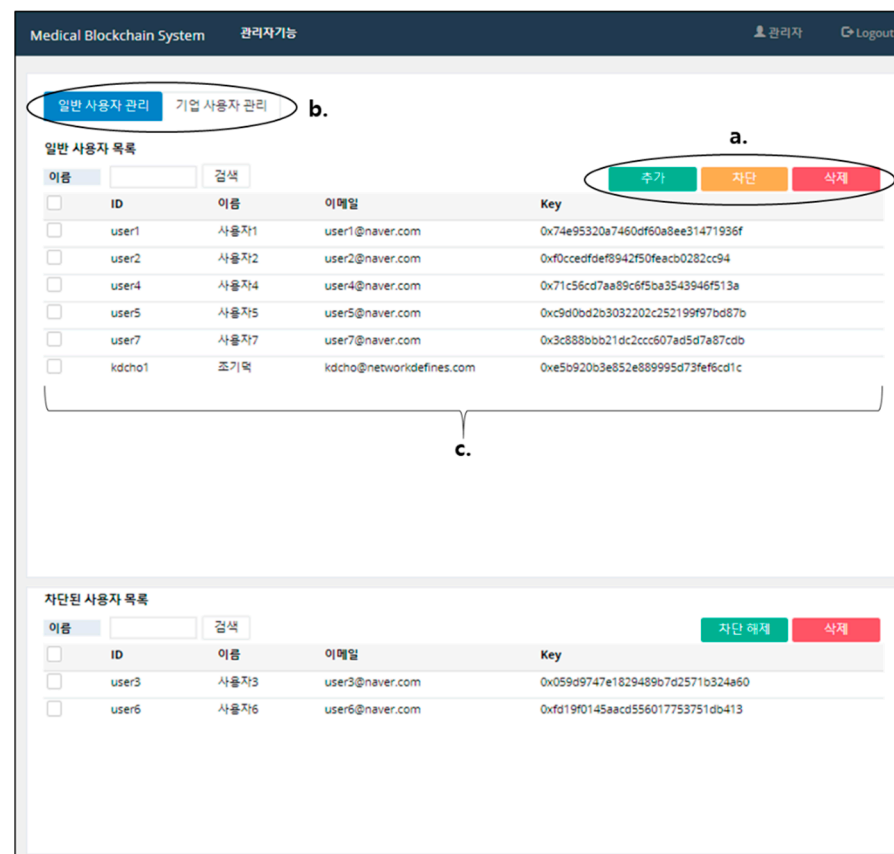


Figure 6. DynamiChain interface of the user management system. (a) User selection tab (data provider/data utilizer). (b) User management button (create/block/delete). (c) User list.



Figure 7. Dynamichain interface of the key management system. (a) Web screen and (b) server screen.

Table 3. Review of the existing medical ecosystem based on blockchain (from 2016 to 2020).

Reference	Main Idea	Target Data	Target Participant	Blockchain Platform	Consensus Mechanism	System Architecture	Not Addressed
DynamiChain	Maximize the autonomy via dynamic consent and Maximize the flexibility to expand participants	Health examination data	Patients, Hospitals, Service providers	Hyperledger	Chaincode based on dynamic consent	Proposed, Implemented	-
Azaria, A. et al. (2016) [21]	Innovative approach for handling EMR data	EMR data	Patients, Hospitals, Service providers	Ethereum	Smart contract, PoW	Proposed	Detailed data description, Healthy participants, Dynamic consent, Dapp
Dubovitskaya, A. et al. (2017) [39]	Present a framework on managing and sharing EMR data for cancer patient care	Radiation oncology EMR data	Cancer patients Hospitals	Hyperledger	Consensus	Proposed, implemented	Detailed data description, Healthy participants, Dynamic consent, Dapp

Table 3. Cont.

Reference	Main Idea	Target Data	Target Participant	Blockchain Platform	Consensus Mechanism	System Architecture	Not Addressed
Liang, X. et al. (2017) [40]	Design a mobile healthcare system for personal health data collection, sharing	Personal health data	Patients, Hospitals, Service providers, Insurance company	Hyperledger	Not specified	Proposed, implemented, Evaluated	Service providers, Dynamic consent
Xia, Q. et al. (2017) [41]	Provide trustworthy data sharing model between cloud service providers in a trust-less environment	EMR data	Cloud service providers	Permissioned blockchain	Smart contract	Proposed, implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, Dapp
Fan, K. et al. (2018) [22]	Resolve the problem of large-scale EMR data management and sharing in an EMR system and allows the efficient EMRs access and retrieval	EMR data	Patients, Hospitals	Consortium	consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, Dapp
Griggs, K.N. et al. (2018) [42]	Resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties	Protected health data	Remote patients, Hospital	Ethereum, Private	Smart contract, Consensus	Proposed	Service providers, Dynamic consent
Ji, Y. et al. (2018) [43]	Investigates the location sharing based on blockchains for telecare medical information systems	Medical data	Patients, Hospitals	Not specified	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, Dapp
Kaur, H. et al. (2018) [44]	Store and manage huge healthcare data in cloud environment	Heterogeneous medical data	Patients, Hospitals, Drug manufacturer, Insurance company	Not specified	Not specified	proposed	Detailed data description, Healthy participants, Dynamic consent, Dapp
Li, H. et al. (2018) [45]	Present a novel data preservation system that provides a reliable storage solution of stored data while preserving users' privacy	Medical data	Not specified	Ethereum	Not specified	Proposed, Implemented, Evaluated	Detailed data description, Participants, Service providers, Dynamic consent, Dapp
Uddin, M.A. et al. (2018) [46]	Presents an architecture that involves a patient agent coordinating the insertion of continuous data streams into blockchain to form an EHREHR data	EHR data	Patients, Hospitals	Bitcoin, Ethereum	Miner	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Zhang, A. et al. (2018) [47]	Proposes a blockchain-based secure and privacy-preserving personal health data sharing scheme for diagnosis improvements in e-Health systems	Personal health data	Patients, Hospitals	Consortium, Private	Consensus, PoC	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Zhou, L. et al. (2018) [48]	Propose a blockchain-based threshold medical insurance storage system	Insurance data	Patients, Hospitals, Insurance company	Ethereum	Consensus, PoW	Proposed, Implemented, Evaluated	Healthy participants, Dynamic consent, DApp

Table 3. Cont.

Reference	Main Idea	Target Data	Target Participant	Blockchain Platform	Consensus Mechanism	System Architecture	Not Addressed
Al Omar, A. et al. (2019) [49]	Present privacy-preserving platform in cloud using Elliptic curve cryptography and MediBChain protocol	Healthcare data	Patients, Hospitals	Permissioned blockchain	Smart contract	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers Dynamic consent, DApp
Casado-Vera, R. et al. (2019) [50]	Create an e-health system based on wireless sensor networks	Medical data	Patients, Hospitals	Ethereum	Not specified	Proposed	Detailed data description, Healthy participants, Service providers Dynamic consent, DApp Consensus
Dwivedi, A.D. et al. (2019) [51]	Provide secure management and analysis of healthcare big data form IoT devices	IoT health data	Patients, Hospitals, Service providers	Bitcoin	Smart contracts	Proposed	Dynamic consent, DApp
Hyla, T. et al. (2019) [52]	Use design-science methodology to create an integrity-protection service model based on blockchain technolher	EHR data	Patients, Hospitals	Permissioned blockchain	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Islam, N. et al. (2019) [53]	Propose an activity monitoring and recognition framework to improve the activity classification accuracy in videos supporting cloud computing-based blockchain architecture	IoT video data	Patients, Hospitals, Service providers	Not specified	Not specified	Proposed, Implemented, Evaluated	Healthy participants, Dynamic consent, DApp
Kuo, T.T. et al. (2019) [54]	Develop a general model sharing framework to preserve predictive correctness, mitigate the risks of a centralized architecture	Healthcare data, genomic data	Patients, Hospitals	Permissioned blockchain	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Li, X. et al. (2019) [55]	Present a secure and efficient data management system for mobile healthcare system based on edge computing	EMR data, Mobile health data	Patients, Hospitals, Service providers	Permissioned blockchain	Consensus	Proposed, Implemented, Evaluated	Dynamic consent, DApp
Nguyen, D.C. et al. (2019) [56]	Propose a novel EHRs sharing framework that combines blockchain and the decentralized interplanetary file system on a mobile cloud platform	EHR data	Patients, Hospitals	Ethereum	Consensus	Proposed, Implemented, Evaluated	Healthy participants, Dynamic consent
Rahmadika, S. et al. (2019) [57]	Present a model for shared storage on a blockchain network that allows the authorized parties to access the data on storage without having to reveal their identity	Personal Health Data	Patients, Hospitals, Service providers	Not specified	Not specified	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Dynamic consent, DApp
Shen, B. et al. (2019) [58]	Propose an efficient data-sharing scheme which combines blockchain, digest chain, and structured P2P network techniques	EHR	Patients, Hospitals, Insurance company, Service providers	Permissioned blockchain	BFT-SMaRt [57]	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Dynamic consent, DApp

Table 3. Cont.

Reference	Main Idea	Target Data	Target Participant	Blockchain Platform	Consensus Mechanism	System Architecture	Not Addressed
Tian, H. et al. (2019) [60]	Establish a shared key that could be reconstructed by the legitimate parties before the process of diagnosis and treatment begins	Medical data	Patients, Hospitals, Pharmacy, Lawyers	Hyperledger	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Wong, D.R. et al. (2019) [61]	Propose a blockchain-based system to make data collected in the clinical trial process immutable, traceable, and potentially more trustworthy	Clinical trial data	Patients, Hospitals,	Not specified	Not specified	Proposed, Implemented, Evaluated	Healthy participants, Service providers, Dynamic consent, DApp
Yang, J. et al. (2019) [62]	Utilizes the transparency, security, and efficiency of blockchain technology to establish a collaborative medical decision-making scheme	Personal health data	Patients, Hospitals, Insurance company	Consortium	Proof of familiarity	Proposed, Implemented, Evaluated	Detailed data description, Dynamic consent, DApp
Zheng, X. et al. (2019) [5]	Integrate IOTA Tangle with IoT to develop a health data sharing system, which could support secure, fee-less, tamper-resist, high-scalable, and granular-controllable health data exchange	IoT health data	Patients, Hospitals, Service providers	IOTA Tangle	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Dynamic consent, DApp
Tanwar, S. et al. (2020) [63]	Proposes an Access Control Policy Algorithm for improving data accessibility between healthcare providers, assisting in the simulation of environments to implement the Hyperledger-based EHR sharing system	EHR	Patients, Hospitals	Hyperledger	Consensus	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent, DApp
Khatoon, A. (2020) [64]	Proposes multiple workflows involved in the healthcare ecosystem using blockchain technology for better large amount of data management	Medical data	Patients, Hospitals, Pharmacy, Insurance company	Ethereum	Smart contract	Proposed, Implemented, Evaluated	Healthy participants, Dynamic consent,
Abou-Nassar, E.M. et al. (2020) [65]	Propose blockchain decentralized interoperable trust framework for IoT zones where a smart contract guarantees authentication of budgets and indirect Trust Inference System Reduces semantic gaps and enhances trustworthy factor (TF) estimation via the network nodes and edges	IoT health data	Patients, Hospitals, Service providers	Ethereum	Smart contract	Proposed	Healthy participants, Dynamic consent, DApp

Table 3. Cont.

Reference	Main Idea	Target Data	Target Participant	Blockchain Platform	Consensus Mechanism	System Architecture	Not Addressed
Sharma, A. et al. (2020) [66]	Analyses the dimensions that decentralization and the use of smart contracts will take the IoMT in e-healthcare, proposes a novel architecture, and outlines the advantages, challenges, and future trends related to the integration of all three	IoT health data	Patients, Hospitals,	Not specified	Smart contracts	Proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers Dynamic consent, DApp
Kim, S.K. et al. (2020) [67]	Use artificial intelligence blockchain algorithms to ensure safe verification of medical institution PHR data and accurate verification of medical data as existing vulnerabilities	EMR, Personal health data	Patients, Hospitals,	Ethereum	Hyper POR	proposed, Implemented, Evaluated	Detailed data description, Healthy participants, Service providers, Dynamic consent

5. Discussion

The case scenario showed that companies can provide, for example, health AI convergence technology-based home training services [68], dietary consumption recommendation services [69], or health beauty services (e.g., cosmetics recommendation [70]) based on individual data provider specialized health data. Insurance companies can also use these data based on the limits set by each data provider. Our proposed system is envisioned to allow several health technology converged services to be launched, contributing to the vitalization of the next-generation healthcare industry converged with proper blockchain technology.

In addition, data integrity and data security, which are a few of the main important blockchain functions mentioned in this paper, provide a solid ground for future personal health records (PHRs) to be rapidly applied in medical systems. Most importantly, the dynamic consent, which can be set by the data owners (data providers), provides the proposed system high reliability and credibility so that data owners do not have to worry about data piracy or data abuse.

As mentioned above, including South Korea, there are many countries [71–73] that have strong regulations against medical data being stored or being transmitted outside certified medical boundaries without strict authorization. Another unique characteristic of our proposed system is that we considered this by adopting the hash-data sync system. By doing so, the actual data did not have to be transmitted unless there was an actual need for the raw data to be transmitted. Otherwise, there would be a regulation huddle for every blockchain transaction.

Several medical blockchain-related studies were reviewed to prove the novelty of DynamiChain in terms of dynamic applicability and expandability (Table 3). Most studies were conducted based on EMR data, not using the other forms of out-of-hospital healthcare data, such as data acquired from mobile healthcare devices (“Target Data” column). Moreover, most of the target patients they dealt with were mainly patients, hospitals, and researchers (“Target Participant” column). That is, they did not consider the additional participation of third parties, such as healthcare service providers, healthy persons (not patients). In addition, data open consent was not dynamically considered in previous studies, which allowed data providers little control over their own data (“Consensus Mechanism” column). Most studies focused only on system implementation and performance evaluation and did not develop DApps that could be used directly by the data providers, resulting in a lack of use cases in the actual scenarios (“System Architecture” column).

They also lacked specific explanation and analysis of data characteristics compared to the proposed research (“Not Addressed” column).

6. Conclusions

This paper proposes DynamiChain, the medical blockchain based on a dynamic consent system and security management system for handling physical examination data. DynamiChain supports modular designs based on the dynamic consent algorithm so that participants can select functions, such as authentication, consensus algorithms, and encryption in the form they want to operate the blockchain. This modularized design provides flexibility because it enables the development of various network models as more organizations to participate in the future. The overall specifications are explained in Section 3, and the actual implementation scenario is presented in Section 4, handling the case of a health service company providing business using our system.

The limitation of this research is that the implementation scenario was conducted in a limited area. More practical implementation should be enforced in actual situations. This research is currently being conducted under a three-year Ministry of Health and Welfare governmental funding project worth a total of 400,000 CHF funds. It has started in 2019, making 2020 the second year, and 2021 the final year. During the first two years, this research project’s goal was full development. The final year, which is next year, is the scheduled performance evaluation of the fully developed system.

For future research, actual data should be cumulated and analyzed to evaluate the performance of the proposed system. The proposed research is envisioned to provide a widely compatible blockchain medical system that could be applied in future healthcare fields.

Author Contributions: Conceptualization, T.M.K. and D.-J.C.; Data curation, T.M.K.; Formal analysis, T.M.K. and S.-J.L.; Funding acquisition, I.-Y.C.; Investigation, T.M.K. and S.-J.L.; Methodology, T.M.K. and D.-J.C.; Project administration, I.-Y.C.; Resources I.-Y.C.; Software, J.K. and T.K.; Supervision, S.-J.L., I.-Y.C. and K.-H.Y.; Validation T.M.K.; Visualization, T.M.K.; Writing—original draft, T.M.K.; Writing—review & editing, T.M.K. and S.-J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by a grant of the Korea Health Technology R & D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI19C0829).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wu, S.; Chen, Y.; Wang, Q.; Li, M.; Wang, C.; Luo, X. CReam: A smart contract enabled collusion-resistant e-auction. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1687–1701. [\[CrossRef\]](#)
2. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern.* **2019**, *49*, 2266–2277. [\[CrossRef\]](#)
3. Gao, F. Data encryption algorithm for e-commerce platform based on blockchain technology. *Discret. Contin. Dyn. Syst. S* **2019**, *12*, 1457–1470. [\[CrossRef\]](#)
4. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [\[CrossRef\]](#)
5. Zheng, X.; Sun, S.; Mukkamala, R.R.; Vatrappu, R.; Ordieres-Mere, J. Accelerating health data sharing: A solution based on the Internet of Things and distributed ledger technologies. *J. Med. Internet Res.* **2019**, *21*, e13583. [\[CrossRef\]](#)
6. Khan, F.A.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaied, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [\[CrossRef\]](#)
7. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 23–25 October 2013; pp. 127–140.
8. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
9. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 15–29.

10. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
11. Mehar, M.I.; Shier, C.L.; Giambattista, A.; Gong, E.; Fletcher, G.; Sanayhie, R.; Kim, H.M.; Laskowski, M. Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *J. Cases Inf. Technol.* **2019**, *21*, 19–32. [\[CrossRef\]](#)
12. Ghaleb, B.; Al-Dubai, A.; Ekonomou, E.; Qasem, M.; Romdhani, I.; Mackenzie, L. Addressing the DAO insider attack in RPL's Internet of Things networks. *IEEE Commun. Lett.* **2019**, *23*, 68–71. [\[CrossRef\]](#)
13. Wadhaj, I.; Ghaleb, B.; Thomson, C.; Al-Dubai, A.; Buchanan, W.J. Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL). *IEEE Access* **2020**, *8*, 43665–43675. [\[CrossRef\]](#)
14. Dwork, C.; Naor, M. Pricing via processing or combatting junk mail. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992; pp. 139–147.
15. Jakobsson, M.; Juels, A. Proofs of work and bread pudding protocols. In *Secure Information Networks*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 258–272.
16. Song, R.; Song, Y.; Liu, Z.; Tan, M.; Zhou, K. GaiaWorld: A Novel Blockchain System Based on Competitive PoS Consensus Mechanism. *CMC Comput. Mater. Contin.* **2019**, *60*, 973–987. [\[CrossRef\]](#)
17. Zhao, Y.; Zhang, S.; Yang, M.; He, P.; Wang, Q. Research on Architecture of Risk Assessment System Based on BlockChain. *CMC Comput. Mater. Contin.* **2019**, *61*, 677–686.
18. Park, Y.; Choi, H.; Cho, S.; Kim, Y.G. Security Analysis of Smart Speaker: Security Attacks and Mitigation. *CMC Comput. Mater. Contin.* **2019**, *61*, 1075–1090. [\[CrossRef\]](#)
19. Albanese, G.; Calbimonte, J.-P.; Schumacher, M.; Calvaresi, D. Dynamic consent management for clinical trials via private blockchain technology. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1–18. [\[CrossRef\]](#)
20. Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research* **2017**, *6*, 1–66. [\[CrossRef\]](#)
21. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
22. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Jiang, X.; Liu, M.; Yang, C.; Liu, Y.; Wang, R. A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access. *CMC Comput. Mater. Contin.* **2019**, *58*, 45–59. [\[CrossRef\]](#)
24. Bordel, B.; Alcarria, R.; Martin, D.; Sanchez-Picot, A. Trust Provision in the Internet of Things Using Transversal Blockchain Networks. *Intell. Autom. Soft Comput.* **2019**, *25*, 155–170. [\[CrossRef\]](#)
25. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [\[CrossRef\]](#)
26. Yan, Y.; Dai, Y.; Zhou, Z.; Jiang, W.; Guo, S. Edge computing-based tasks offloading and block caching for mobile blockchain. *Comput. Mater. Contin.* **2020**, *62*, 905–915. [\[CrossRef\]](#)
27. Nguyen, B.L.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.V.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Comput. Mater. Contin.* **2020**, *65*, 87–107. [\[CrossRef\]](#)
28. Wang, Q.; Zhu, F.; Ji, S.; Ren, Y. Secure provenance of electronic records based on blockchain. *Comput. Mater. Contin.* **2020**, *65*, 1753–1769. [\[CrossRef\]](#)
29. Cheng, J.; Li, J.; Xiong, N.; Chen, M.; Guo, H.; Yao, X. Lightweight mobile clients privacy protection using trusted execution environments for blockchain. *Comput. Mater. Contin.* **2020**, *65*, 2247–2262. [\[CrossRef\]](#)
30. Ali, S.; Hafeez, Y.; Jhanjhi, N.Z.; Humayun, M.; Imran, M.; Nayyar, A.; Singh, S.; Ra, I.H. Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based. *IEEE Access* **2020**, *8*, 148007–148020. [\[CrossRef\]](#)
31. Singh, S.; Jeong, Y.S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* **2016**, *75*, 200–222. [\[CrossRef\]](#)
32. Naresh, V.S.; Pericherla, S.S.; Sita, P.; Reddi, S. Internet of things in healthcare: Architecture, applications, challenges, and solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421. [\[CrossRef\]](#)
33. Parvathavarthini, S.; Visalakshi, N.; Shanthi, S.; Mohan, J. An Improved Crow Search Based Intuitionistic Fuzzy Clustering Algorithm for Healthcare Applications. *Intell. Autom. Soft Comput.* **2020**, *26*, 253–260. [\[CrossRef\]](#)
34. Bailey, B.W.; LeCheminant, G.; Hope, T.; Bell, M.; Tucker, L.A. A comparison of the agreement, internal consistency, and 2-day test stability of the InBody 720, GE iDXA, and BOD POD (R) gold standard for assessing body composition. *Meas. Phys. Educ. Exerc. Sci.* **2018**, *22*, 231–238. [\[CrossRef\]](#)
35. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Muralidharan, S. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
36. Sharma, G.; Srivastava, G.; Mago, V. A framework for automatic categorization of social data into medical domains. *IEEE Trans. Comput. Soc. Syst.* **2020**, *7*, 129–140. [\[CrossRef\]](#)

37. Manevich, Y.; Barger, A.; Tock, Y. Endorsement in Hyperledger Fabric via service discovery. *Ibm J. Res. Dev.* **2019**, *63*, 1–9. [[CrossRef](#)]
38. Lahbib, A.; Toumi, K.; Laouiti, A.; Laube, A.; Martin, S. Blockchain based trust management mechanism for IoT. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference, Marrakesh, Morocco, 15–18 April 2019; pp. 1–8.
39. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and trustable electronic medical records sharing using blockchain. *Amia Annu. Symp. Proc.* **2017**, *2017*, 650. [[PubMed](#)]
40. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on PIMRC, Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
41. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [[CrossRef](#)]
42. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [[CrossRef](#)] [[PubMed](#)]
43. Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, *42*, 147. [[CrossRef](#)] [[PubMed](#)]
44. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* **2018**, *42*, 156. [[CrossRef](#)] [[PubMed](#)]
45. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **2018**, *42*, 141. [[CrossRef](#)]
46. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A patient agent to manage Blockchains for remote patient monitoring. *Stud. Health Technol. Inform.* **2018**, *254*, 105–115.
47. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [[CrossRef](#)] [[PubMed](#)]
48. Zhou, L.; Wang, L.; Sun, Y. Mistore: A blockchain-based medical insurance storage system. *J. Med. Syst.* **2018**, *42*, 149. [[CrossRef](#)] [[PubMed](#)]
49. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comp. Syst.* **2019**, *95*, 511–521. [[CrossRef](#)]
50. Casado-Vara, R.; Corchado, J. Distributed e-health wide-world accounting ledger via blockchain. *J. Intell. Fuzzy Syst.* **2019**, *36*, 2381–2386. [[CrossRef](#)]
51. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [[CrossRef](#)]
52. Hyla, T.; Peja's, J. eHealth integrity model based on permissioned blockchain. *Future Internet* **2019**, *11*, 76. [[CrossRef](#)]
53. Islam, N.; Faheem, Y.; Din, I.U.; Talha, M.; Guizani, M.; Khalil, M. A blockchain-based fog computing framework for activity recognition as an application to Healthcare services. *Future Gener. Comput. Syst.* **2019**, *100*, 569–578. [[CrossRef](#)]
54. Kuo, T.T.; Gabriel, R.A.; Ohno-Machado, L. Fair compute loads enabled by blockchain: Sharing models by alternating client and server roles. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 392–403. [[CrossRef](#)] [[PubMed](#)]
55. Li, X.; Huang, X.; Li, C.; Yu, R.; Shu, L. EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems. *IEEE Access* **2019**, *7*, 22011–22025. [[CrossRef](#)]
56. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access* **2019**, *7*, 66792–66806. [[CrossRef](#)]
57. Rahmadika, S.; Rhee, K.H. Toward privacy-preserving shared storage in untrusted blockchain P2P networks. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–13. [[CrossRef](#)]
58. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [[CrossRef](#)]
59. Silva, C.A.; Aquino, G.S.; Melo, S.R.; Egídio, D.J. A fog computing-based architecture for medical records management. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–16. [[CrossRef](#)]
60. Tian, H.; He, J.; Ding, Y. Medical data management on blockchain with privacy. *J. Med. Syst.* **2019**, *43*, 26. [[CrossRef](#)] [[PubMed](#)]
61. Wong, D.R.; Bhattacharya, S.; Butte, A.J. Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Commun.* **2019**, *10*, 917. [[CrossRef](#)]
62. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-familiarity: a privacy-preserved blockchain scheme for collaborative medical decision-making. *Appl. Sci.* **2019**, *9*, 1370. [[CrossRef](#)]
63. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [[CrossRef](#)]
64. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [[CrossRef](#)]
65. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; Abd El-Latif, A.A. DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access* **2020**, *8*, 111223–111238. [[CrossRef](#)]
66. Sharma, A.; Tomar, R.; Chilamkurti, N.; Kim, B.G. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics* **2020**, *9*, 1609. [[CrossRef](#)]
67. Kim, S.K.; Huh, J.H. Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records. *Electronics* **2020**, *9*, 763. [[CrossRef](#)]

-
68. Dor-Haim, H.; Katzburg, S.; Leibowitz, D. A novel digital platform for a monitored home-based cardiac rehabilitation program. *Jove J. Vis. Exp.* **2019**, *146*, e59019. [[CrossRef](#)]
 69. Subramaniaswamy, V.; Manogaran, G.; Logesh, R.; Vijayakumar, V.; Chilamkurti, N.; Malathi, D.; Senthilselvan, N. An ontology-driven personalized food recommendation in IoT-based healthcare system. *J. Supercomput.* **2019**, *75*, 3184–3216. [[CrossRef](#)]
 70. Holder, C.J.; Ricketts, S.; Obara, B. Convolutional networks for appearance-based recommendation and visualisation of mascara products. *Mach. Vis. Appl.* **2020**, *31*, 1–13. [[CrossRef](#)]
 71. Narayanasamy, S.; Markina, V.; Thorogood, A.; Blazkova, A.; Shabani, M.; Knoppers, B.M.; Prainsack, B.; Koesters, R. Genomic sequencing capacity, data retention, and personal access to raw data in Europe. *Front. Genet.* **2020**, *11*, 1–15. [[CrossRef](#)] [[PubMed](#)]
 72. Bild, R.; Bialke, M.; Buckow, K.; Ganslandt, T.; Ihrig, K.; Jahns, R.; Merzweiler, A.; Roschka, S.; Schreiweis, B.; Stäubert, S.; et al. Towards a comprehensive and interoperable representation of consent-based data usage permissions in the German medical informatics initiative. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 1–9. [[CrossRef](#)] [[PubMed](#)]
 73. Park, D.W.; Jeong, H.H.; Jeong, M.J.; Ryoo, H.S. Improving legislation on the use of healthcare data for research purposes. *Korean Soc. Law Med.* **2016**, *17*, 315–346.