electronics

MDPI

Article

A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital

Lei Hang [1], Eunchang Choi [2] and Do-Hyeun Kim [1,*]

[1] Department of Computer Engineering, Jeju National University, Jeju-si 63243, Korea; hanglei@jejunu.ac.kr
[2] Daegu-Gyeongbuk Research Center, Electronics and Telecommunications Research Institute, Daegu-si 42994, Korea; ecchoi@etri.re.kr
* Correspondence: kimdh@jejunu.ac.kr; Tel.: +82-64-7543658

Received: 27 March 2019; Accepted: 18 April 2019; Published: 25 April 2019

Abstract: Recent advancements in information and communication technology is enabling a significant revolution in e-Health research and industry. In the case of personal medical data sharing, data security and convenience are crucial requirements to the interaction and collaboration of electronic medical record (EMR) systems. However, it's hard for current systems to meet these requirements as they have inconsistent structures in terms of security policies and access control models. A new solution direction is essential to enhance data-accessing while regulating it with government mandates in privacy and security to ensure the accountability of the medical usage data. Blockchain seems to pave the way for revolution in the conventional healthcare industry benefiting by its unique features such as data privacy and transparency. In this paper, a blockchain-based medical platform using a smart contract is proposed to secure the EMR management. This approach provides patients a comprehensive, immutable log and easy access to their medical information across different departments within the hospital. A case study for hospital is built on a permissioned network, and a series of experimental tests are performed to demonstrate the usability and efficiency of the designed platform. Lastly, a benchmark study by leveraging various performance metrics is made and the outcomes indicate that the designed platform surpasses the ability of existing works in various aspects. The results of this work reveal that the proposed solution has the great potential to accelerate the development of a decentralized digital healthcare ecosystem.

Keywords: healthcahre; distributed ledger; medical blockchain; smart contract; EMR sharing

1. Introduction

e-Health is a technology that is growing in importance over time, varying from remote access to medical records, to real-time data exchange from different wearable sensors coming from different patients [1]. It is reported that the usage of electronic medical records (EMRs) has increased dramatically while only 9% of non-federal acute care hospitals used in them 2008, this rate reached to 96% by 2015 [2]. In general, an EMR is the digital collection of patient health information that is comprised of various features, including text document, images, and video data. The conventional EMR systems are designed to store data accurately and to capture the state of a patient across time. However, the issue of legal interoperability arises in the case of cross-border EMR sharing since different providers and hospital systems may have various legal requirements for the content or usage of EMRs, which would seriously obstruct the sharing of medical data. The lack of coordinated data management and exchange leads the personal medical data to be fragmented rather than unitive [3]. The innovation for healthcare systems reforms slowly under years of high regulatory pressure and inefficient bureaucracies. Nowadays, a critical need for such innovation arises since data science and personalization services prompt patients to participant in the details of their healthcare and restore intermediary over their medical

data [4]. Blockchain technology offers promising possibilities for a technological innovation to solve these issues in healthcare [5]. In one word, blockchain is an authenticated, and decentralized platform, holding a sequence of transaction logs in blocks like a conventional public ledger where a consensus driven approach is applied to reach an agreement among multiple untrusted entities through the use of the ledger. This would allow every participant (e.g., patient, provider, pharmacist, insurance company) in the medical ecosystem to submit their identities with qualifications to get an authority on the blockchain. With the given authority and the permission of the candidate, each participant would have access to the ledger and to those records that have already been collected in a digital format.

Current blockchains are essentially transparent platforms, using smart contracts [6] to interact between end users, realized by a secure digital identity reference, and are accessible to every network participant [7]. Blockchain technology can guarantee the data sharing and transparency between hospitals, insurance companies, and any other research centers by offering a normative mechanism to all network members for the exchange of the highly sensitive medical data. This can be achieved by providing the mechanism to reach consensus among untrusted entities, even without the governance of a centralized trusted party [8]. Any member healthcare organization that participates in a blockchain consortium is able to access the shared medical information, in spite of their native record system. The conventional healthcare organizations can benefit tremendously from the features of blockchain technologies in a number of respects, for example, treatments and diagnoses delivered via data sharing, and patient follow-up via transaction record tracking [9]. In short, the key benefits of applying the blockchain technology in healthcare can be summarized as follows: Transparency, irreversibility, encrypted and verifiable transactions, and integrity.

Existing studies of blockchain-based healthcare systems focus on a distributed ledger [10], a decentralized application (DApp) [11], smart contract development [12,13], and a permission-less network [14–19]. Most of existing studies concentrate on the permission-less network in which the participant identities are anonymous and therefore entirely untrusted. However, for the use case where the patient related data are highly sensitive, it is hard for the current permission-less blockchain technologies to fulfill this requirement. Data transparency may lead to critical issues in medical data sharing solutions, where a policy of confidentiality is required to offer the permission of the medical data only to a certain number of users [20]. Therefore, an additional access control policy that works asides the blockchain must be designed to force the privacy of contents in terms of user identity [21]. Health data ownership, and governance of the emerging EMR sharing infrastructure must be followed in a healthcare blockchain network [22]. Furthermore, most of the existing systems require the using of native cryptocurrency such as token to incent the costly mining, however the processing rate is in a low level. For example, the popular cryptocurrency platform Ethereum [23] has a limited capacity with a transaction speed of only up to 20 transactions per second. Many significant challenges [24] still exist in the development of healthcare systems by using this technology. As a result, a highly reliable healthcare blockchain network that can be systemically operated for enterprise use is still a formidable challenge for the existing blockchain approaches.

The contributions of this work can be summarized as follows: First, we propose a medical blockchain platform in which personal health data could be stored on a secure, permissioned chain and shared back and forth quickly like email. The designed blockchain platform moves towards a web-driven paradigm with the development of web front-end technologies such as JavaScript and HTML5 to improve management of the resources within the network. For example, user interfaces for creating and supervising participants, for visualizing EMR information, for submitting transactions, and for monitoring transaction history in blockchain. In addition, Representational State Transfer Application Programming Interfaces (REST APIs) are utilized to expose the product-specific services provided by the blockchain network. A smart contract is used to provided controlled access to the ledger in order to ensure the data consistency of the personal medical information and to host the ledger functions across the network. We also specify access control policy, which allows participants to access a certain number of contents or transactions that are authorized, for instance, only patients are

permitted to share health data to others. As blockchain technology is not intended for large transaction data payloads, we deploy the Couch DB alongside each peer to enable the large file storage and minimize the duplication across the entire blockchain filesystem. Lastly, we prove the practicability of our proposed approach by implementing a real-life case study in hospital, using the Hyperledger Fabric [25] which is a permissioned decentralized platform designed for building DApps or distributed ledger solutions on top of it.

The remaining of this paper is structured as follows: Section 2 gives a brief introduction on healthcare towards blockchain and overviews a number of the related projects. Section 3 describes the medical blockchain scenario, the system architecture, the design of the smart contract, and the general transaction process of the designed medical blockchain platform. Section 4 details the implementation of the case study on top of the designed platform and presents execution results of the case study with various snapshots. Section 5 presents the evaluation results of the proposed platform in different performance metrics and highlights the significance of the proposed work through a benchmark analysis with existing works. Section 6 discusses some of the limitations of the proposed system. Finally, Section 7 concludes the paper and discusses some future research directions.

2. Related Work

Nowadays, healthcare is witnessing an innovative approach to disease prevention and treatment that incorporates an individual patient's genetic makeup, lifestyle and environment. IT advancement has produced large data storage of health information and provided mechanisms to track engaged individuals more with their own healthcare. It can be speculated that by combining healthcare with information technology, it would bring a structural shift in the field of health IT. The blockchain is both a data structure and a timekeeping mechanism for that data structure. As a proof of the history of data, it is also easily reportable [26]. Blockchain technology shows the great potential to address interoperability challenges in current health IT systems and is hoped to become a part of the core technical standard, enabling individual users, healthcare providers, and medical research centers to share electronic health data in a more secure way [27].

The following section discusses some of the notable projects and applications for medical- and health-care built on blockchain. MediBloc [28] follows an open-source protocol and defines itself as a decentralized healthcare information ecosystem built on blockchain technology for patients, healthcare providers, and researchers. Its blockchain platform allows it to track and record everything revolving around your healthcare world such as doctors' visits and record updates. The platform is a DApp formulated on the Ethereum Virtual Machine (EVM). It uses the Medi Point system (MP), a points-based system that measures user participation. This token can be used in medical transactions such as insurance payments. MedRec [29] is a novel, decentralized record management system to handle EMRs, using blockchain technology. It leverages various blockchain properties to manage confidentiality, authentication, sharing and data accountability, which should be taken into account when processing sensitive medical information. This system is designed with a modular architecture that integrates with the existing data storage infrastructure and approaches, which makes the designed system more interoperable and adaptable. Furthermore, a unique incentive method is proposed to stimulate medical stakeholders (patient, health researchers, etc.) to act as miners in the blockchain network. Participants involved with the network can get access permission to aggregated and anonymized medical data as mining rewards, for contributing computing power to secure and sustain the network. MediLedger [30] is an initiative to establish the first peer-to-peer network for the pharmaceutical industry. The MediLedger network establishes a number of standards, interoperable protocol primitives that allow the pharmaceutical industry to easily exchange data across organizations. The network is powered by the blockchain in order to implement and execute cross-industry business processes and validate messages that are exchanged amongst the participants. Permission-based private messaging is used to share only the data the user wants to share with the partners they wants to share it with. It connects with trading partners and trusted service providers at the vanguard of

emerging solutions for the pharmaceutical industry. HealthCoin [31] is a blockchain technology-based currency, the seemingly different aspects of preventive healthcare—hospitals, employers, health plans, insurers, governments, non-governmental organizations, wellness apps—are brought under a single roof. The medical data is verified without any loss in transactions by using massive database analytics and nationwide collaboration, and a targeted program is developed to prevent various disorders. It works by tokenizing measurable improvements in health. Information about health apps, doctors, health plans, and insurer biometric screening is recorded. For diabetes, in particular, A1c, high-density lipoprotein, blood pressure, even gene markers, and family history is noted down which can indicate the affinity to develop Type II Diabetes. Connecting Care [32] is a digital care record sharing system used in several cities of England such as Bristol, North Somerset and South Gloucestershire. This system is made to provide secure access to import information held by hospitals and other health and social care organizations. It also allows clinical professionals involved in care to access users' health and social care records and reduces the time cost by professionals checking details from different health and social care organizations. Furthermore, it can also reduce delays to the treatment due to the lack of information. Connecting Care is only accessible to authorized users who have been assigned with work roles, which define user levels to which information they can see. Robomed Network [33] is another decentralized medical network intended to provide effective medical care services. As the value criteria of clinical pathways, a smart contract is utilized by this project to connect healthcare service providers and patients. This particular concept which focus on patient outcomes has driven the conventional healthcare market in to a new era, which creates a single point of care for patients. Robomed Network issues its own tokens to support a smart contract between healthcare providers and patients. A comprehensive review of potential application using blockchain technologies in terms of healthcare is discussed in [34]. For example, the authors in [35] propose a novel blockchain framework specified for resource-constraint medical devices. To eliminate the use of mining, a lightweight cryptographic approach based on key pairs are presented. This method ensures the patient-centric access control for medical data over the blockchain network. This work gives a good indication to make Internet of Things (IoT) data secure and transparent using the blockchain technologies. FHIRChain is another system utilizing the smart contract for exchanging health data in standard Fast Healthcare Interoperability Resources (FHIR) [36], where clinical data is stored off chain while the blockchain itself stores encrypted metadata which act as references to the primary data source. The authors in [37] propose a user-centric health data sharing solution on the basis of a permissioned blockchain network. A mobile application is implemented to collect health data from wearable health devices and synchronize data to the cloud for sharing with other partners. A similar mobile-based system proposed in [38] uses smartphones to collect and send EMR data to a permissioned blockchain network. The authors in [39] propose a secure and trustable EMR management system using permissioned blockchain. The designed system enables the EMR (specified for cancer patient care) data sharing between healthcare providers and research studies. The EMR data registered to the blockchain network is resistant to tampering and revision. A provenance system based on a distributed network and smart contracts is proposed [40] to instrument some widely used international EMR standards such as Integrating the Healthcare Enterprise (IHE) and Health Level Seven International (HL7). A proof of concept implementation is built on a permissioned network to indicate the usability and efficiency of the proposed architecture.

Some of these existing systems are built on a permission-less blockchain network where anyone can participate. In order to mitigate the absence of trust, these existing systems usually employ the use of native cryptocurrency or transaction fees that can result in high computing power consumption. Although a few works are built on a permissioned network, these works only focus on the sharing of EMR data and is not suitable for a deployment in a practical product environment. This paper aims to solve all these issues and presents a flexible and easy-to-use blockchain platform that can be deployed in real hospitals.

3. Proposed Medical Blockchain Platform for EMR Integrity Management

3.1. System Architecture of the Proposed Medical Blockchain Platform

Blockchain provides a unique opportunity to provide benefits in the healthcare industry. Figure 1 presents a graphical description of the conceptual architecture, where the medical blockchain preserves a complete up to date history of all medical data, covering the EMR, visits, prescriptions, billing, and IoT data, which would follow an individual user for life. The medical data lake is an independent data repository, known as stored-off blockchain. It would be a valuable tool used for a variety of analysis not only restricted to hospital usage, for example, in health insurance and disease prevention and research.

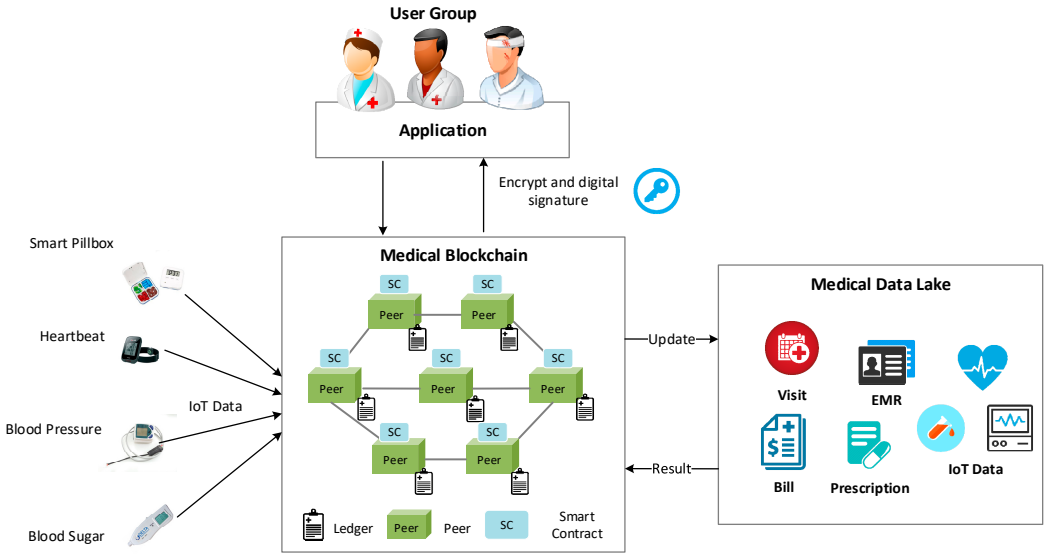


Figure 1. Conceptual scenario of medical blockchain.

More precisely, the medical blockchain network consists of trusted validating peers and each peer holds a copy of the ledger for the network in order to maintain the consistence of the distributed ledger. The ledger consists of a blockchain to store the immutable, sequence transaction record in blocks, and a data lake to maintain various medical data. The blockchain is a transaction log that records all the changes resulted in the data lake while the data lake is an off-chain state database that holds the current values of a set of data, for example, the latest EMR of a patient. IoT-connected devices enable medical devices capable of transmitting data on an ongoing basis. These data are useful in data analytics and ultimately produce a variety way of services such as preventive care and critical care response. The healthcare providers can assist their patients faster and more accurately with the instant sharing of IoT data. The user group contains users in different roles, for example, the administrator who is able to manage all the resources within the hospital. The doctor can check all the information of patients and give a prescription for the treatment. The pharmacist instructs and suggests on the proper use and side effects of prescribed drugs and medicines. The patient can access their medical data through any network peer where their information is preserved. Moreover, the patient is allowed to set up the access permission of their medical information to any other doctors within the network. This is realized by specifying the access control policy in the smart contract, which will be deployed into the entire blockchain network to ensure the patient's privacy and data security. All the interactions between the end user and medical blockchain are encrypted with a digital signature to ensure the security of the system.

Figure 2 describes the main technical components and gives a solid understanding of the proposed medical blockchain platform. The designed platform encompasses not just a technical infrastructure but also a user service framework that exposes the distributed ledger and smart contract as services to applications. The end user (patient, doctor, nurse, admin, etc.) can submit transaction proposals to the

blockchain network through the application to invoke services such as reservation, the EMR, payment, and identity services provided by the blockchain network. A transaction can be defined as a process of creating, updating, deleting or transferring EMR data that is performed among the connected peers. In order to conduct private and confidential transactions, we apply the concept of subnetwork to separate the overall network into different private networks which allow communication between two or more specified departments. In case they want to keep medical data private from other departments, these departments are allowed to create their own subnetworks, comprising the necessary departments who require data accessing. This is of great significance for enterprise usage, as some participants may be competitors and not want every transaction they make known to all, for example, a special price they're offering to some participants and not others.

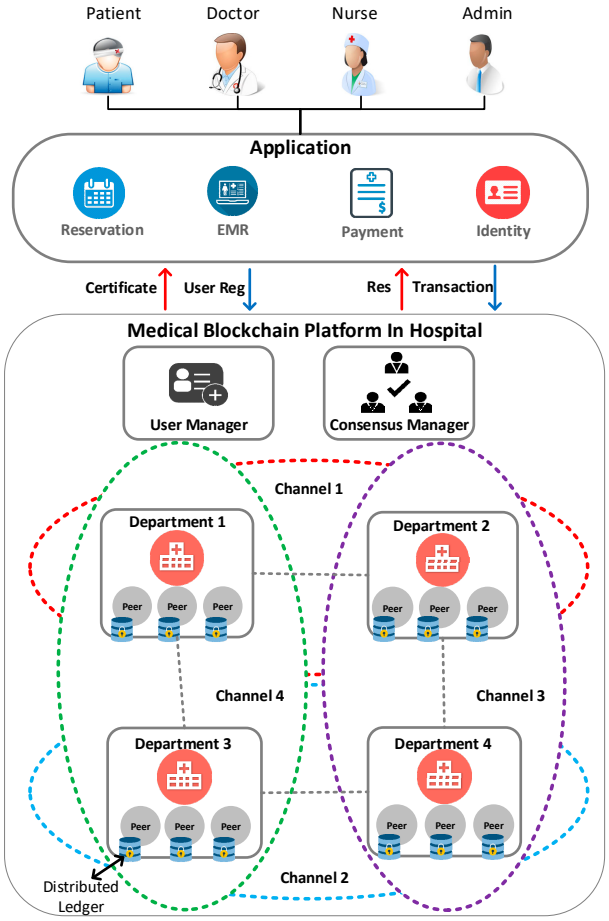


Figure 2. Proposed medical blockchain platform for electronic medical records (EMRs) integrity management.

The most notable point which makes the proposed platform different from some other blockchain systems is that it is built on permissioned network. Rather than an open permission-less system that allows unknown identities to participate in the network, the members of the designed blockchain network enroll through a trusted user manager. The user manager abstracts away all cryptographic mechanisms and provides a number of certificate services. More specifically, these services relate to user enrollment, the rules by which those identities are governed (identity validation) and authenticated (signature generation and verification), and secured connections between users or components of the blockchain. In order to meet the diversity of enterprise use case requirements, the proposed platform has been designed to have a modular structure, where pluggable consensus on the order of transactions can be swapped in and out, smart contracts run within a container environment, ledger data can be stored in a variety of storage technologies, and different identity management protocols

are supported. The consensus manager provides the interface through which departments can connect to the subnetwork and is responsible for the order of transactions and whether to insert into the final block. Each department in the medical blockchain consists of various peers, which contain the smart contract and data storage to endorse proposal for transaction or write block of transaction to the ledger. The distributed ledger records the transparent and immutable history corresponding to all actions that have happened to the network. Consensus protocol and cryptographic primitives such as hashing and digital signatures are employed to make sure the consistence of every copy of the ledger.

Figure 3 details the internal structure of a single peer in the blockchain network. State component is the database in which the state of the ledger at a given point in time is described. The block component records all the transactions to keep a record of the update history for the world state, where all transactions are in the order in which they occur and resulted in the current value of the world state. Therefore, the ledger is a combination of the state database and the transaction log history. Figure 3 gives a sample to describe the relation between block and state, we can see that the ledger state contains state that correspond to patient 1, patient 2, and patient 3. Each patient has a specific key along with a value that indicates its name and gender. There are four blocks in the blockchain, in which block 0 is the genesis block, which does not contain any transactions that relate to patients. Each of the other three blocks contains a single transaction and these transactions are associated with the corresponding patient in the ledger state. The policy defines which peers need to agree on the results of a transaction before it can be added to the ledger. For example, AND ('Dept1.member', 'Dept2.member') requests one signature from both of the departments. The policy is specified for a subnetwork's smart contract at instantiation time. The business logic of the blockchain application is written as a smart contract, functioned as a distributed application, which gains its security from the blockchain and the underlying consensus among the peers. A smart contract is installed onto peers and instantiated to one or more subnetworks. The client application which is external to the blockchain network, invokes the smart contract in order to interact with the world state database of the ledger.

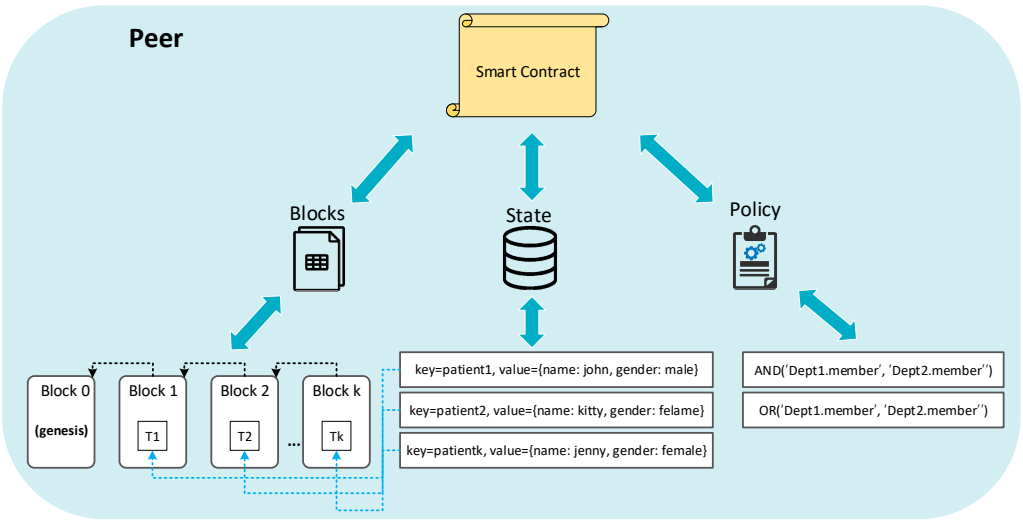


Figure 3. Detailed internal structure of peer in medical blockchain platform.

3.2. Smart Contract in the Proposed Medical Blockchain Platform

The smart contract functions as a trusted distributed application that gains its trust from the blockchain and the underlying consensus among the peers. Most of the smart-contract based blockchain platforms, ranging from permission-less platforms such as Ethereum to permissioned platforms such as Quorum [41] and Tendermint [42]. Smart contracts executed in an order–execute blockchain architecture must be deterministic in order to reach consensus among all of the peers. In principle, smart contracts used in these platforms are written in a non-standard, or domain-specific language (such as Solidity) so that non-deterministic operations can be eliminated. This becomes one of the

greatest challenges to the wide-scale usage of the smart contract because blockchain developers must learn a new language to write smart contracts, and this may lead to various problems in coding. Moreover, transaction execution performance and scale are limited since all transactions are executed by all peers in sequence. To address these issues, we deploy smart contracts to a specified subset of peers rather than to all peers, hence, the transaction need only be executed by a set of peers. This approach also supports parallel execution, which can prominently increase overall performance and scale of the system. Furthermore, we use the standard languages such as Node.js or Java to code the smart contract so that developers can use their familiar programming languages without spending time learning a new language. As shown in Figure 4, the smart contract in the proposed system contains various functions that allow users to interact with the ledger. For example, users can create, update, and query their personal EMR information by submitting transactions to the smart contract. The application running on the smart contract receives the transaction and runs different kinds of queries and updates, in turn, appends the transaction in the blocks and updates the ledger state. In the end, the ledger updating result is returned to the application as the response.

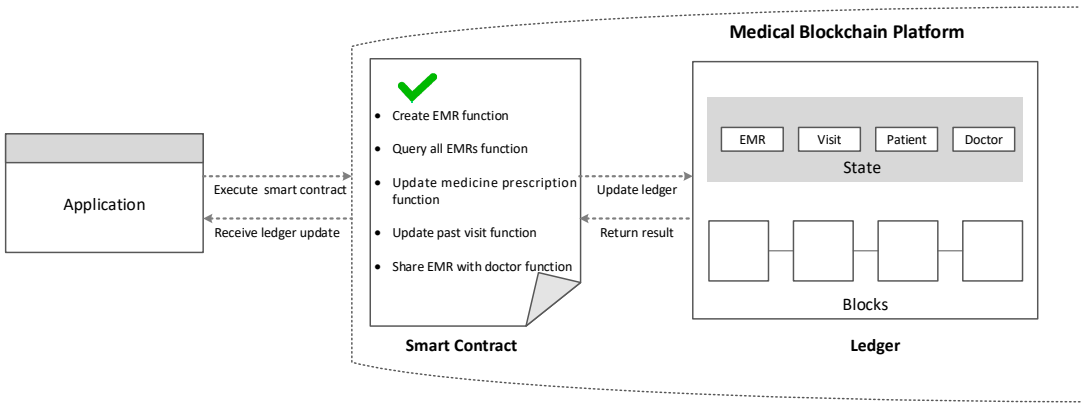


Figure 4. Ledger query and updating using smart contract.

3.3. Transaction Process of the Medical Blockchain Platform

This section details the transactional mechanics that taken place during a transaction operation over the blockchain network as shown in Figure 5. The client application must have credentials issued by the user manager so as to get the authorized permission for submitting transaction proposals. The user manager owns user IDs and authenticates clients who want to enroll in the network. Transactions start out with client applications sending transaction proposals to peers and the communication between the network and client application happens over the application software development kit (SDK). These peers can either be endorser or committers, endorsers simulate and sign transaction proposals, respond granting or deny approval while committers validate transactions results prior to writing block of transactions to the ledger. There is an overlap between endorser and committer peers, as we can say endorser peers can be a special kind of committer peers that must hold a smart contract. Each endorser peer receives and executes the transaction proposal by invoking the smart contract in their own simulated environment without updating the ledger. The endorser peers will capture the set of read and written data, called RW sets. These RW sets capture what was read from the current world state as well as what would have been written to the world state according to the transaction been executed while simulating the transaction. These RW sets are then signed by the endorser peer and returned to the client application. The client application packages the signed transaction which is a response to the results of the simulated transaction and then submits this transaction along with RW sets to the consensus manager. Consensus happens across the network, in parallel with signed transactions and RW sets are submitted, then these data are ordered into a block, and delivered to all committer peers. Each committer peer validates the transaction by verifying whether the RW sets match the current world state. When the committer peers validate the transaction, the transaction

is written to the ledger, and the world state is updated with the write data from the RW set. Lastly, the committing peers asynchronously notify the client application whether the submitted transaction succeed or not. These events can be subscribed by client applications in order to be notified by each committer peer when events occur.

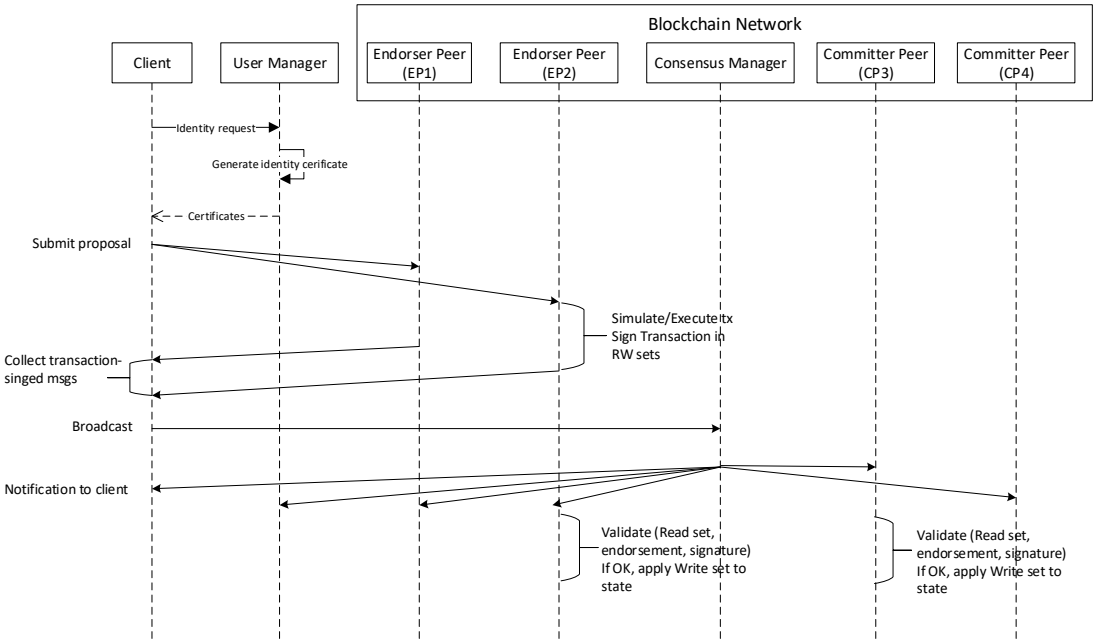


Figure 5. Medical blockchain platform transaction operational process.

4. Design and Implementation for EMR Integrity Management in the Medical Blockchain Platform

4.1. Development Environment

The proposed case study consists of two parts as shown in Figure 2, so that the development environments are summarized into two tables to describe each part, respectively. The technology stacks for implementing the medical blockchain network are depicted as shown in Table 1. The operating system is Ubuntu Linux v18.04.2 (Canonical Ltd, London, United Kingdom) LTS with Intel Core i5-8500 @ 3.00 GHz processor (Intel, Santa Clara, CA, USA) and 8 GB memory. Docker engine (v18.06.1-ce, Docker, San Francisco, CA, USA) provides the docker running environment and docker-compose (v1.13.0, Docker) provides the integrated development environment (IDE) to configure docker images and containers in the virtual machine. The Hyperledger Fabric (v1.2, Linux Foundation, San Francisco, CA, USA) project, is an open-source blockchain framework hosted by the Linux Foundation. Node (Linux Foundation) and Python (Python Software Foundation, Wilmington, DE., United States) are installed to implement the client SDK and smart contract. The web playground provides a user interface to design and generate the smart contract definition containing existing assets and the transactions related to them. Composer CLI tool (Linux Foundation) enables developers and administrators to deploy and managed smart contract definitions. REST APIs which are generated by the REST server, including participant API, asset API, transaction API, and query API that expose the blockchain logic to web or mobile applications.

Table 1. Development environment for the medical blockchain network.

Component	Description
CPU	Intel Core i5-8500 @ 3.00 GHz
Memory	8 GB
Operating Systems	Ubuntu Linux 18.04.1 LTS
Docker Engine	Version 18.06.1-ce
Docker-Compose	Version 1.13.0
Node	v8.11.4
Python	v2.7.15
Hyperledger Fabric	v1.2
IDE	composer-playground
CLI Tool	composer-cli, composer-rest-server

Table 2 presents the development technologies and tools to implement the medical blockchain client application. We have used a variety of web techniques such as HTML, Cascading Style Sheets (CSS), and JavaScript to construct the backbone of the web application. Two popular open-source toolkits, Bootstrap (Bootstrap, San Francisco, CA, USA) and jQuery (jQuery Foundation, San Francisco, CA, USA), are used to help in prototyping the frontend of the web application in order to provide a more user-friendly way to visualize the information. The client can interact with the REST server so that the end user can invoke the APIs to perform their functionalities by HTTP requests such as GET and POST.

Table 2. Development environment for the medical blockchain web app.

Component	Description
Operating System	Windows 10 Pro 64 bit
IDE	WebStorm (2018.2.2)
Browser	Firefox, Safari, Google Chrome
Library and Framework	Bootstrap, jQuery
Programming Language	HTML, CSS, JavaScript

4.2. Medical Blockchain Network Topology

Figure 6 overviews the sample network topology for the medical blockchain based on Hyperledger Fabric. The network topology includes four departments, surgery, dentistry, neurology, and neurosurgery (represented as D1, D2, D3, and D4) in two channels. These four departments have jointly written into an agreement of network policy that they will set up and initialize a blockchain network. D1 and D2 call for a private communication within the channel and so do D3 and D4. Channel 1 (C1) is governed according to the policy rules specified in channel policy 1 (CP1) established by D1 and D2. It is under the control of peer 1 (P1) and peer 2 (P2), where smart contract 1 (SC1) and ledger 1 (L1) are hosted. Similarly, channel 2 (C2) is governed by channel Policy 2 (CP2) established by D3 and D4. It is managed by peer 3 (P3) and peer 4 (P4), where smart contract 2 (SC2) and ledger 2 (L2) are hosted. It is worth nothing that one department can hold multiple peers in our use case, for example, two peers per department. The ordering service acts as a network peer manager that can create a channel or allow other peers to join the specific channel. It also supports the communication with channel C1 and C2, for the sake of ordering transactions into blocks per channel. Client applications A1, A2 can use C1 to connect to other network entities while A3, A4 are permitted to do this on C2. Each of the departments is associated with a permanent certificate authority (CA), for example, client application A1 belongs to department D1 is issued by certificate authority CA 1. CA issues public key infrastructure (PKI) based certificates to network member departments and their users.

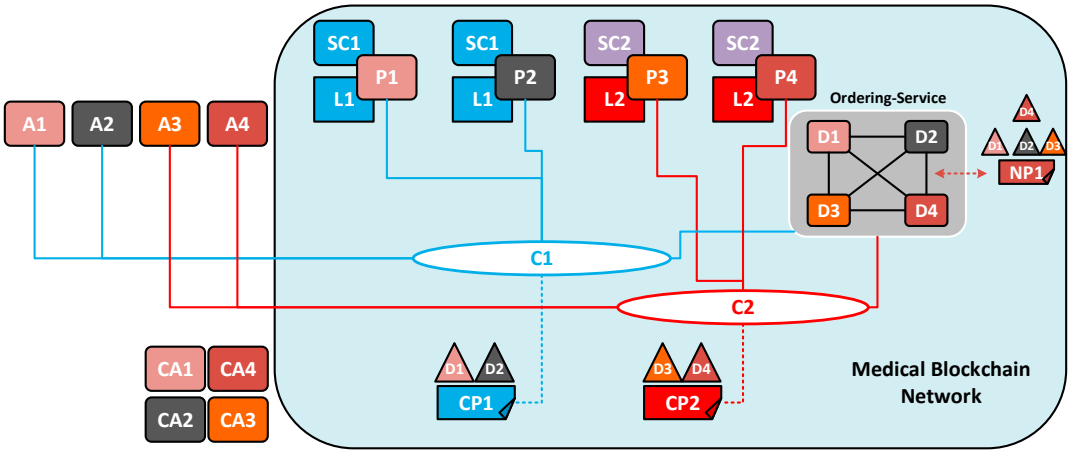


Figure 6. Sample medical blockchain network topology based on Hyperledger Fabric.

4.3. Smart Contract Modeling of the Medical Blockchain Platform

The smart contract is designed and implemented by using the Hyperledger Composer [43], which makes it easier to integrate the blockchain applications with the existing business systems. The smart contract consists of a model, script, access control rules, and query definitions. Participants are members of a business network, who own assets and submit transactions. In this case, they can be patients, doctors, nurses, and any other identities within a hospital. Participant types are modeled and must have a unique identifier to be identified by the network. Assets can be goods, services, or property, and are stored in registries. They can represent almost anything in a business network, for example, as represented in Table 3, EMR that typically contains general information such as personal information and medical history of the treatment. It specifies the contents and format of the EMR asset, which is preserved in the state database. Detailed structure of the state database is discussed in the next subsection.

Table 3. EMR definition in the medical blockchain.

Component	Type
patient_record_id	String
patient_id	String
doctor_id	String
name	String
day_of_birth	String
gender	String
address (country, city, street, zip)	String
contact_details (email, phone)	String
visit_date	DateTime
procedure (e.g., blood testing)	String array
medicine_prescribed (e.g., Aspirin)	String array

As part of the smart contract, transactions are defined to interact with assets. Participants can interact with them and each of which can be associated with an identity, across multiple blockchain networks. Events are defined in the same way as assets or participants. Once events have been defined, they can be included in the transaction processor functions to be emitted as part of a transaction. These definitions mentioned above are described in the model file, and Table 4 presents part of the transactions and events defined in this file.

Table 4. Transaction and event definition in medical blockchain.

Component	Type	Role
Share record with doctor	Transaction	Set the record access permission
Update past visits	Transaction	Update the past visit array in record (date, procedures, medications)
Update appointment	Transaction	Update the specific appointment (time)
Send bill	Transaction	Send the bill info to a specific patient
Pay bill	Transaction	Pay the bill to a specific money pool
Share record with doctor notification	Event	Inform that the record is shared with the specific doctor
Update past visits notification	Event	Inform that the past visit info is updated by the specific doctor
Update appointment notification	Event	Inform that the appointment is updated by the specific regulator
Send bill notification	Event	Inform that the bill is sent to the specific patient
Pay bill notification	Event	Inform that the bill is paid by the specific patient

The script file specifies the transaction process functions that act on assets and participants to either create, update or delete properties on assets and participants. As shown in Figure 7, transactions processor functions are written in JavaScript as part of a smart contract definition. The structure of transaction processor functions includes decorators and metadata followed by a JavaScript function, both parts are required for a transaction processor function to work. This function defines the share record type as the association transaction and defines it as the parameter record. It updates the EMR record asset in the registry, and then emits an event.

```
/**
* Share the patient record with doctor
* @param {composers.healthrecords.shareRecordWithDoctor} record - the shareRecord transaction
* @transaction
*/
async function shareRecordWithDoctor(record) {
    //payBill.patient.balanceDue -= payBill.bill.amount;
    return getAssetRegistry('composers.healthrecords.PatientRecord')
        .then(function(assetRegistry){
        record.patientRecord.doctor = record.doctorId;
        console.log(record.patientRecord.doctor);
        let factory = getFactory();
        let shareRecordEvent = factory.newEvent('composers.healthrecords', 'shareRecordWithDoctorNotification');
        shareRecordEvent.patientRecord = record.patientRecord;
        emit(shareRecordEvent);
        return assetRegistry.update(record.patientRecord);
    })
    .catch(function (error) {
    // Add optional error handling here.
    });
}
```

Figure 7. Transaction processor function in script file.

The access control file is an optional file, which describes assets or groups of assets and defines the participants who can perform operations which affect those assets and under what conditions. Queries are written in a bespoke query language and are defined in a single query file within a smart contract definition. By using queries, data can be easily extracted from the blockchain network. As shown in Figure 8, queries contain a description and a statement. The query descriptions are a string that describe the function of the query. The query statements contain the operators and functions that control the query behavior. For example, we can use the following queries to return all EMRs or specific EMRs with an identity parameter such as record identity and patient identity.

Table 5 summarizes a part of REST APIs generated by the composer-rest-server for communication between the web client and the medical blockchain platform. The resource typically represents the path of the data entity, and the verb specifies the desired action to be performed for a given resource along with the request, for example, the GET request is used to retrieve the information of a data entity, while for creating a new entity on the resource, the POST request is used. There is an observance in place such that a GET request to an entity Uniform Resource Identifier (URI) such as /api/PatientRecord returns a list of EMRs, probably matching some criteria that are sent with the request.

```
/**
 * Queries for EMR blockchain business network
 */

query selectHealthRecords {
  description: "Select all health records"
  statement:
      SELECT composers.healthrecords.PatientRecord
}

query selectHealthRecordByPatientRecordID {
  description: "Select health record by record ID"
  statement:
      SELECT composers.healthrecords.PatientRecord
          WHERE (PatientRecordID == _$PatientRecordID)
}

query selectHealthRecordByOwner {
  description: "Select health record based on their owner"
  statement:
      SELECT composers.healthrecords.PatientRecord
          WHERE (patient == _$patient)
}
```

Figure 8. Query definition in medical blockchain.

Table 5. HTTP requests in Representational State Transfer Application Programming Interfaces (RESTful API).

Resource	Verb	Action
/api/Patient	GET, POST, PUT, DELETE	Patient management
/api/Doctor	GET, POST, PUT, DELETE	Doctor management
/api/Regulator	GET, POST, PUT, DELETE	Regulator management
/api/PatientRecord	GET, POST, PUT, DELETE	EMR management
/api/updatePastVisits	POST	Update EMR
/api/shareRecordWithDoctor	POST	Share EMR with doctor
/api/Bill	GET, POST, PUT, DELETE	Medical bill management
/api/sendBill	POST	Send medical bill to patient
/api/payBill	POST	Pay medical bill to hospital
/api/HospitalMoneyPool	GET, POST, PUT, DELETE	Hospital moneypool management
/api/system/historian	GET	Retrieve transaction history

4.4. Distributed Ledger Storage Structure of the Medical Blockchain Platform

This section explains the ledger structure of the proposed medical blockchain platform, which has been divided into two distinct parts, a world state and a blockchain. The world state, also known as the current state, is a database used to hold the current values of a set of ledger states. This approach greatly enhances the transaction processing performance since we do not need to traverse the overall transaction log. The world state changes ceaselessly each time the state value is updated, such as when a new house is created, or the ownership of a house is transferred from one owner to another. CouchDB is a state database that provides rich query support when the smart contract data is modeled as JavaScript Object Notation (JSON). Namely, the data must be modeled in JSON format in order to perform content-based JSON queries in CouchDB. It supports various query methods such as get, put, and delete in conjunction with a state key, which enables the application to invoke smart contract to access world states through simple APIs. The example in Figure 9 shows ledger states for one record, record1 in CouchDB, which contains a key and a value. The Couch DB supports a simple state value with only one key-value pair and a complex state value with multiple key-value pairs as well.

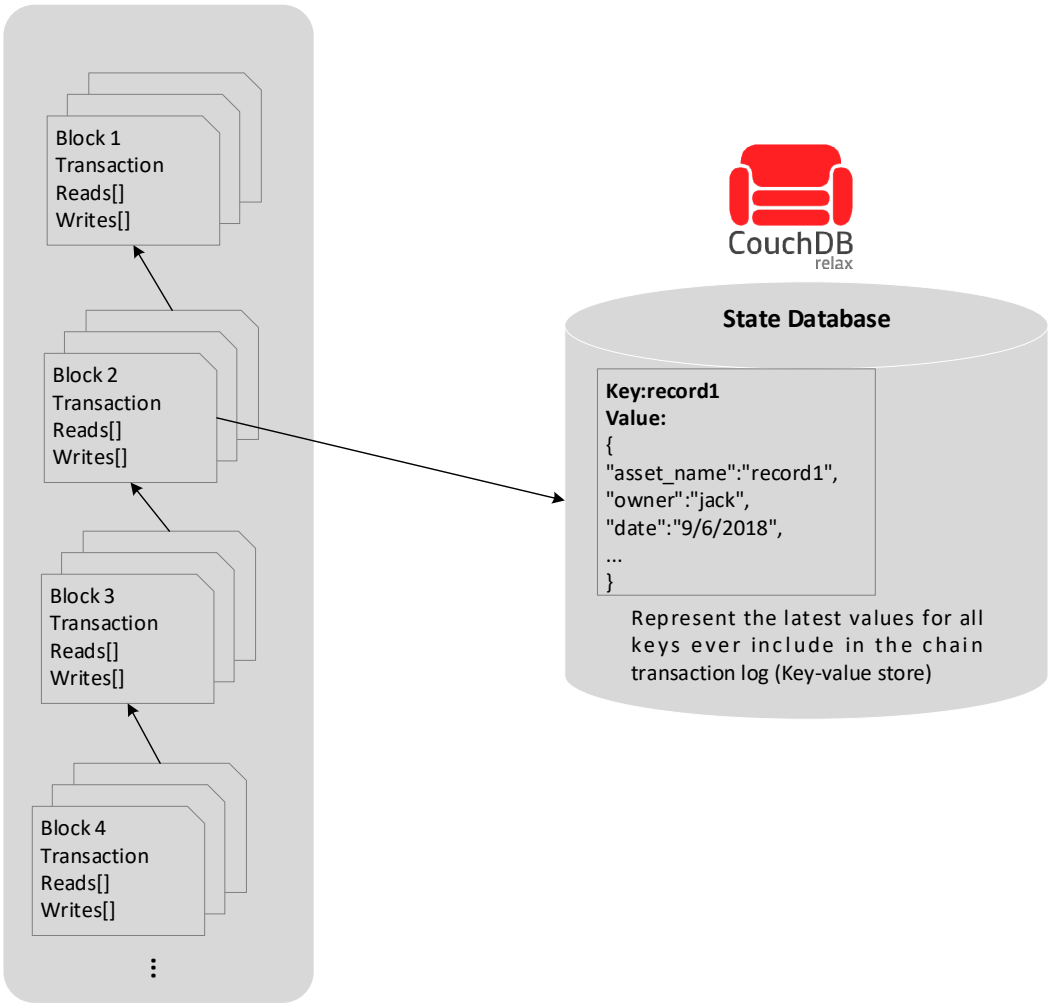


Figure 9. Distributed ledger storage structure of the medical blockchain.

In contrast to world state, the blockchain is physically implemented in a file, which is a wise design choice as the blockchain data structure is always used to record a limited small set of simple operations. The blockchain is a transaction log that records all the changes that represents the world state. Transactions are therefore collected into blocks that are cryptographically linked together to form a sequence of chain, where all transactions on the ledger are sorted in time order, enabling the user to know the history changes that happened in the world state. A most remarkable difference between the blockchain data structure and the world state is the data immutability, once data is written, it cannot be modified even by the network administrator. A block contains a hash value of the transactions and a copy of the hash value of the prior block in order to insure the security of the ledger data. Even if the ledger hosted by one peer was tampered with, it would not be able to convince all the other peers because the ledger is distributed throughout a network of independent peers.

4.5. Execution Process of the Medical Blockchain Platform

The section discusses the execution process of the proposed medical blockchain platform. Figure 10 represents the user identity registration and enrollment, which is the indispensable stage before the user can access the system. To obtain the identity for a user, the network administrator submits the registration request to the enrollment CA, which issues a secret for the enrollment process. Enrollment request is then sent from the client to the CA passing the enroll ID and secret obtained in the registration process. In response, the CA passes the Enrollment Certificate (ECert) along with the public key.

The ECert is used to request for the Transaction Certificate (TCert), and the transaction CA passes the TCert along with the private key for signing the transactions.

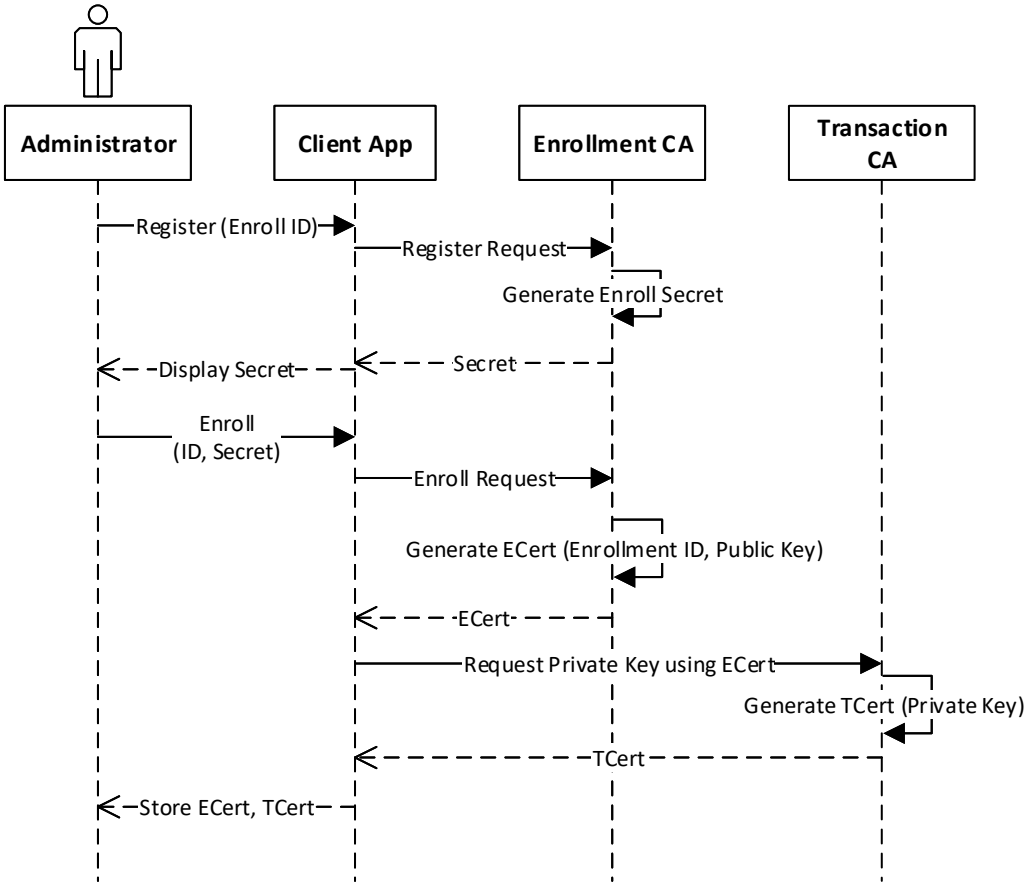


Figure 10. User identity registration and enrollment in the medical blockchain.

After enrollment, the patient is allowed to access the blockchain platform with the issued certificate. Figure 11 illustrates various operational processes to submit the transaction for generating an EMR and sharing the EMR in blockchain. The patient can input information of the EMR through the client application, and the client generates the transaction proposal request using the POST method to invoke the smart contract function on the endorser peers. The smart contract is then executed to produce transaction results and the set of these values are passed back to the client. The client application verifies the proposal responses according to the endorsement policies and broadcasts the endorsed transactions to the ordering service. The ordering service orders them chronologically by channel and creates blocks of transactions per channel. Then the blocks of transactions are delivered to all peers on the channel for validation. Each peer appends the block to the chain and the EMR record is saved to the current state database. Finally, an event is emitted to the client application to inform the patient that the EMR is created in the blockchain. To share the EMR to a particular doctor, the patient should set the doctor ID to specify who can access their EMR record through the client application. The rest of the transaction processes are similar to those in the EMR generation transaction. Lastly, an event is emitted to inform the patient that the EMR has been shared with a certain doctor and the transaction has been attached to the blockchain.

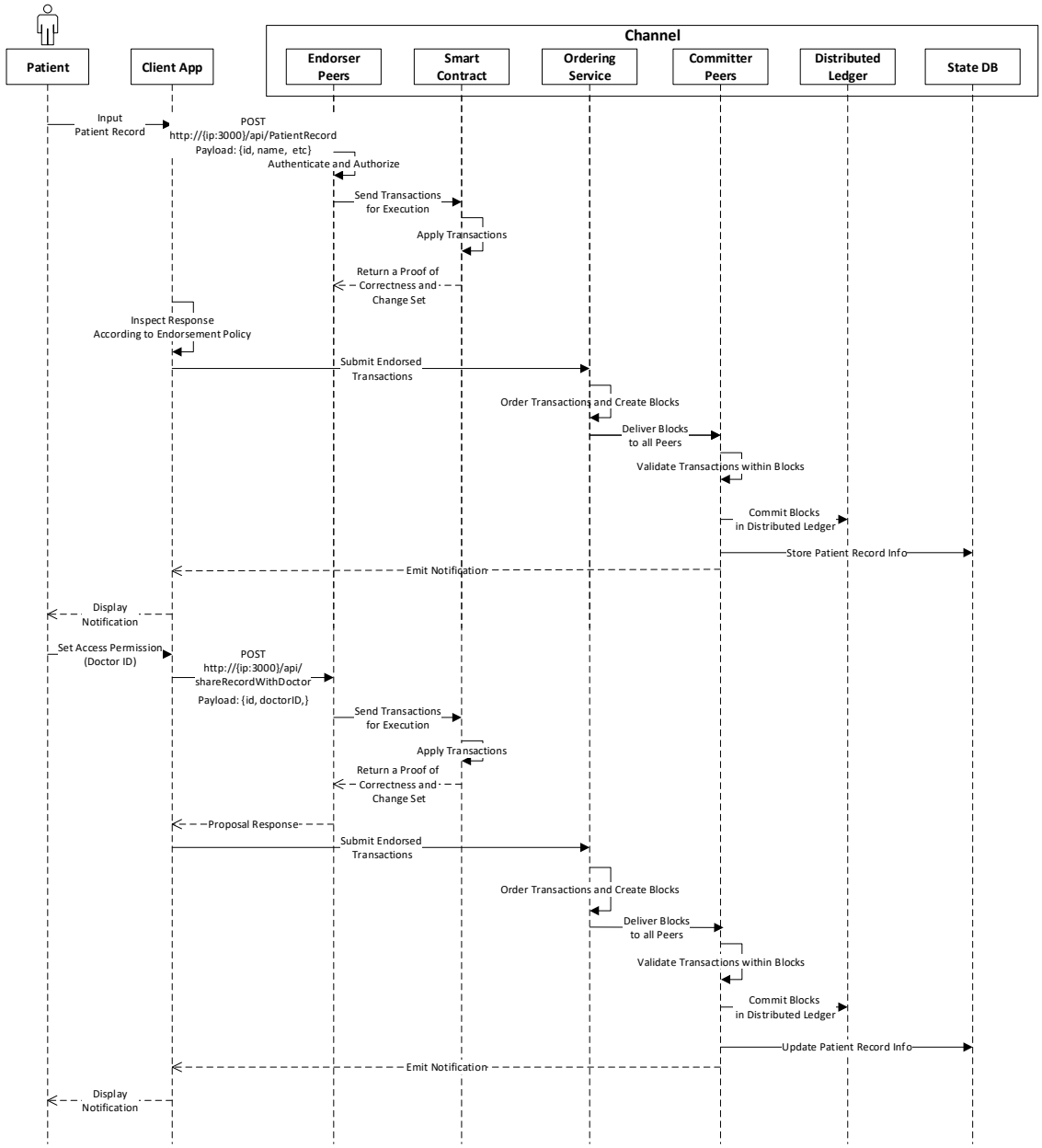


Figure 11. EMR generation and sharing in the medical blockchain.

Figure 12 represents the execution procedures for a doctor to query the shared EMR. The doctor can request the API endpoint using the GET method to query the EMR record from the state database using the patient ID. As the smart contract only queries the ledger, the platform would not submit the transaction to the consensus service since all of peers keep a local copy of the ledger so that no consensus process is required, therefore, the query result of an EMR is returned immediately.

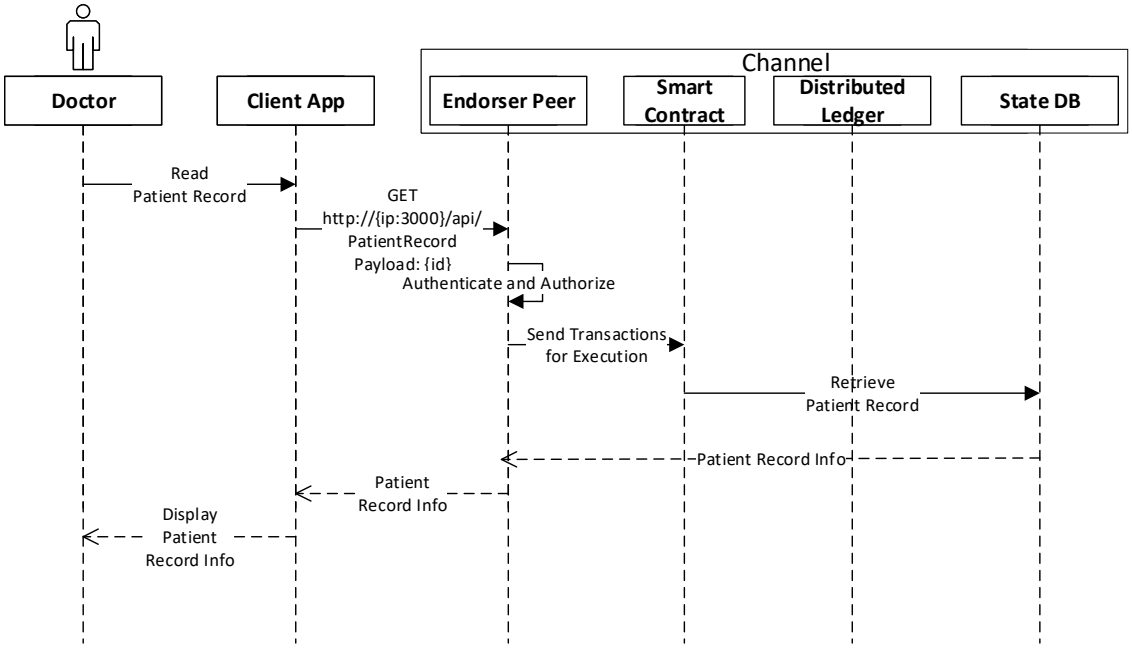
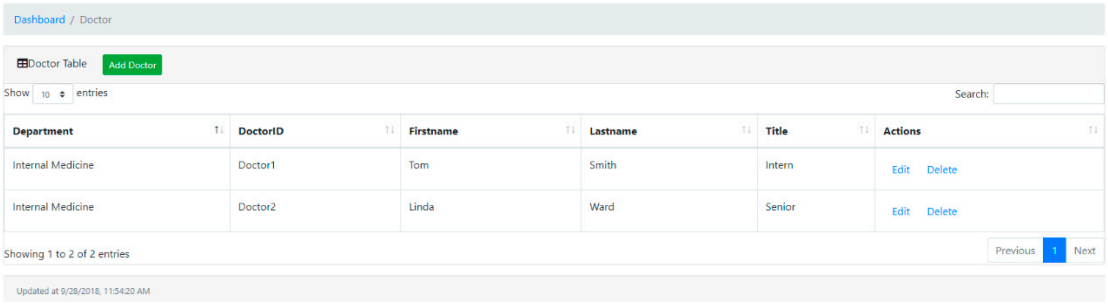


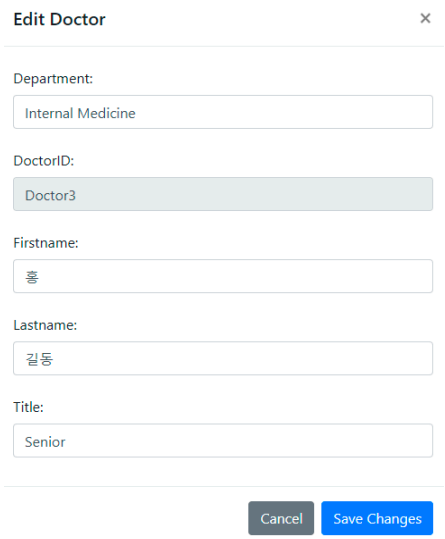
Figure 12. EMR query in the medical blockchain.

4.6. Execution Results

This section overviews some snapshots of various user interfaces in terms of the communications endpoints shown in Table 5 along with their respective responses displayed through the web interface. The client initializes a request to the REST server for submitting the transaction to the medical blockchain network after the user identity is authenticated by the network. The blockchain network invokes the relevant functions in the smart contract to perform the transaction accordingly and returns the response to the client when the transaction is executed. Figure 13 represents the snapshot of the doctor dashboard which includes the department, doctor ID, name, and title. The dashboard provides web editors which enables users to update or delete the selected doctor. As shown in Figure 13b, the user can modify the information of the specified doctor, and after confirming the operation, the request is sent to the blockchain network, in turn, the dashboard will be repopulated according to the response.



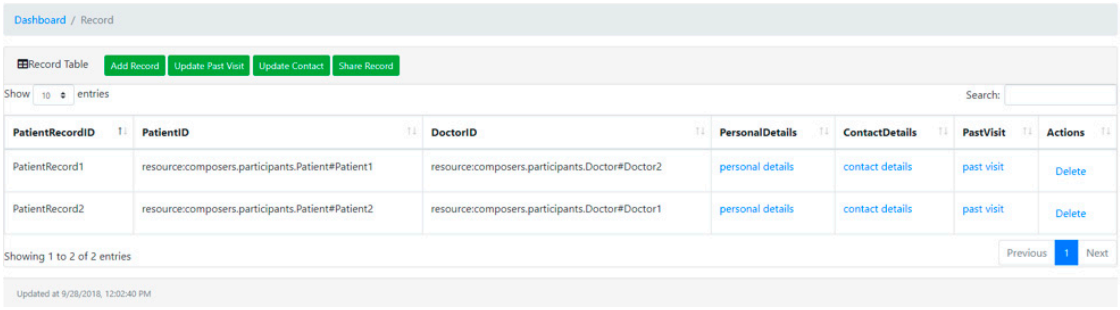
(**a**)



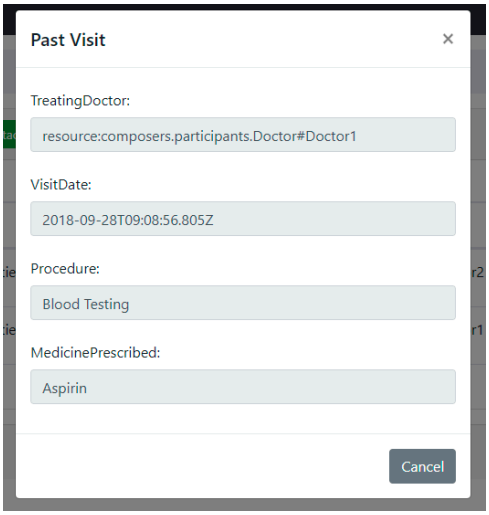
(**b**)

Figure 13. Snapshot of the doctor dashboard. (**a**) Doctor dashboard; (**b**) doctor updating.

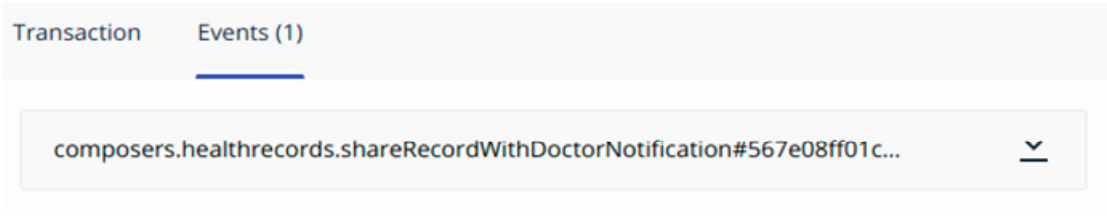
Figure 14a represents the snapshot of the EMR dashboard that provides a portal to access a certain piece of the EMR, for example, the user can access the past treatment record as shown in Figure 14b. It also provides various interfaces to perform operations, for example, sharing the EMR. The event notification occurs whenever the EMR is shared to other doctors as shown in Figure 14c.



(**a**)



(**b**)



(**c**)

Figure 14. Snapshot of the EMR dashboard. (**a**) EMR dashboard; (**b**) EMR updating; (**c**) EMR sharing event notification.

Figure 15 represents the snapshot of transaction history including timestamp, type, and participant. Timestamp is an unalterable blockchain ledger record time indicating when the transaction processed. "Type" presents the transaction type and "participant" represents the user who submits the transaction. The dashboard also provides an entry that shows the detailed information of a specific transaction.

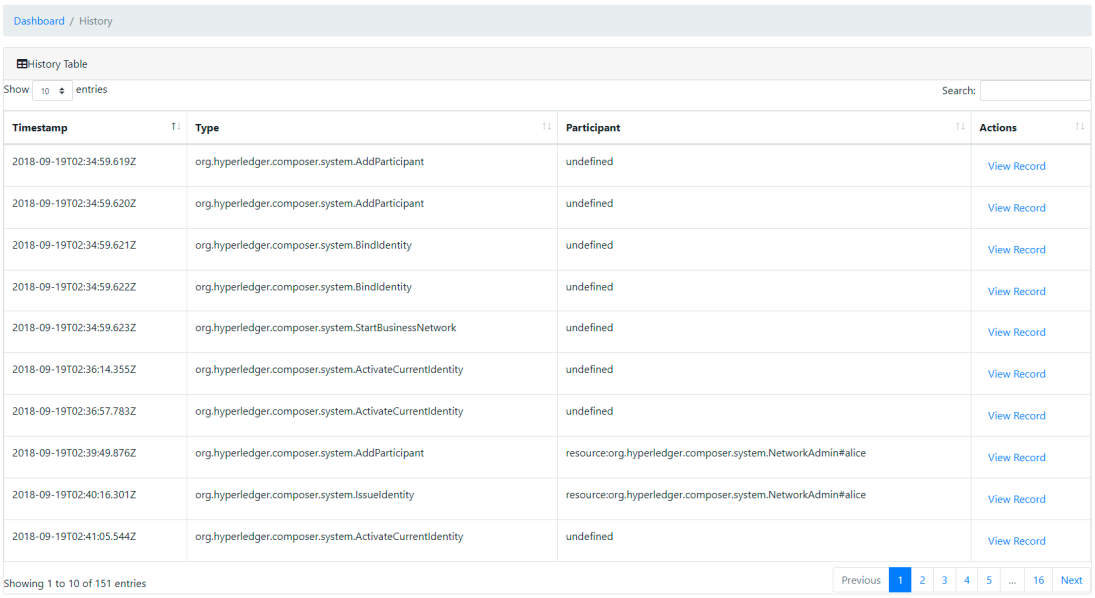


Figure 15. Snapshot of the transaction history dashboard.

5. Performance Evaluation and Comparison

This section presents comprehensive evaluation of results that demonstrate the performance of the proposed medical blockchain platform. For the experiment analysis, the prototype blockchain network was comprised of one orderer node, four CAs, and four departments (two peers per department). In addition, the network was divided into two channels (channel 1 and channel 2), where the smart contract was deployed in each of these channels, respectively. Peers were the fundamental entity of the blockchain network since they maintained the ledger and ran smart contracts to perform operations to the ledger. The CA was the certificate authority component, which issued certificates (ECert and TCert) to each authorized user. A channel was a subnetwork that allowed data isolation and confidentiality, in other words, only the peers in the channel were allowed to access the specific ledger shared across the channel. The orderer node provided transaction ordering that packaged the transaction in sequence by channel and created blocks of transactions per channel.

The first experimental test was carried out by evaluating the transaction round-trip time in the blockchain network. The round-trip time is the time that a transaction request takes to be sent plus the length of time it takes for an acknowledgement to be received by the web client. For this test, we utilized the Postman, which is a tool to dissect RESTful APIs. It provides a sleek user interface with which to customize scripts for simulating a heavy load on network. Two cases were performed, the first case corresponding to the round-trip time spent on performing query transactions and the second one to the time spent on performing invoke transactions. Both of them were carried out by varying the number of users. The first case was analyzed for performance and the results are shown in Figure 16. Four groups of 50, 250, 500, and 1000 users were provided to the system, and each group of users was allowed to initiate query requests to the blockchain network ten times at randomly selected system resource utilization levels. The minimum, average, and maximum time in milliseconds taken to query EMRs were recorded. It was obvious to see that the round-trip time slow grows with the increase of user requests. However, the increase is at such a relatively small level that it can be ignored since it has no direct impact on user experience.

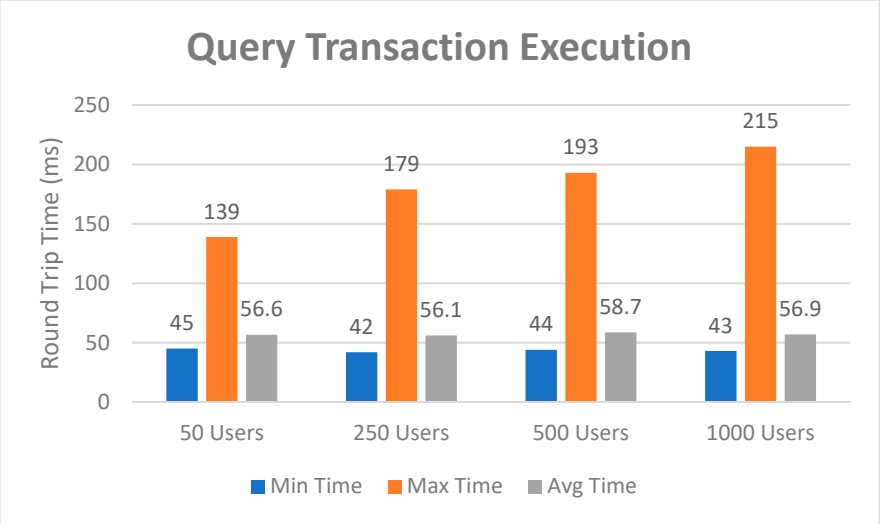


Figure 16. Performance analysis of the query transaction execution.

Similarly, same approaches are applied to the second case, and the evaluation results are presented in Figure 17. It can be seen from the graph that this case spends much more time on performing transactions than the first case. This is due to the invoke transaction requiring endorsement while endorsement is not required for the query transaction. However, the response graph is steady, and the overall transaction execution capability can be assessed if no network congestion happens. In general, Bitcoin takes near 10 minutes to mine a blockchain, and it can be expected that a transaction takes around an hour on average as at least six confirmations are required before a transaction is finalized. For Ethereum, the average transaction times to mine a block are around 15 seconds, however, the time cost varies significantly in terms of network environments. The average transaction execution time for the proposed blockchain network is around 3 seconds, which races far ahead than most popular blockchain platforms.

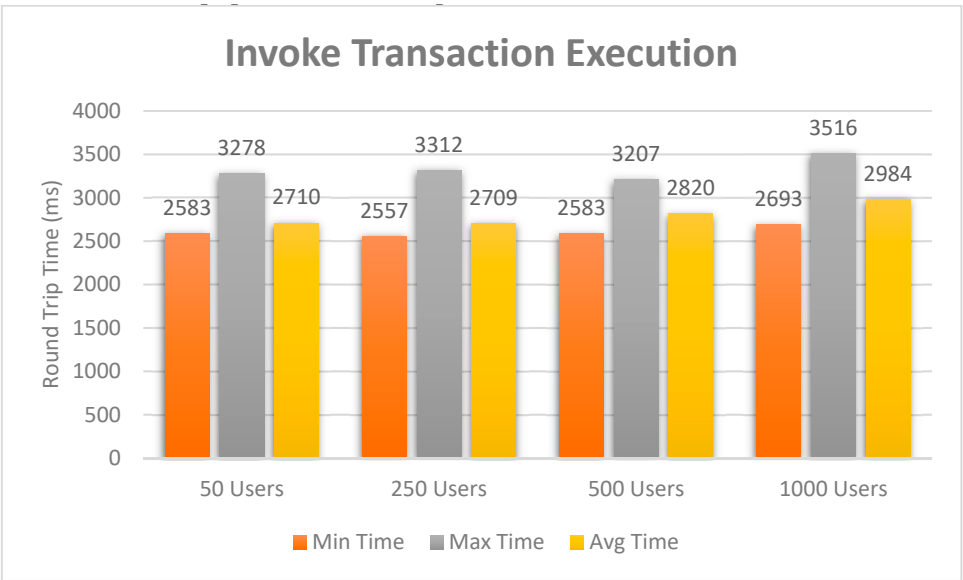


Figure 17. Performance analysis of the invoke transaction execution.

Nevertheless, a more measurable performance comparison analysis is required to be regulated as round-trip time qualitative analysis is not persuasive enough to assess the performance of the blockchain network. Specifically, the round-trip time can greatly vary from one to the other depending on the

network environment. We choose to evaluate the blockchain network by using a more professional benchmark tool, called Hyperledger Caliper [44]. It allows users to measure the performance of a specific blockchain implementation with a set of indicators. For this analysis, five round tests were carried out and the experiment results are shown in Table 6. The first three rounds of experiments were conducted to test the network overload for invoke transactions while the last two were for query transactions. The term transactions per second (tps) refers to the number of transactions performed by the blockchain network per second, also called throughput. For testing the invoke transactions, we evaluated the throughput of the proposed system by varying the send rate from 480 to 1100 tps. It can be seen from the table that the send rate has great impact on the transaction throughput and latency. Similarly, the throughput for query transactions decreases drastically by varying the send rate from 1000 to 1920 tps. It is clear that the blockchain network has a bottleneck in transaction processing power, for example, in the second-round test of which the send rate is 81 transactions per second, the throughput drastically drops to 480 transactions per second. This phenomenon is more severe in the last-round test of which the send rate is 1920 transactions per second, the throughput drastically drops to 1090 transactions per second. This bottleneck is mainly caused by the network size since we only deploy four peers for each channel, and the throughput capability can be improved by extending the network with more peers.

Table 6. Performance analysis summary of the medical blockchain network.

Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	invoke	10,000	0	480 tps	12.23 s	2.34 s	7.22 s	430 tps
2	invoke	10,000	0	810 tps	20.79 s	7.39 s	12.34 s	480 tps
3	invoke	10,000	0	1100 tps	19.88 s	6.88 s	13.97 s	500 tps
4	query	50,000	0	1000 tps	1.41 s	0.01 s	0.20 s	1000 tps
5	query	50,000	0	1920 tps	44.26 s	2.02 s	23.19 s	1090 tps

Table 7 describes the resource utilization test results in various performance indexes. This table presents the maximum, average memory and central processing unit (CPU) utilization rate by the blockchain network. For the local-client, the maximum memory allocation taken in the ten iterations was recorded to be 105.2 MB, averaging at 90.5 MB, and the maximum CPU utility was recorded to be 14.64%, averaging at 8.76%. For each peer, the average maximum memory allocation taken in the ten iterations was recorded to be 112.9 MB, averaging at 103.9 MB, and the maximum CPU utility was recorded to be 12.60%, averaging at 6%. For the orderer node, the average maximum memory allocation taken in the ten iterations was recorded to be 39.6 MB, averaging at 23.4 MB, and the maximum CPU utility was recorded to be 5.16%, averaging at 1.85%. For each CA node, the average maximum memory allocation taken in the ten iterations was recorded to be 5.5 MB, averaging at 5.5 MB, and the CPU utility was recorded to be 0%. The CPU and memory consumption are maintained within a narrow range and the peak value is under 20%. End users can take advantage of this as the system load is in such a low level, otherwise there is too much resource utilization, for example, CPU usage over 30%, may cause poor performance.

Table 7. Performance analysis of resource utilization of the medical blockchain network.

Type	Name	Memory (max)	Memory (avg)	CPU (max)	CPU (avg)	Traffic In	Traffic Out
Process	local-client.js	105.2 MB	90.5 MB	14.64%	8.76%	-	-
Docker	peer1.surgery.com	117.0 MB	108.2 MB	11.36%	5.73%	4.6 MB	5.0 MB
Docker	peer0.dentistry.com	116.2 MB	108.0 MB	17.92%	8.75%	5.8 MB	13.9 MB
Docker	peer0.surgery.com	92.6 MB	88.7 MB	11.95%	6.75%	5.0 MB	5.6 MB
Docker	peer1.dentistry.com	135.4 MB	117.5 MB	10.20%	3.74%	3.7 MB	31.0 KB
Docker	peer1.neurology.com	107.0 MB	98.2 MB	10.46%	4.53%	4.8 MB	4.5 MB
Docker	peer0.neurosurgery.com	114.3 MB	110.0 MB	14.92%	6.24%	5.6 MB	11.5 MB
Docker	peer0.neurology.com	95.6 MB	86.7 MB	12.65%	7.55%	5.2 MB	5.5 MB
Docker	peer1.neurosurgery.com	125.4 MB	114.5 MB	11.32%	4.72%	4.7 MB	89.0 KB
Docker	orderer.com	39.6 MB	23.4 MB	5.16%	1.85%	4.1 MB	15.2 MB
Docker	ca_nodeDept1	5.5 MB	5.5 MB	0.00%	0.00%	546 B	0 B
Docker	ca_nodeDept2	5.5 MB	5.5 MB	0.00%	0.00%	476 B	0 B
Docker	ca_nodeDept3	5.5 MB	5.5 MB	0.00%	0.00%	526 B	0 B
Docker	ca_nodeDept4	5.5 MB	5.5 MB	0.00%	0.00%	456 B	0 B

A comparative analysis of the proposed work with some of the similar projects reviewed in the related work is presented. In order to demonstrate the efficiency and capability of the designed platform, a benchmark study has been carried out, and the evaluation results are displayed in Table 8.

This analysis was performed by considering these features which are considered to be important evaluation factors affecting the system performance. Also, it reflects the overall performance of the blockchain system and shows the significance of our proposed approach. Some of the existing systems like MediBloc, MedRec, Healthcoin, and Robomed Network are built on a permission-less network that requires all nodes to build consensus which significantly increases the energy consumption and reduces efficiency. Moreover, these systems issue their own tokens to incent costly mining or to fuel smart contract execution, which increase the computing power consumption and obstructs the interaction with other distributed systems. In contrast, the proposed system is built on a permissioned network, which reduces the overheads when deployed on the blockchain network. Although some of these systems are based on permissioned networks, they only concentrate on the EMR management. However, the proposed work is investigated thoroughly on actual requirements. In addition to support a secure distributed storage for preserving the EMR, it also provides some other functionalities like reservation, prescription, and billing, which are feasible and practical in a real product environment. There is demand for a flexible medical blockchain platform that offers a permissioned network, no currency exchange, identifiable participants, scalable architecture, high transaction throughput, and low latency of transaction, and this work aims to look for the potential to solve all these issues mentioned above.

A real-life case study for hospital, which implemented as part of the experimental test for demonstrating the feasibility of the proposed approach, is proposed in this work. This system has the potential to be extended in many other application fields such as digital identification, music media rights, and supply chain, which can easily benefit from the consequence of this work. For example, the proposed system can be expanded in the food supply chain to improve transparency and efficiency since the blockchain technologies can provide a trusted source of information and traceability across the food network. By making a shared ledger accessible to each party in the supply chain, all food processing steps can be recorded and stored on the blockchain, including digital compliance documentation, test results and audit certificates.

Table 8. Comparative analysis of the proposed platform with the existing systems.

Name	Cryptocurrency	Consensus Determination	Consensus	Efficiency	Smart Contract	Network Type	Functionality
MediBloc [28]	Yes	All nodes	DPoS	Low	Yes	Permissionless	EMR management
MedRec [29]	Yes	All nodes	PoW	Low	Yes	Permissionless	EMR management
MediLedger [30]	No	One organization	PoA	High	Yes	Permissioned	Pharmaceutical supply security
Healthcoin [31]	Yes	All nodes	PoW	Low	Yes	Permissionless	EMR management
ConnectingCare [32]	Yes	One organization	PoA	High	Yes	Permissioned	EMR management
Robomed Network [33]	Yes	All nodes	PoW	Low	Yes	Permissionless	EMR management
[35]	No	One organization	PoS	High	Yes	Permissioned	Medical data preservation
FHIRChain [36]	Yes	One organization	PoS	High	Yes	Permissioned	EMR management
[37]	No	Selected set of nodes	PBFT	High	Yes	Permissioned	EMR management
[38]	No	Selected set of nodes	PBFT	High	Yes	Permissioned	EMR management
[39]	No	Selected set of nodes	PBFT	High	Yes	Permissioned	EMR management
[40]	No	Selected set of nodes	PBFT	High	Yes	Permissioned	EMR management
Proposed Work	No	Selected set of nodes	PBFT	High	Yes	Permissioned	EMR management, reservation, prescription, billing, etc.

6. Limitation and Discussion

This section discusses the limitations existed in the proposed work. First, although it is nearly impossible to hack and tamper records stored in the blockchain, this is not that case for the programming codes in the smart contract. For example, a hacker exploited a software vulnerability of Decentralized Autonomous Organization (DAO) and stole $50 million worth of virtual currency. The DAO is built on a smart contract that does exactly what their makers program tells them to do and sometimes those programs have unintended consequences. In other words, an easy programming mistake could lead to a disastrous chain of events. This is worthy of our vigilance and requires the utmost attention. Another limitation is related to the consensus algorithm used in the blockchain network. The Practical Byzantine Fault Tolerance (PBFT) algorithm used in the proposed blockchain platform can be disabled if more than a third of the peers are offline at the same time. This incident could happen in small networks with a limited number of peers. It is essential to increase the number of peers to prevent malicious peers from occupying the whole system.

7. Conclusions and Future Direction

It is visible to see that there are many conducive benefits for integrating blockchain technology into healthcare research, from data sharing and tracking to the needed transparency and privacy concerns for patients. This paper outlines a novel procedure for the design and implementation of a decentralized platform to handle EMRs using blockchain technologies. It aims to provide a safe, transparent and meaningful medical assistance for patients and healthcare providers within the hospital by means of services. A medical blockchain case study has been implemented as the proof of concept using the Hyperledger Fabric, which is designed for enterprise use from the outset. Various performance indexes are used to perform experimental tests, which indicate a steady level, allowing effective transaction throughput and low resource utilization. Furthermore, a comparative analysis of the designed system with existing approaches highlights the significance of this work, and the result demonstrates that the designed system outperforms other systems in variety of respects. Although the coevolution of blockchain and healthcare research studies is still in its infancy, it is the goal of this work to suggest a feasible way in building blockchain-based healthcare applications, to benefit the patient, and to revolutionize healthcare industry developments. Moreover, the proposed work can be expanded to many other application scenarios such as supply chain and digital identification based on the designed application. The limitation of this work mainly depends on the blockchain network size and the computer specifications. In order to remedy this issue, future research directions include expanding the network size into a large scale and deploying the proposed solution into the cloud architecture.

Author Contributions: Data curation, L.H.; Formal analysis, L.H.; Funding acquisition, D.-H.K.; Investigation, L.H.; Methodology, D.-H.K.; Software, L.H.; Supervision, D.-H.K.; Validation, E.C.; Visualization, L.H.; Writing—original draft, L.H.; Writing—review & editing, E.C. and D.-H.K.

Funding: This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government, and this research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2016-0-00313) supervised by the IITP (Institute for Information & communications Technology Promotion).

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

References

1. Braunstein, M.; Todd, B. Disruptive Technology in the Healthcare Space. In Proceedings of the GaTech Seminar on Technology Innovation in the Healthcare Space, Atlanta, GA, USA, 10 February 2016.
2. Henry, J.; Pylypchuk, Y.; Searcy, T.; Patel, V. Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals. ONC Data Brief 2008-2015. Available online: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php (accessed on 26 March 2018).

3. Mandl, K.D.; Szolovits, P.; Kohane, I.S. Public standards and patients' control: How to keep electronic medical records accessible but private. *BMJ* **2001**, *322*, 283–287. [CrossRef] [PubMed]
4. Rifi, N.; Rachkidi, E.; Agoulmine, N.; Taher, N.C. Towards using blockchain technology for eHealth data access management. In Proceedings of the 2017 Fourth International Conference on Advances in Biomedical Engineering, Beirut, Lebanon, 19–21 October 2017.
5. Al-Megren, S.; Alsalamah, S.; Altoaimy, L.; Alsalamah, H. Blockchain Use Cases in Digital Sectors: A Review of the Literature. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July–3 August 2018.
6. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Available online: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 15 January 2019).
7. 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.
8. Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef] [PubMed]
9. Kamel Boulos, M.N.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*. [CrossRef] [PubMed]
10. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
11. Zhang, P.; Walker, M.A.; White, J.; Schmidt, D.C.; Lenz, G. Metrics for assessing blockchain-based healthcare decentralized apps. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017.
12. Zhang, P.; White, J.; Scmidt, D.C.; Lenz, G. Applying Software Patterns to Address Interoperability in Blockchain-Based Healthcare Apps. Available online: https://arxiv.org/pdf/1706.03700.pdf (accessed on 18 January 2019).
13. Kim, H.; Laskowski, M. A perspective on blockchain smart contracts: Reducing uncertainty and complexity in value exchange. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017.
14. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
15. Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S.; Wang, G.; Atiquzzaman, M.; Yan, Z.; Choo, K.K.R. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–15 December 2017.
16. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A Blockchain-Based Approach to Health Information Exchange Networks. Available online: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf (accessed on 20 January 2019).
17. Witchey, N.J. Healthcare Transaction Validation Via Blockchain Proof-of-Work, Systems and Methods. U.S. Patent US20150332283A1, 19 November 2015.
18. Yang, H.; Yang, B. A Blockchain-based Approach to the Secure Sharing of Healthcare Data. In Proceedings of the Norwegian Information Security Conference 2017, Oslo, Norway, 11–15 September 2017.
19. Conceição, A.F.; da Silva, F.S.C.; Rocha, V.; Locoro, A.; Barguil, J.M. Eletronic Health Records using Blockchain Technology. Available online: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/07-181717-1.pdf (accessed on 21 January 2019).
20. Cyran, M.A. Blockchain as a Foundation for Sharing Healthcare Data. *Blockchain Healthc. Today* **2018**, *1*. [CrossRef]
21. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; Wiley: Hoboken, NJ, USA, 2016.
22. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016.

23. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 23 January 2019).
24. Radanović, I.; Likić, R. Opportunities for Use of Blockchain Technology in Medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef] [PubMed]
25. Androulaki, E.; Cachin, C.; Ferris, C.; Murhalidharan, S.; Sethi, M.; Murthy, C.; Nguyen, B.; Vukolic, M.; Singh, G.; Smith, K.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018.
26. Why Blockchain Works for Data Integrity. Available online: https://www.uledger.co/blockchain-works-data-integrity/ (accessed on 24 January 2019).
27. Linn, L.A.; Koo, M.B. Blockchain for Health Data and Its Potential Use in Health It and Health Care Related Research. Available online: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf (accessed on 1 February 2019).
28. MEDIBLOC. Available online: https://medibloc.org/en/ (accessed on 2 February 2019).
29. MedRec. Available online: https://medrec.media.mit.edu/ (accessed on 3 February 2019).
30. MediLedger. Available online: https://www.mediledger.com/ (accessed on 3 February 2019).
31. HealthCoin. Available online: https://www.f6s.com/healthcoin (accessed on 4 February 2019).
32. ConnectingCare. Available online: https://www.careconnect.com/ (accessed on 5 February 2019).
33. Robomed Network. Available online: https://robomed.io/ (accessed on 6 February 2019).
34. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
35. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
36. Peng, Z.; Jules, W.; Schmidt, D.C.; Gunther, L.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278.
37. 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 Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.
38. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-resistant mobile health using blockchain technology. *JMIR mHealth uHealth* **2017**, *5*, e111. [CrossRef] [PubMed]
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*, 650–659. [PubMed]
40. Massi, M.; Miladi, A. Using PROV and Blockchain to Achieve Health Data Provenance. Available online: https://eprints.soton.ac.uk/421292/1/PROV_BC_Healthcare.pdf (accessed on 8 February 2019).
41. Quorum. Available online: https://www.jpmorgan.com/quorum (accessed on 9 February 2019).
42. Tendermint. Available online: https://tendermint.com/ (accessed on 9 February 2019).
43. Hyperledger Composer. Available online: https://www.hyperledger.org/projects/composer (accessed on 10 February 2019).
44. Hyperledger Caliper. Available online: https://www.hyperledger.org/projects/caliper (accessed on 11 February 2019).