Songklanakarin J. Sci. Technol.
43 (2), 335-343, Mar. - Apr. 2021

http://www.sjst.psu.ac.th

Original Article

The electronic medical record exchange using a Blockchain technology

Juthamas Nuansanong and Supaporn Kiattisin*

Department of IT Management, Faculty of Engineering,
Mahidol University, Phutthamonthon, Nakhon Pathom, 73170 Thailand

Received: 20 July 2019; Revised: 6 December 2019; Accepted: 16 January 2020

Abstract

The medical record exchange (EMR) between hospitals is a challenge in medical health. The health information data are sensitive and require the utmost privacy. This research proposes an improved new process for the hospital context, which is based on Blockchain technology. A key characteristic is the general distributed method with the consensus mechanism, which gives the benefits of immutability, security, trust, and near-real-time transactions. This study designed the standard data structure under HIPPA Law and GDPR regulations. These fields have been encrypted on the system architecture, which builds on the Hyperledger Fabric using chaincode validation. The scenario testing illustrates a proof of concept, which is on the real environment and simulated medical records, in terms of throughput, fault tolerance, and immutability. Performance analysis confirms that Blockchain technology is valuable and meaningful to the healthcare system. This research also found that the medical Blockchain provides absolute real-time EMR with security.

Keywords: medical record exchange, electronic medical record, Blockchain healthcare, Blockchain, Hyperledger

1. Introduction

In the past, hospitals and public health agencies have applied information technology extensively in their services. The hospitals have changed the internal processes from paper-based to more electronic systems. As an example, medical records are medical documents used to record and collect patient histories, including personal history, treatment history, and drug allergy, and the hospital stores medical records in an electronic format for increased service efficiency, convenience, speed, and accuracy.

However, previous research has noted that healthcare agencies have massive amounts of health information, which often differ in type, format, nature, and are also stored in several databases with different management platforms (Jardim, 2013). Concerning the disruptive technologies in healthcare agencies, there is strong resistance to the adoption of e-health systems, known as the Electronic Medical Records (EMR). Nevertheless, there are problems and barriers in operations related to electronic records, which are the policy and practice issues in data redundancy, data security, data quality, patients' trust, data disclosure, and EMR exchanges between hospitals. For example, the requesting process for information is still complicated and time-consuming, or the data are not standardized for usage. If such problems occur for patients with chronic diseases that need ongoing treatment or for patients with a severe history of drug allergy, they might result in the death of the patient.

Thus, this study focuses on an improved new process for EMR exchange between hospitals, which is based on a suitable solution to address the weaknesses or issues mentioned above.

2. Background and Related Work

2.1 Challenge of health information exchange

Medical records exchange is challenging in healthcare agencies. The manual or paper document is a simple process, although the hospital information system has been implemented in almost hospitals. Medical error is No.3 ranked as cause of death in the U.S., behind cancer and heart disease (Makary & Daniel, 2016). A key factor contributing to this problem is the lack of transparency between medical agencies and the inadequacy of hospital information systems

*Corresponding author
Email address: supaporn.kit@mahidol.edu

to safely and efficiently share data. The challenges are untrusted system, incompatibility of clinical document format, privacy, and security, as the most concerning issues. Blockchain delivers a reliable system to track transactions across hospital information systems (HIS) (Iansiti & Lakhani, 2017). It holds a significant promise for healthcare interoperability. Blockchain can process the transactions from multiple HIS or health systems. The patients can manage and participate in access to their health information and records by the digital signature (Halamka, Lippman & Ekblaw, 2017). Other studies suggest that the interoperability between health information systems (HIS) is just a channel of standard messages, which must be adopted by all products of this type of technology for improved function of these systems.

Among the different standards that should be emphasized for their features, there are HL7 and open EHR (Atalag, Kingsford, Paton & Warren, 2010). Therefore, the bottleneck for health medical records is in the interoperability, caused by a lack of system architectures and data standards that allow the secure transfer of sensitive clinical data between hospitals. Figure 1 shows the traditional process of Health Information Exchange.

2.2 Blockchain in healthcare

2.2.1 Blockchain overview

Blockchain technology began with financial transactions, in which Blockchain network system will allow transactions without going through an intermediary. Blockchain system creates a token that is like an asset in a system that could be traded or exchanged through "Cryptocurrency" such as Bitcoin, Litecoin, Ethereum, and Ripple. Initially the term Blockchain was coined in 2009 by Satoshi Nakamoto (Nakamoto, 2009) in the source code for the digital currency Bitcoin. However, the healthcare sector may venture into Blockchain technology and develop Blockchain based applications that will serve in the business operations for improved transparency and efficiency. There are currently various platforms in the Blockchain development technology. Each platform has different key features and purposes of use, as shown in Table 1.

The appropriate platform that should be chosen for this study is “Hyperledger”, considering that it is open-source, widely used, and most of its developers have strong experience for debugging. The important thing is that there are many case studies in the healthcare sector. Also, Hyperledger has established Hyperledger Healthcare Working Group (HLHC Working Group) to support the development of health data sharing and improve quality using Blockchain technology, which is more secure than traditional networks (Hyperledger, 2017). Moreover, the cost of setting up a Blockchain using Hyperledger is in the "Very Low" range. This approach is made easier by the cloud computing market leaders that already provide Hyperledger Fabric infrastructure.

2.2.2 Key benefits of the Blockchain

On comparing Blockchain with the traditional database management system (DBMS) such as MySQL, SQL, Microsoft, Oracle, and DB2 for healthcare applications (Kuo, T.-T., Kim & Ohno, 2017), the benefits are;

1) Distributed management. While Blockchain is a shared database or well-known as a Distributed Ledger Technology (DLT), DBMSs are logically centralized-managed. Hence, Blockchain is suitable for independent healthcare stakeholders such as hospitals, patients, insurers, and auditors that need to cooperate without having to control it as a central management intermediary.

2) Immutable Audit Trails. DBMSs support Create, Read, Update, and Delete (CRUD) similar to any database systems, while Blockchain has been formulated to include a security data set so that the previous transactions cannot be changed or modified, and all users will see the same data. Blockchain provides a structure for storing the electronic medical record on the block, such that it could be analyzed but remains private, with an embedded economic layer to compensate for data contribution and use (Swan, 2015).

3) Data ownership. The ownership of digital assets on DBMS is controlled and modified by administrators, while on Blockchain, the only one who can change the data is an owner by using the principles of cryptography. Therefore, Blockchain is suitable for handling critical digital data such as EMRs.

4) Availability. Although DBMS and Blockchain are based on distributed technology and do not experience a single point of failure, DBMS is high-priced when trying to achieve a high level of redundant data issues, so Blockchain is proper for the protection and the availability of business continuity.

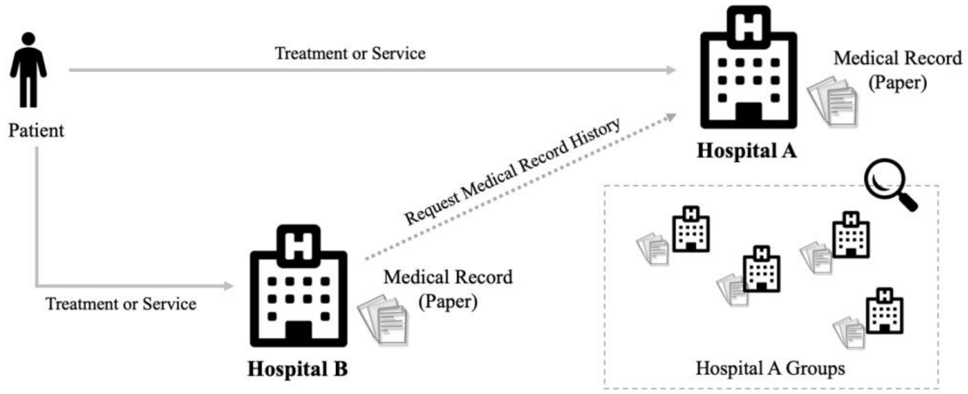


Figure 1. The traditional process of Health Information Exchange

Table 1. Comparison of some open source Blockchain platforms

Platform	Description	Type	Database	Languages	Consensus	Usage Cost [1]
Ethereum	General purpose	Public & Permissionless	Decentralized	Go, C++, Python	PoW	Pay in Ether to execute smart contracts (Moderate)
Hyperledger	General purpose	Private & Permissioned	Distributed	Java, Go, Node.js	PBFT / Pluggable	Open-source (Very low)
EOS	General purpose	Public & Permissioned	Decentralized	Rust, C, C++	DPoS	Paid by contract owner (Moderate)
Tendermint	General purpose	Public & Permissionless	Decentralized	Java, C++, Python, Go	BFT	Open-source (Very low)
R3 Corda	Financial Services	Private & Permissioned	Decentralized	Java, Kotlin	Pluggable	Commercial Licensing cost per transaction (High)
Ripple	Financial Services	Public & Permissioned	Distributed	Java, C++	RPCA	Fixed per transaction (High)
MultiChain	Financial Services	Private & Custom	Distributed	C, C++, Python, Javascript	PBFT / Customizable validation	Commercial Licensing per year (High)
HydraChain	Private Network	Public & Permissioned	Distributed	Python	PBFT	Open-source base on Ethereum (Moderate)
Quorum	Cross-Industry	Private & Pemissioned	Decentralized	Go, Solidity	RAFT, Istanbul BFT	Open-source base on Ethereum (Moderate)
Shipchain	Cross-Industry	Public & Permissioned	Distributed	Go, C++, Python	PoW	Commercial Licensing per year (High)
OpenChain	Digital Asset Management	Private & Pemissioned	Distributed	JavaScript	PoA, PoW	Open-source (Very low)

[1] Generally, the cost of Blockchain development varies depending on the type, infrastructure, and implementation service; the price ranges are defined as Very low, Low, Moderate, and High.

5) Security and Privacy using Cryptographic Algorithms. DBMS uses the username and password to access the data with a risk of being hacked, resulting in data leakage and stolen data. On the other hand, the encryption model used by Bitcoin is named the 256-bit Secure Hash Algorithm (SHA-256), and is a highly secure encryption method used for both data encryption and bitcoin mining. Besides, the SHA-256 can also be used to verify ownership of bitcoin users. Its operations use mathematical and computer principles, which are called hash functions.

2.2.3 Use cases

The Blockchain has already been adopted in healthcare industries. The survey of Hyperledger said that around 43% of healthcare organizations expect faster Blockchain implementation with interoperability (Plasma business intelligence, 2018). Medical data include the patient health information, the electronic health record, the data from medical devices, and health insurance claims. The sharing method requires security and data integrity (MIT, 2017). According to Figure 2, the MedRec project (Azaria, Ekblaw, Vieira & Lippman, 2016) launches for electronic medical record sharing on Ethereum smart contract. The medical records are on a decentralized network. The Blockchain system manages the digital signature, and the medical information does not accumulate in the Blockchain.

During the 21st century, the United States experiences problems from overdose deaths, especially from painkillers and opioids prescribed to patients. For example, a redundant prescription causes the patient to receive a double-dose of the drug accidentally. Therefore, the BlockMedX project (BlockMedX, 2017) was created to address prescription drug abuse, with the principle of using an electronic prescription instead of a paper-based process. This system is highly cryptographically secured and more efficient by using Ethereum Blockchain to give trust between patients, doctors, and pharmacists under the HIPAA Laws standard.

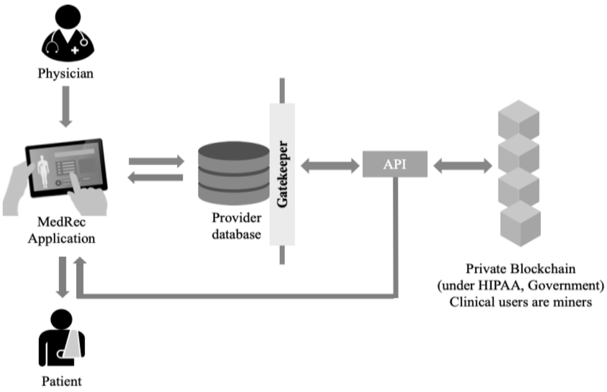

Physician
MedRec Application
Provider database
Gatekeeper
API
Private Blockchain (under HIPAA, Government) Clinical users are miners
Patient

Figure 2. MedRec: Electronic medical records on the Blockchain

Table 2 shows a summary of Blockchain case studies that have many features and applications, which can be useful in healthcare, as well as limitations. The meaningful benefits investigated in many of these studies apply to decentralized structures, helping interoperability, security, authentication, and integrity. The core issues combined with the framework are scalability, digging motivation, blockchain-specific attacks, and key management.

2.2.4 Healthcare regulations

Complying with the GDPR requires more specific and sensitive data, and individuals can ask for in-depth

Table 2. Summarized Blockchain case studies – challenges and limitations

Application	Challenge	Limitation	Field of work
Gem Health (Mettler, 2016)	Sharing of Health information and legal issues addressed	Scalability and key replacement are not addressed	Medical Startup
MedRec (Azaria, 2016)	Improve Medical Record Access	Legal issues are not addressed	Laboratory
BlockMedX (BlockMedX, 2017)	Anti-prescription drug abuse with e-prescribing	EMR API access and integration	Prescription drug industry
OmniPHR (Roehrs, 2017)	Sharing of Patient Records	The user needs to approve all access requests and duplication of data	Laboratory
Change Healthcare (Change Healthcare, 2018)	Improve claims lifecycle throughput and transparency	Data duplication issue	Healthcare industry
FarmaTrust (FarmaTrust, 2018)	Manage inventory on a supply chain	Scalability of node implementation	Pharmaceutical companies
MedicalChain (MedicalChain, 2018)	Exchange and usage of medical data	Legal issues are not addressed	Laboratory
Healthchain (Xu, Xue, Li, Tian, Hong, & Yu, 2019)	Validate privacy data	Personally identifiable information (PII) stored off-chain, and GDPR compliance is on the pilot study	Medical Startup

information on how their data have been processed and received in an electronic form before transferring to others. While HIPAA was defined to prevent unauthorized data access within a healthcare provider, GDPR indicates the differences between privacy and security. At the same time, HIPAA in the U.S. and GDPR in the EU provide a meaningful motivation for the Blockchain solutions in healthcare. The technology offers a practical and trustworthy way to ensure data preservation obligations. Though there often remain questions on issues of privacy and erasure, the research strongly believes in having answered these issues and is rushing to address any new challenges. The concerns around Blockchain use in healthcare involve HIPAA compliance and interoperability. Healthcare agencies need to integrate HIPAA policies into the new technology, which will mean converting 1996 regulations into 21st-century technology.

3. Method

The main goals of this study are developing a prototype of the EMR standardized data structure and building a blockchain-based system for exchanging the EMR between hospitals with healthcare regulations. To solve those problems, we need to identify a proven theory that is useful in addressing issues related to structure and management, followed by a systematic way to create research questions. Such as gathering the requirements from hospital users, including physicians, IT technicians, and clinical data specialists. Second, the design of a new processes comprised of the data structure, network, and system architecture by applying the characteristics of several theories to Blockchain over a general distributed method. Third, to implement and develop the platform, chaincode, genesis block, and user interface. Finally, this study has tested the system with clinical transaction data in a real hospital environment.

3.1 The requirement

This study delivers the Blockchain into the mix; the hypothesis is that the new design method can simplify processing, make it more efficient, and enable services to be provided more quickly with trust and reliability. The highest concerns are data protection and data privacy because the EMR carry highly sensitive data. The authentication process should include both patients and providers to allow data sharing. Requirements to design a Blockchain for the healthcare sector include building an innovation system that can scale to healthcare business that would require millions of transactions of the medical records. This study seeks to: 1) Improve quality, safety, efficiency, and reduce health disparities; and 2) Improve care coordination.

3.2 The system design

This system design does not directly connect with the Hospital Information System (HIS) but will connect to a virtual database to simulate the network through the database view that the hospitals have built on private cloud (Intranet Network) for EMR exchanges specifically, including connecting to the hypothetical medical records database. System implementation regards the privacy of patient information.

All medical records used in the testing phase, such as patient data, hospital information, are simulated data for the experiments only.

3.2.1 Health data standard

According to the requirements, the standard data structure design is as in Figure 3. The EMR transactions are stored in the block. The Blockchain layer contains unidentified data and shares to other hospitals (or nodes). The decentralized database is in the network (Zyskind, Nathan, & Pentland, 2015). The authorized nodes request and view the patient record. The citizen identification number (CID) is a rational choice for the primary key. However, this identifier data has to be encrypted under the HIPAA law standard (Azaria, Ekblaw, Vieira, & Lippman, 2016).

As shown in Figure 3, this study has designed the standard data structure based on clinical practice, such as treatment, diagnosis, drug allergy history, medical history, and patient transfer. This can group the data into two types, as

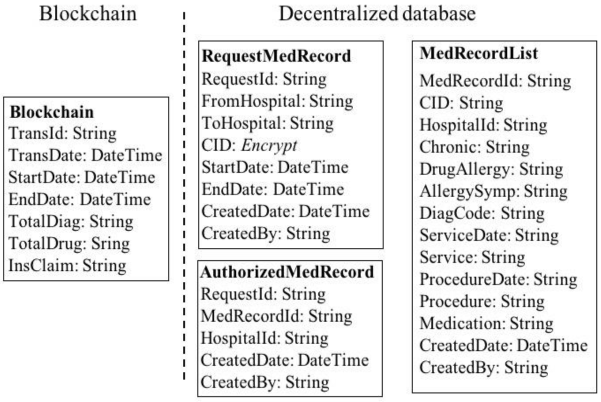


Figure 3. The data structure

follows. 1) Blockchain holds a list of Blockchain transactions; and 2) Decentralized database stores reference of a medical record, as RequestMedRecord, AuthoriedMedRecord, and MedRecordList.

3.2.2 Choosing Blockchain platform

This study proposes two criteria for choosing the Blockchain platform, which comes to the definition of an environment. First, the level of anonymity of validators. The member is not a criterion but rather a feature. The network can have anonymous users even though validators are known and regulated. Second, the level of trust in validators is a factor that unites a particular user and a validator and cannot be held global.

Figure 4 illustrates a matrix of the Level of anonymity of validators and the Level of trust in validators. The bottom right quadrant is for permissioned and private, in which a validator needs to be licensed or be a member. This is the only type where Blockchain is not public. For example, an internal banking system with a single entity validates Blockchain. The time consuming consensus algorithm depends on high trust to a validator (PBFT, multi-signature). Immutability depends on the agreement between validators. This is suitable for banking, fast payment infrastructure, and corporate usage.

With reference to these reasons, the Hyperledger Fabric is permissioned and suitable for a private sector like the healthcare organizations. Its differences compared to Ethereum, Bitcoin, or other platforms are that people who join the system must verify their identity by registering with the Membership Service Provider, the networks need to restrict access, and it is highly secure with PBFT algorithm.

3.2.3 Proposed system architecture

The overview of system architecture is shown in Figure 5. When the record has been requested, the system will verify the digital signature. The patients are assigned participation in the process. The system requires a personal digital signature to access the data. The hospital public keys are used in the authentication step as well. The clinical transactions are exchanged via the RESTful application programming interface over the HTTP. The Hyperledger chaincode is the program to validate the data and approve the requested transaction (Cachin, 2016).

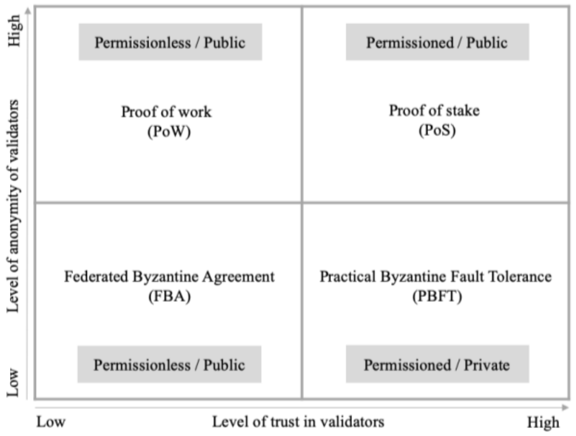


Figure 4. The criteria-model matrix

3.3 The application development

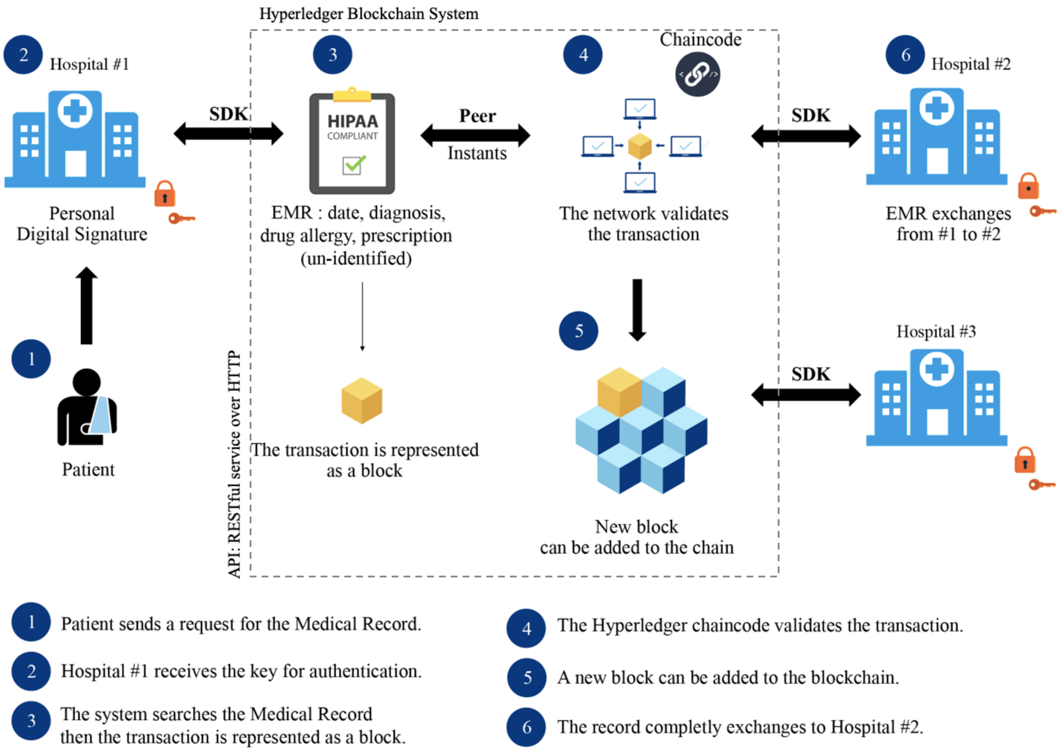
Installing the development environment is the initial step. The development tools are Docker, Node.js, and Golang. This study created a secured network by using the Hyperledger Fabric. The public and private keys are generated. The Hyperledger network is divided into three components as follows: the application (web server), the peer (hospital or node), and the orderer. The orderer manages the consensus, then the chaincode or smart contract is developed for data accuracy and validation. The genesis block is the first block in the chain that has been created. Finally, the web-based application and API are configured to link between the command line interface and user (Bennett, 2016).

3.4 The testing metrics

Performance evaluation is the method of regulating the performance of a system under test. This testing can cover system-wide measures such as response time or latency. This study applies simulated data and situations to verify the system functionality and the business requirements achievement. The sampling data (un-identified data) from the hospital and the fake CID are generated for testing in the simulated environment. Before discussing the testing platform, it is very important to define the metrics of system performance. This study considers two primary metrics for measuring the performance of a Blockchain: throughput and fault tolerance.

i. Transaction throughput is the rate of the transactions committed by the Blockchain System Under Test (SUT) in a defined time period (Hyperledger, 2018). It is a parameter for measuring the number of successful transactions per second (Pongnumkul, Siripanpornchana, & Thajchaya pong, 2017) by using equation (1).

$$\text{No. of transactions per block} = \frac{\text{Block size in bytes}}{\text{Average transaction size in bytes}} \qquad (1)$$



1 Patient sends a request for the Medical Record.

2 Hospital #1 receives the key for authentication.

3 The system searches the Medical Record then the transaction is represented as a block.

4 The Hyperledger chaincode validates the transaction.

5 A new block can be added to the blockchain.

6 The record completly exchanges to Hospital #2.

Figure 5. The system architecture

ii. Fault load is imperative to the Blockchain security. In Hyperledger it is called Practical Byzantine Fault Tolerance (PBFT), which is an excellent consensus algorithm for enterprise consortiums where members are partially trusted.

The testing needs a minimum of 3f + 1 replicas (Sukhwani, Martínez, Chang, Trivedi, & Rindos, 2017) where f is the maximum number of faulty replicas. The minimum ensures the system has enough non-faulty replicas to discover the faulty ones. Thus, a replica set |R| with the maximum number of replicas that can be faulty is of size:

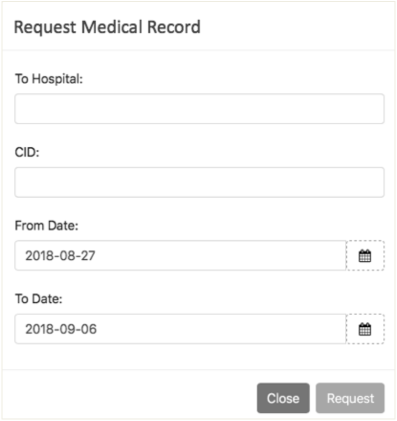
$$|R| = 3f + 1 \qquad (2)$$

4. Results and Discussion

4.1 Experimental results

The application has a satisfying function according to the requested transactions complete across facilities, and the data accuracy ensures interoperability. Figure 6 shows the application interface for medical record requests. The hospital users have to fill the destination hospital, citizen identification number, and time-frame.

The transaction exchange uses the Application Programming Interface (API) technology, which is a program developed for the interface between applications or modules in the form of web service. The popular concept is "RESTful Service" that is simple about work processes using HTTP capabilities, which are the basis of web technology with GET, POST, PUT, and DELETE.



Request Medical Record

To Hospital:

CID:

From Date: 2018-08-27

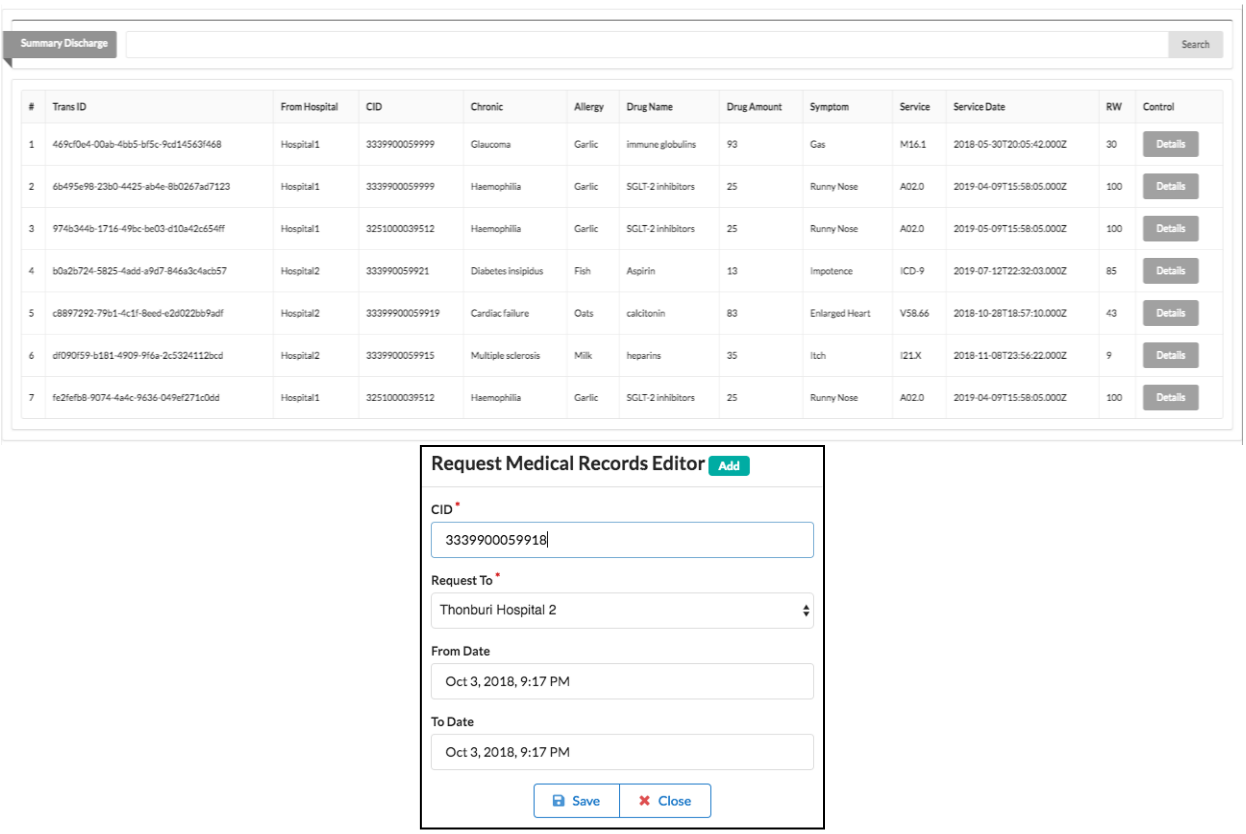
To Date: 2018-09-06

Figure 6. The medical record request window

The result is the transaction status, as shown in Figure 7. The system design presents data privacy and complies with the HIPAA law. The hospital users require authentication via the hospital intranet in order to see the information. Medical record details limit on outpatient service, including date, diagnosis, drug allergy, and prescription detail. The discharge summary information from inpatient service has been developed.

4.2 Performance analysis

This section describes two different cases that create different issues for measuring system performance.



#	Trans ID	From Hospital	CID	Chronic	Allergy	Drug Name	Drug Amount	Symptom	Service	Service Date	RW	Control
1	469cf0e4-00ab-4bb5-bf5c-9cd14563f468	Hospital1	3339900059999	Glaucoma	Garlic	immune globulins	93	Gas	M16.1	2018-05-30T20:05:42.000Z	30	Details
2	6b495e98-23b0-4425-ab4e-8b0267ad7123	Hospital1	3339900059999	Haemophilia	Garlic	SGLT-2 inhibitors	25	Runny Nose	A02.0	2019-04-09T15:58:05.000Z	100	Details
3	974b344b-1716-49bc-be03-d10a42c654ff	Hospital1	3251000039512	Haemophilia	Garlic	SGLT-2 inhibitors	25	Runny Nose	A02.0	2019-05-09T15:58:05.000Z	100	Details
4	b0a2b724-5825-4add-a9d7-846a3c4acb57	Hospital2	333990059921	Diabetes insipidus	Fish	Aspirin	13	Impotence	ICD-9	2019-07-12T22:32:03.000Z	85	Details
5	c8897292-79b1-4c1f-8eed-e2d022bb9adf	Hospital2	33399900059919	Cardiac failure	Oats	calcitonin	83	Enlarged Heart	V58.66	2018-10-28T18:57:10.000Z	43	Details
6	df090f59-b181-4909-9f6a-2c5324112bcd	Hospital2	3339900059915	Multiple sclerosis	Milk	heparins	35	Itch	I21.X	2018-11-08T23:56:22.000Z	9	Details
7	fe2fefb8-9074-4a4c-9636-049ef271c0dd	Hospital1	3251000039512	Haemophilia	Garlic	SGLT-2 inhibitors	25	Runny Nose	A02.0	2019-04-09T15:58:05.000Z	100	Details

Request Medical Records Editor

CID *: 3339900059918

Request To *: Thonburi Hospital 2

From Date: Oct 3, 2018, 9:17 PM

To Date: Oct 3, 2018, 9:17 PM

Figure 7. The summary of medical record request and status

4.2.1 Case 1: System under test with transaction throughput

The performance of the proposed application was tested by comparing across different scenarios for increased Transactions per Second (TPS). In order to increase the TPS, the EMR could adjust two variables. The first variable is block size (B), which is hardcoded at 1 MB. Conceptually, B should be increased to increase TPS. The second variable is block generation time (TB) dependent on complexity of the hashing puzzle. Conceptually, TB should be reduced to increase TPS as shown in Table 3.

In scenario 1, the EMR block generation time is every 4 seconds for a new block to be mined. In 4 seconds, EMR could average around 8.19 transactions. In other words, the EMR could currently guarantee only 2.05 transactions per second. In scenarios 2 and 3, in order to grow TPS from 2.05 to 4.09, EMR would need to scale its TPS twofold. In other words, B would need to be increased from 1MB to 2MB, or TB would need to be reduced from 4 seconds to 2 seconds. The scenario testing found that the average time of record display through the validation process via chaincode and web application takes an average of 2-4 seconds per task.

4.2.2 Test environment with fault load

To assure the security of system and improve its fault tolerance, the message count is significant. In the experiment, the system sets 4 replicas with one of them being the primary, if the replica sets are to tolerate up to 1 faulty replica. The system gets 4 replicas by applying the 1 faulty replica to the equation: 3 (1 faulty replica) + 1 = 4 replicas. The total minimum message count for this replica set is:

$$1 + 3f + 3f(3f - f) + 3f - f + 1)(3f + 1) + 3f - 1 \qquad (3)$$

According to equation (3), the minimum message count is 24 total messages for 1 request when using 4 replicas. PBFT could function on the condition that the maximum number of faulty replicas must not be greater than or equal to one-third of all the replicas in the system.

Table 3. The different scenarios for increasing TPS

Scenario	S1	S2	S3
Adjustment	1MB	Increase (B) to 2MB	Increase (TB) to 2s
a. EMR block size (B) in bytes	1,048,576	2,097,152	1,048,576
b. Block generation time (TB) in seconds	4	4	2
c. Average transaction (Tx) size in bytes	128,000	128,000	128,000
d. Average transactions per block = a/c	8.19	16.38	8.19
e. EMR transactions per second (TPS) = d/b	2.05	4.09	4.09

4.3 Discussion

Blockchain is a form of distributed ledger managed by a shared ledger. The consensus method provides the advantages of integrated data sets that communicate to reduce human errors, near-real-time performance, and adaptability to change the records. Considering that no owner on the origin of the data is contained in the shared ledger, Blockchain leads to raised security, reliability, and transaction integrity between the participating members. However, the benefits of Blockchain are captivating and indeed express a significant step in the right direction for healthcare operations exchanges. If Blockchain in healthcare becomes commercial, it will offer more benefits. The expanding demand for healthcare services delivery accompanied by the medical record management that gives rise to a need to cut out the middlemen.

The results show that the system deployed with Blockchain technology could be used to exchange health information records or medical records effectively, both in safety and with reduced time compared to the traditional approach. However, there are key takeaways that are important to further development of this system, as follows:

1) The consensus and validation processes defined within the chaincode could be changed depending on the business context and situation of each hospital.

2) Sensitive personal data protection, i.e., genetic data or biometric data, is an important thing to consider and must be implemented under various laws or regulations such as HIPAA and GDPR.

3) The system using PBFT consensus should have at least three nodes, with reference to the fault load calculation. Moreover, there are alternative ways to increase the efficiency of the consensus method, such as mining or defining the audit agencies who act as validators.

5. Conclusions

The proposed solution with Blockchain is appropriate for medical records exchange. The distributed database provides data verification to stakeholders in the network. The clinical transaction data are shared directly between hospitals. The transparency has improved because the system allows the transactions to be visible to another node in the network and traceable as well. The data in Blockchain are permanent, and edited data will be saved as a new block in the system. The digital signature (Public and private key) increases patient participation as a data owner. The system provides data governance, security as well as interoperability. The shared data should be clinical transaction data, including service date, diagnosis, allergies, and prescriptions, which suffice for continued care. The Blockchain technology has a value and meaningful use in the healthcare system, especially in electronic medical records.

The results of this study indicate that the success factors for further development, which lead to improved level of public health services, consist of:

1) Health data standard. Generally, EMR never considered managing lifetime medical data among different agencies. During a lifetime, patients distribute their medical records over the complexity of agencies and from one HIS silo to another, often losing sensitive data. Health data standard is an important issue to consider on Blockchain Healthcare.

2) Cooperation with stakeholders such as government auditors, healthcare providers, private sector, system administrators, and system operators. The objective is to prepare and understand the user experience, to make interactions with their related healthcare agencies.

3) Healthcare Infrastructure. Hospital interface, storage, and network on a distributed architecture should provide mutual information exchanges in real-time and with accuracy.

Acknowledgements

The authors acknowledge the Thailand Research Fund (TRF) for a research grant in 2018-2019.

References

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *The 2nd International Conference on Open and Big Data* (OBD), 25-30. doi:10.1109/OBD.2016.11

Barger, A., & Cachin, C. (2018). Hyperledger fabric: A distributed operating system for permissioned Blockchains. *EuroSys '18 Proceedings of the Thirteenth EuroSys Conference Article 30*. doi:10. 1145/3190508.3190538.

Bennett, M. (2016). Hyperledger announces the hyperledger healthcare working group. Retrieved from https:// www.hyperledger.org/

BlockMedX LLC, (2017). Combating prescription drug abuse with a secure decentralized application built on Ethereum, White Paper.

Halamka, J. D., Lippman, A., & Ekblaw, A. (2017). The potential for Blockchain to transform electronic health records, Harvard business review. Retrieved from https://hbr.org/Hearn, M. (2016).

Corda: A distributed ledger —The white paper. Retrieved from https://www.corda.net/

Hyperledger. (2017). Hyperledger architecture, Volume 1— The white paper. Retrieved from https://www. hyperledger.org/wp-content/uploads/2017/08/ Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Hyperledger. (2018). Hyperledger Blockchain performance metrics—The white paper. Retrieved from https:// wiki.hyperledger.org/groups/pswg/performance-and -scale-wg

Iansiti, M. & Lakhani, K. R. (2017). The truth about Blockchain, Harvard business review. Retrieved from https://hbr.org/

Jardim, S. (2013). The electronic health record and its contribution to healthcare information systems interoperability. *Procedia Technology, 9,* 940-948, doi:10.1016/j.protcy.2013.12.105.

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220. doi:10.1093/ jamia/ocx068

LaFever, G. (2016, May 2). Blockchain and big data privacy in healthcare, International Association of Privacy Professionals. Retrieved from https:// iapp.org/news/

a/blockchain-and-big-data-privacy-in -healthcare/

Makary, M. A., & Daniel, M. (2016). Medical error — the third leading cause of death in the US. *BMJ, i2139*. doi:10.1136/bmj.i2139

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. doi:10.1109/HealthCom. 2016.7749510

MIT Media Lab. (2017). MedRec—The white paper. Retrieved from https://medrec. media.mit.edu

Nagpal, R. (2017, April 12). 17 Blockchain platforms—a brief introduction. Retrieved from https://medium. com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

Pilkington, M. (2016). *Blockchain technology: Principles and application, Research handbook on digital transformations*. Retrieved from https://scholar. google.fr/

Pongnumkul, S., Siripanpornchana, C. & Thajchayapong S. (2017). Performance analysis of private Blockchain platforms in varying workloads. *The 26th Inter national Conference on Computer Communication and Networks (ICCCN)*, 1-6. doi:10.1109/ICCCN. 2017.8038517

Purkayastha, S. (2017, September 6). Compare eight Blockchain platform to kick start your next project. Retrieved from http://radiostud.io/eight-blockchain-platforms-comparison/

Roehrs, A., Costa, C., & Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics, 71*, 70-81. doi:10.1016/ j.jbi.2017.05.012

ShipChian. (2017). ShipChian —The white paper. Retrieved from https://shipchain.io/

Sukhwani, H., Martínez, J., Chang, X., Trivedi, K., & Rindos, A. (2017). Performance modeling of PBFT consensus process for permissioned Blockchain network (Hyperledger Fabric). *IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, 253-255. doi:10.1109/SRDS.2017.36

Swan, M. (2015). Blockchain: Blueprint for a new economy. Retrieved from https://books.google.co.th/books

Zyskind, G., Nathan, O. & Pentland A. (2015). Decentralizing privacy: Using Blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 180-184. doi:10.1109/SPW.2015.27