


Article

Blockchain Paradigm for Healthcare: Performance Evaluation

Leila Ismail *  and Huned Materwala

Department of Computer Science and Software Engineering, College of Information Technology, United Arab Emirates University, Al Ain, Abu Dhabi 15551, UAE; huned.m@uaeu.ac.ae

* Correspondence: leila@uaeu.ac.ae

Received: 2 June 2020; Accepted: 17 July 2020; Published: 22 July 2020

Abstract: Electronic health records (EHRs) have become a popular method to store and manage patients' data in hospitals. Sharing these records makes the current healthcare data management system more accurate and cost-efficient. Currently, EHRs are stored using the client/server architecture by which each hospital retains the stewardship of the patients' data. The records of a patient are scattered among different hospitals using heterogeneous database servers. These limitations constitute a burden towards a personalized healthcare, when it comes to offering a cohesive view and a shared, secure and private access to patients' health history for multiple allied professionals and the patients. The data availability, privacy and security characteristics of the blockchain have a propitious future in the healthcare presenting solutions to the complexity, confidentiality, integrity, interoperability and privacy issues of the current client/server architecture-based EHR management system. This paper analyzes and compares the performance of the blockchain and the client/server paradigms. The results reveal that notable performance can be achieved using blockchain in a patient-centric approach. In addition, the immutable and valid patients' data in the blockchain can aid allied health professionals in better prognosis and diagnosis support through machine learning and artificial intelligence.

Keywords: artificial intelligence; blockchain; client/server; electronic health records; health information management; privacy; security

1. Introduction

Healthcare data management is the process of storing and analyzing patients' health records to improve patient treatment, track the causes of diseases efficiently, manufacture effective medicines and establish an accurate prevention agenda. The early form of data management includes documenting patient's complaints, diagnosis and the corresponding treatment manually introduced in a health record. Later, with the development of digital data, electronic health records (EHRs) came into existence [1]. For accurate health care, EHRs are often required to be shared among different healthcare organizations, medical drug manufacturers, pharmacists, medical insurance providers, researchers and patients. This poses a serious challenge in keeping the patients' sensitive data secure and up to date. A patient may visit/get transferred to different hospitals during the treatment lifecycle. A patient in such a situation owns the right over their own medical data and may require defining access control limits, says the U.S Department of Health and Human Services [2] and the European Parliament and the Council of the European Union [3]. The patient needs to sign a consent form stating what data will be shared and with whom and for how long. The consent form and the data are then posted to the recipient instead of sending them over the Internet due to security concerns [2]. Consequently, the process of sharing a patient's data between multiple hospitals becomes complex, time-consuming and difficult to coordinate. With the trend toward a personalized healthcare for better diagnosis

and prognosis, current EHR systems using the client/server approach are limited when it comes to providing a cohesive view and secure shared-access to patients' health history to multiple stakeholders, including the patients. In a centralized client/server approach, electronic health records are vulnerable to mistakes that can lead to life-threatening situations. Moreover, the patients need to trust the service provider and their exists privacy and security concerns.

Blockchain [4,5] is a very promising technology that enables a secure, private and distributed environment among peers without any trusted third-party using consensus. It is based on a shared, distributed and immutable ledger. Each transaction in the blockchain network is processed and validated by the majority of the network participants that eliminates the need of a trusted third-party. The validated transactions after verification are packed in blocks. Each block is linked to the preceding block by hashing the block's data along with the previous block's hash, providing immutability. The blocks in the network are considered valid when more than 50% of the participants reach an agreement using a consensus algorithm [6]. The immutable and replicated blockchain ledger is capable of solving the issues of scattered data, delayed sharing, lack of audit trail, privacy and security that prevail in the client/server model [7]. In addition, blockchain has an important characteristic of enforcing smart contracts—pieces of codes that are executed automatically once certain conditions are met. Blockchain-based EHRs have a tremendous potential in healthcare to enable allied health professionals to manage and share, not only clinical data, but also important patient-reported social and contextual data. Moreover, implementing artificial intelligence approaches on the ledger data that includes patients' health data from all the hospital in the network can aid allied health professionals in better prognosis and diagnosis support. While many researchers investigated the development blockchain-based system for healthcare data management, most of the works focus on the comparison of different blockchain development platforms [8–10]. As far as we know, this is the first work to evaluate and compare the blockchain technology with the current client/server model.

The major contributions of the paper are as follows:

- While the blockchain characteristics are suitable for implementing a healthcare system, these mechanisms are still costly considering execution time and amount of data transferred for ledger update.
- In spite of these costly mechanisms, notable performance can be achieved thanks to the blockchain model, especially in a patient-centric approach. In this approach, the patients and/or the physicians are constantly visiting the health records to construct a cohesive view from different hospitals for a better diagnosis or prognosis of diseases using artificial intelligence.

The rest of the paper is organized as follows. We overview the related work in Section 2. In Section 3, we introduce the principles of blockchain and its benefits to healthcare. We discuss the system model for the developed blockchain-based healthcare platform in Section 4. We present the experiments, and comparative analysis of client/server model versus blockchain using several application scenarios in Section 5. Section 6 concludes this paper.

2. Related Work

Traditionally, EHRs are employed by the healthcare organizations using a client/server architecture where the hospitals retain primary stewardship [11]. The medical data of a patient receiving treatment from multiple hospitals are scattered among different databases. To address this issue, several cloud-based eHealth applications are proposed [12–17]. However, privacy and security are the major concerns in the client/server and cloud-based models. Several research efforts address the privacy concern by managing the health data in cloud storage and recording the hash of the data in a special blockchain network [18–25]. Wang et al. [26–33] propose mechanisms for data integrity and authenticity of health records in a blockchain.

Several works [8–10,34–43] propose a blockchain-based healthcare data management system involving multiple hospitals. Azaria et al. [35] propose an interoperable blockchain-based application

that enables allied health professionals to share patients' health records. Dagher et al. [8] and Li et al. [36] propose an Ethereum-based blockchain framework for smart contract enabled medical data access. However, the blockchain networks in [8,35,36] use the energy-hungry and non-scalable Proof of Work (PoW) consensus mechanism [44–46]. Fan et al. [9] and Zghaibeh et al. [34] develop an EHR blockchain-based framework using Practical Byzantine Fault Tolerance (PBFT) consensus which is more energy-efficient and has better performance than PoW [47]. The healthcare data management systems proposed by [37,38,42,43] allow patients to retain the primary stewardship of the medical data because only the patients have the right to upload their data to the network. In these systems, the allied health professionals can only access the patients' health record. Uddin et al. [10,39–41] propose a blockchain-based healthcare system with both allied health professionals and patients having data update authority. As far as we know, there is no work that compares the client/server and blockchain-based healthcare data management systems. In this paper, we implement a minimal blockchain-based healthcare platform and compare its execution time and amount of data transferred with the client/server system model for health records update and query. This is with increasing number of records and hospitals.

3. Blockchain Paradigm

Figure 1 shows the blockchain architecture. The architecture consists of the following layers [6]:

1. *Infrastructure layer*: It includes the network nodes (known as participants), network modules and storage provisions. There are three types of participants: (1) simple which only performs the transactions, (2) validating which performs and validates transactions, and has a copy of the ledger and (3) mining which generates a new block and has a copy of the ledger.
2. *Platform layer*: It includes modules for communication between the blockchain participants.
3. *Computing layer*: It includes the underlying blockchain mechanisms for immutability, availability, finality, provenance, privacy and security.
4. *Application layer*: It enables the blockchain participants to communicate with the application.

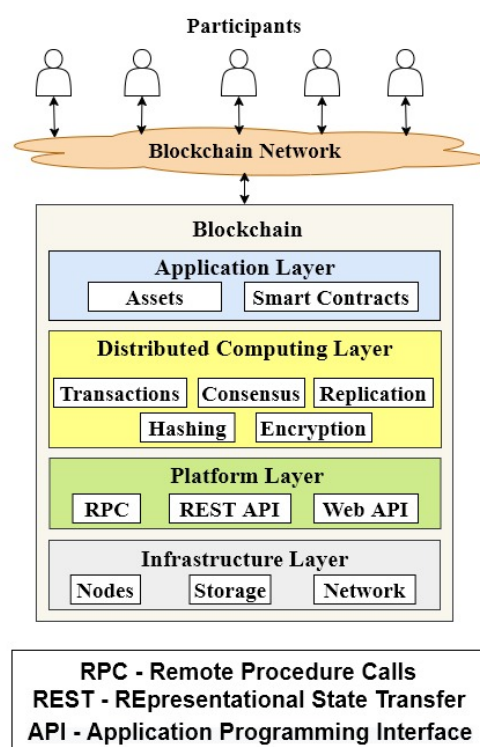


Figure 1. Blockchain architecture.

A blockchain network can be classified as either permission-less or permissioned [48]. The permission-less network (also called public) is open for anyone to join using a pseudo-name [49]. The users are encouraged to join the network for enhanced security by offering incentives. The ledger data in this network are visible to everyone. The permissioned network (also known as private) is an invitation-based network that allows only authorized participation. The visibility of the data is subject to access control rights as defined by the certificate authority. Considering the restricted network participation, the permissioned blockchain is more scalable and has a higher throughput compared to the permission-less.

3.1. Features of Blockchain

Blockchain is a peer-to-peer network that enables the stakeholders to share transactions with each other ensuring decentralization. It has the following features:

- *Decentralization*: A centralized third-party is not required as the ledger is updated after the majority of the participants in the network reaches a consensus.
- *Immutability*: A block in the ledger is hashed using its contents and the hash of the previous block. Consequently, any modification in a block will modify all the following blocks in the ledger. This makes the modification of a block in blockchain computationally difficult because the ledger is replicated among peers. In case data are entered by error, these data are corrected by issuing a new transaction.
- *Transparency*: Any change in the network is recorded as a transaction and can be viewed by all the participants maintaining a copy of the ledger.
- *Traceability*: The replication of any event in the network enables convenient tracing and audit trail.
- *Trustless*: Participants unknown to each other can perform transactions among each other as the consensus mechanism maintains the trust in the network.

3.2. Transaction Execution Mechanism

A transaction is an action that alters the blockchain ledger. It is application dependent and can be the transfer of monetary assets or execution of a smart contract. The transaction execution flow in blockchain is as follows:

- *Transaction proposal*: The user hashes the transaction using a hashing algorithm. The user's private key is then used to encrypt this hashed value. The result is known as the digital signature. The digital signature along with the data is broadcasted to the network.
- *Transaction validation*: The transaction is validated by each validating node. This is by authenticating the user identity and ensuring the data integrity. The identity is authenticated by decrypting the signature and the integrity is ensured by hashing the transaction and comparing it with the decrypted result. The valid transaction is sent to the mining node.
- *Block generation*: The mining node (selected based on the consensus protocol used) verifies the valid transactions and groups them in a block in a way that the block size does not exceed a predetermined threshold. It hashes the transactions data, block version, timestamp and previous block's hash value, and then hashes this hash value to obtain the hash of the block. The miner broadcasts the block to the network.
- *Replication*: The validating and mining nodes verify the validity of the block as part of the consensus protocol. Once valid, each node updates its copy of the ledger by appending the block.

3.3. Benefits to Healthcare

A blockchain-based healthcare platform provides the following benefits compared to the client/server approach:

- *Fault tolerance*: In a client/server-based system the patients' health data are managed in a centralized database. Once the data are lost, they cannot be recovered. The replication characteristic of blockchain aids in fault tolerance.
- *Data sharing*: In the current client/server systems, a patient's data are scattered over multiple hospitals' databases. The sharing of data among different hospitals and medical organizations is a complex process. However, in a blockchain-based platform, the patients' data recorded in the ledger is replicated among all the hospitals in the network.
- *Interoperability*: In a client/server-based system, each hospital stores the patients' data in a different database using heterogeneous data formats and structures resulting in interoperability challenges. The synchronized and replicated ledger in the blockchain solves this issue.
- *Avoidance of tests repetition*: Currently the patients' data are scattered across different healthcare providers, a patient often needs to repeat various laboratory and pathological tests. This not only incurs huge medical bills but also has adverse effects on the human body. The replicated blockchain ledger aids in avoiding medical tests.
- *Security*: The existing client/server-based system is prone to different cyber-attacks such as phishing and hacking. The stolen health records can be used to buy medical equipment by creating a fake ID or combining a patient number with a false provider to claim medical insurance. Table 1 shows the number of health data records breached in America based on a report by the Health Insurance Portability and Accountability Act (HIPAA) [50], and the cost per breached health record based on a report by the Federal Bureau [51] between 2009–2019. This cost of health record breach includes the expenses for forensic experts, outsourcing hotline support, the value of customer loss and free subscriptions and discounts for future services [52]. The table shows a spike in the number of health records breached in 2015. This is due to the largest health records breach encountered so far by the health insurance company, Anthem, with almost 78.8 million individuals affected as the patients' records were not encrypted [53]. The immutability feature of blockchain ensures data security.

Table 1. Number of health record breaches and cost per breached health record between 2009–2019.

Year	Number of Health Records Breached	Cost per Breached Record (USD)
2009	0	204
2010	6,006,063	214
2011	13,407,992	194
2012	2,808,042	233
2013	7,401,928	255
2014	12,946,972	308
2015	113,270,000	363
2016	27,300,000	355
2017	5,138,179	380
2018	13,947,909	408
2019	41,335,889	429

4. A Blockchain-Based Healthcare System Model

We develop a basic blockchain platform for healthcare which provides minimal functionality to program healthcare transactions. This is using a permissioned blockchain network due to its advantages over the permission-less. The blockchain-based healthcare system model consists of participants such as patients, allied health professionals (doctors, nurses and pharmacists) and administrators; assets such as medical test data; and transactions such as health record update and query. Figure 2 shows the developed blockchain-based healthcare platform overview. It shows that the platform involves several hospitals and participants, including patients, connected to the blockchain network. A hospital includes different departments such as radiology and pathology laboratories

as well as doctors, nurses, pharmacists and administrators. Let N represent total hospitals, K total participants and M total patients ($M < K$) in the network. Each hospital i , $i \in \{1, \dots, N\}$, maintains a copy of the ledger. A participant k , $k \in \{1, \dots, K\}$ updates/queries the health record of a patient j , $j \in \{1, \dots, M\}$. For every healthcare transaction, the doctors and pharmacists act as full nodes and the administrator acts as a mining node. The developed minimal blockchain-based healthcare platform supports two types of transactions: (1) data update and (2) data query.

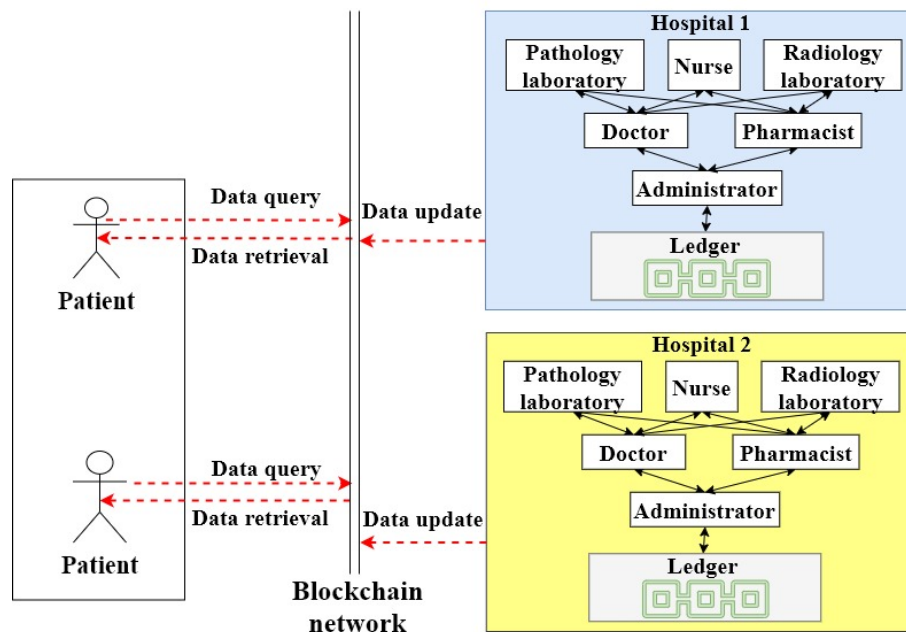


Figure 2. Blockchain-based healthcare data management platform.

In the developed platform, in order to perform a healthcare transaction, the patient and/or allied health professionals send the transaction to the blockchain network. The doctors and pharmacists validate the transaction, and the validated transaction is sent to the administrator that acts as a miner. The administrator will generate the block for the transaction and broadcast it to all other hospitals' administrators for replication. The execution flow for the healthcare transaction in the developed blockchain-based healthcare platform is shown in Figure 3. The selection of the miner and the ledger update is done using a consensus protocol.

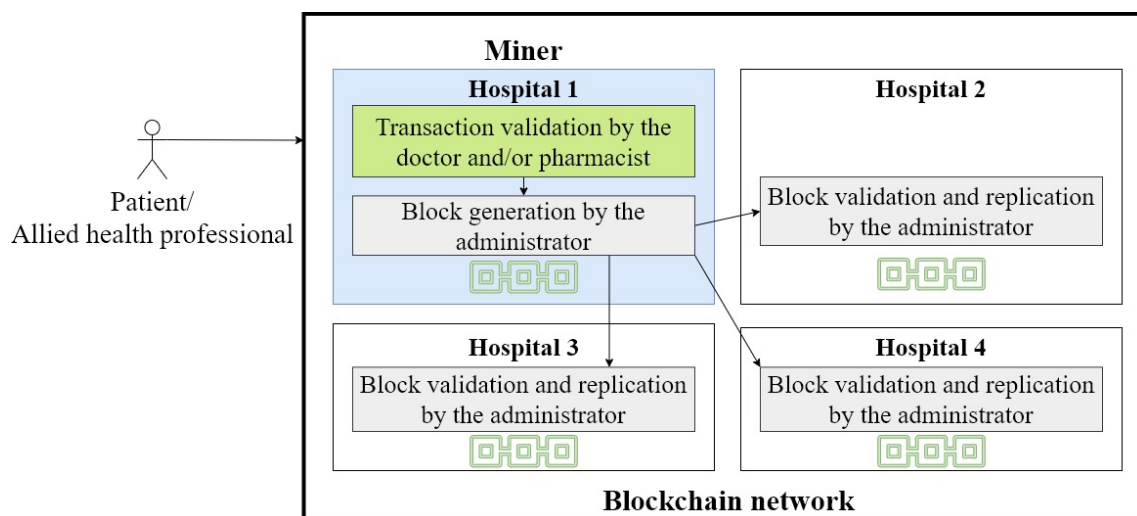


Figure 3. Healthcare transaction execution flow.

The consensus protocol used in the developed blockchain-based healthcare platform is the PBFT [54]. The PBFT consensus protocol is selected over the mostly used Proof of Work (PoW) because the latter consumes more energy [44,45] and less throughput [46] than the former. In PBFT, the mining nodes are known as peer nodes. A leader node is selected from the peers in a round-robin manner. The leader receives all the transactions from the network participants. The transactions are validated and a block is generated. The block is then broadcasted to all the peers. Each peer node verifies the transactions in the block, recalculates the block's hash and broadcasts the block's hash to all other peer nodes in the network. Each peer node then updates its ledger with the block if it receives the same block's hash value from 2/3 of the total peer nodes in the network.

A block in the ledger corresponding to a health record of a patient j primarily consists of the transaction with the workload $W_t(j)$ and the block's hash with the workload $W_{bh}(j)$. The total workload of the block is represented by $W_b(j)$, which is the summation of $W_t(j)$ and $W_{bh}(j)$. When a participant k initiates an update/query transaction to a health record of patient j , the execution time (ET_j) is given by Equation (1).

$$ET_j = TC_j + TP_j \quad (1)$$

where TC_j represents the communication time for transferring the total workload between the communicating nodes. It is calculated by dividing the total workload by the network bandwidth between the communicating nodes. TP_j indicates the processing time which is calculated as the summation of the time taken to generate the digital signature of the transaction j , the time taken to generate the block by the leader node and the time taken to validate the hash of the block by the peer nodes. In this paper, we consider the communication time and neglect processing time. The communication time (TC_j) for the blockchain ledger update/query is calculated as stated in Equation (2).

$$TC_j = TC_{j(k, miner_i)} + TC_{j(validator_i, leader_i)} + TC_{j(leader_i, peer)} + TC_{j(peer)} + TC_{j(miner_i, k)} \quad (2)$$

where $TC_{j(k, miner_i)}$ represents the communication time for transferring the health record transaction of patient j between the participant k and the blockchain mining node i (hospital), $TC_{j(validator_i, leader_i)}$ indicates the transaction communication time between the validator and the miner of the mining node i , $TC_{j(leader_i, peer)}$ denotes the block communication time between the leader of the node i and the peer nodes, $TC_{j(peer)}$ represents the block's hash communication time between the peer nodes and $TC_{j(miner_i, k)}$ denotes the communication time for the acknowledgement between the mining node i and the participant k . Equations (3)–(7) show the calculation of these terms.

$$TC_{j(k, miner_i)} = \frac{W_t(j)}{C_{k,i}} \quad (3)$$

$$TC_{j(validator_i, leader_i)} = \frac{W_t(j)}{C_{validator_i, leader_i}} \quad (4)$$

$$TC_{j(leader_i, peer)} = \sum_{i \in \{N\} - \{leader\}} \frac{W_b(j)}{C_{leader, i}} \quad (5)$$

$$TC_{j(peer)} = \sum_{h \in \{N\} - \{leader\}} \sum_{i \in \{N\} - \{leader, h\}} \frac{W_{bh}(j)}{C_{h, i}} \quad (6)$$

$$TC_{j(miner_i, k)} = \frac{W_{ack}(j)}{C_{i, k}} \quad (7)$$

Similarly, the amount of data transferred ($W_{total}(j)$) to update/query the health record of a patient j can be calculated using Equation (8).

$$W_{total}(j) = 2 * W_t(j) + W'_b(j) + W'_{bh}(j) + W_{ack}(j) \quad (8)$$

where, $W_t(j)$ represents the amount of data transferred while broadcasting the transaction from the participant to the mining node. It is similar to the amount of data transferred between the validating and the mining node. Consequently, the term $W_t(j)$ is multiplied by 2 in Equation (8). It can be calculated using the size of the transaction. The term $W_{ack}(j)$ denotes the amount of data transferred between the mining node and the participant for acknowledgment and it is same as the size of the acknowledgment signal. $W'_b(j)$ and $W'_{bh}(j)$ in Equation (8) are calculated using Equations (9) and (10), respectively.

$$W'_b(j) = \sum_{i \in \{N\} - \{leader\}} W_b(j) \quad (9)$$

$$W'_{bh}(j) = \sum_{h \in \{N\} - \{leader\}} \sum_{i \in \{N\} - \{leader, h\}} W_{bh}(j) \quad (10)$$

where $W'_b(j)$ indicates the amount of data transferred while broadcasting the block having workload $W_b(j)$ from the leader node to the peer nodes and $W'_{bh}(j)$ represents the amount of data transferred between the peer nodes for consensus.

The blockchain-based healthcare system model enables the sharing of health records to provide more accurate and timely patient care. However, protecting the privacy, confidentiality and security of the records is crucial to effective data sharing [55]. Privacy refers to the rights of a patient to control their own data. Confidentiality refers to the obligations of allied health professionals and administrators who use patient's data to maintain the privacy of patient identity. According to the title 42 of the Code of the Federal Regulations part 2 in the USA, the healthcare providers are required to obtain the patient's written consent in order to share the health records with other medical organizations, even for treatment [56]. The Data Protection Act 1998 [57] and the Human Rights Act 1998 [58] provide a framework that governs a confidential usage and sharing of patients' health records. These privacy and confidentiality laws can be reinforced using smart contracts and access control mechanisms. Furthermore, according to the HIPAA security rule [59], the integrity of health records should be ensured by employing proper encryption and authentication methods. In blockchain, security is established by signing every health transaction digitally using encryption mechanisms [60] and hash-chaining of transactions to reinforce data integrity.

In order to maintain data privacy and security, various blockchain participants have different role-based access rights to patients' health records. A primary care health provider should have full access to all patient's health history, including patient's identification such as name, contact details, photographic image, biometric details and medical record number; biological data such as height, weight and waist circumference; medical data such as body temperature, blood pressure, sugar level, diagnosis, treatment and allergies; laboratory and pathological results such as x-rays, magnetic resonance imaging, electrocardiography and computed tomography scans; and social data such as smoking habits, sleeping patterns, physical activity and diet plans. This provides the primary care with a cohesive view of the patient's health records for a personalized care and artificial intelligence-based prognosis/diagnosis. For biomedical research purposes, another level of accessibility to patients' data is defined. Biomedical researchers have access to anonymous data. Anonymity is reinforced via consent rules executed by the blockchain smart contracts.

5. Performance Evaluation

In this section, we analyze in which conditions the blockchain platform outperforms the client/server model by using two application scenarios. We evaluate and compare the execution time and amount of data transferred of these models for health records update and query with increasing number of health records and hospitals in the network.

5.1. Methods

5.1.1. Application Scenarios

We perform two experimental application scenarios to evaluate the performance of client/server and blockchain models: (1) health records update and (2) health records query.

In the first scenario, an allied health professional updates patients' health records. We develop this scenario using the client/server model where the allied health professional updates the hospital local database that acts as the server, as shown in Figure 4. After successful data update, the server sends an acknowledgement to the allied health professional. We then measure the total execution time and the amount of data transferred for this process. We also developed the application using our minimal blockchain platform, in which case the allied health professional sends a health record to the blockchain network (Figure 4). The administrator of the mining node elected as the leader creates a block for that record and sends it to the administrators of the peer nodes for verification. Each administrator will verify the block and send the block's hash to all other administrators in the network. An administrator updates the hospital's copy of the ledger once it receives the same hash value from the majority of the administrators. Once the block containing the health record is added to the chain, an acknowledgement is sent back to the allied health professional notifying successful data update. The execution time and the amount of data transferred for this process are then measured.

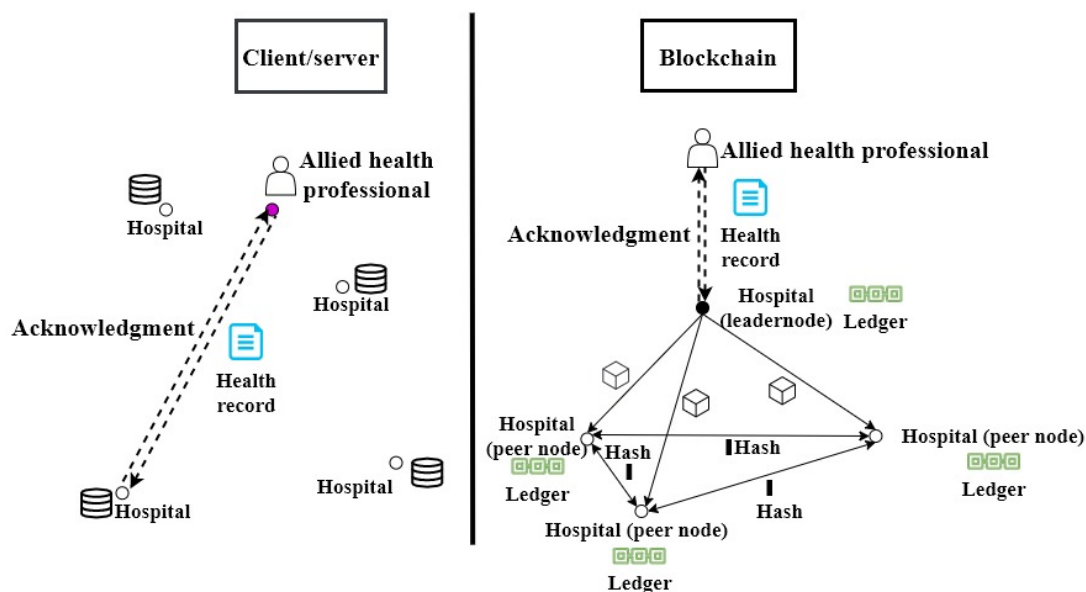


Figure 4. Application scenario for health record update using client/server and blockchain models.

In the second scenario, a patient and/or an allied health professional queries a health record. We develop this scenario using the client/server system model where the patient and/or allied health professional sends a health record query request to the hospital that has that record as shown in Figure 5. In response to the request, the hospital sends back the health records. We measure the total execution time and the amount of data transferred for this process. We also developed the application scenario using the minimal blockchain-based healthcare platform in which the patient and/or allied health professional sends the query request to the blockchain network (Figure 5). The administrator of the mining node elected as the leader creates a block for the query transaction and sends it to the other hospitals' administrators in the network. Each administrator will verify the block and send the block's hash to all other administrators in the network. An administrator updates the hospital's copy of the ledger once it receives the same hash value from the majority of the administrators. Upon ledger update, the health record is forwarded to the patient or allied health professional. The allied health

professional will retrieve the health record from its local copy of the ledger whereas the patient will retrieve it from the nearest hospital having a copy of the ledger.

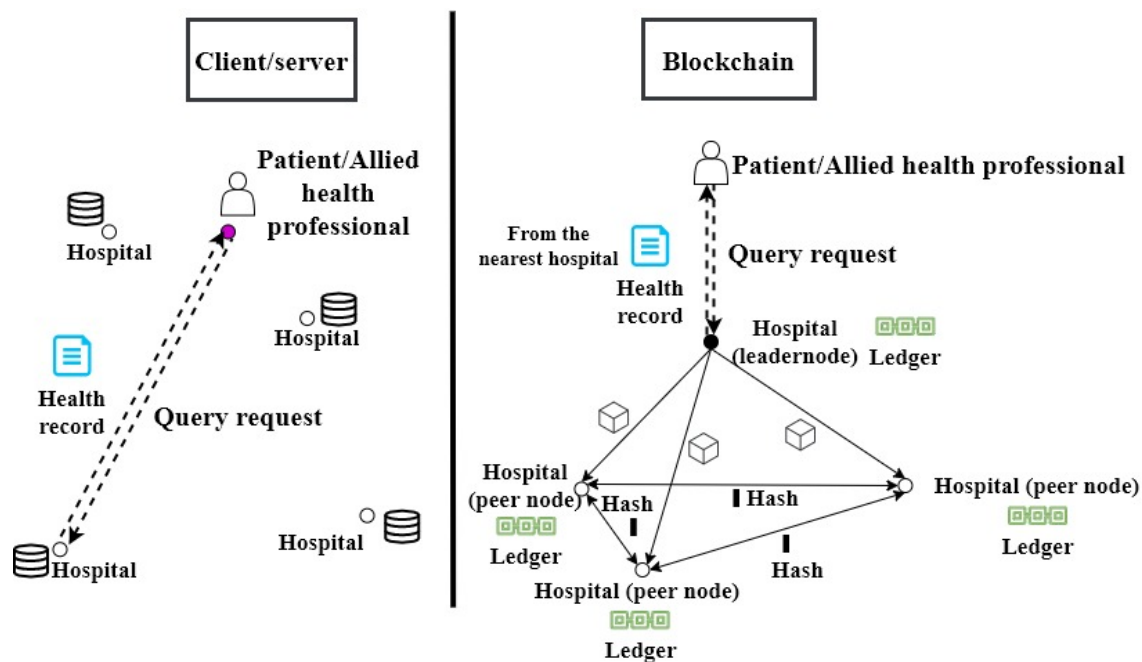


Figure 5. Application scenario for health record query using client/server and blockchain models.

5.1.2. Experimental Environment

To evaluate the client/server model and the blockchain-based healthcare platform, we implemented both network models. In the blockchain system model, we consider a block consisting of a single health record. This is to avoid the delay in the processing of health records in a situation when several records are grouped into a block that is limited by the block size. We use a health record of the size of 25.86 MB in the experiments. This is by considering that a record consists of images and texts of standard sizes, such as intraoral photography (1.64 MB), dental panoramic X-ray (0.85 MB), orthodontic cephalogram (1.20 MB) and skin lesion photography (22.17 MB) [61]. For the query application scenario, we used the block size of 1MB that represents a health record query. A block in blockchain consists of header and body. The body includes a health record in our experiments and the header consists of metadata information such as previous block's hash, timestamp, Merkle root hash value, block number and version [6]. In our experiments, we use the standard block header size of 80 Bytes. The hashing algorithm used in the experiments is SHA-256 that generates a unique 256-bit output for a given input [62]. The selection of SHA-256 is due to its popularity among the blockchain implementations. To evaluate the impact of a dynamic healthcare data management system, we perform all the experiments for the client/server and blockchain system models with increasing number of health records (4000, 5000, 6000, 7000, 8000 and 9000) and increasing number of hospitals (10, 20, 30, 40, 50 and 100). We increase the number of records while keeping the number of hospitals constant at 10, and we increase the number of hospitals while keeping the number of records constant at 4000. The selection of the minimum number of records, i.e., 4000 represents the average patients' records, visiting 10 hospitals (minimum number of hospitals in the experiments) per day, based on the Center for Health Statistics report [63]. We use Network Simulator NS3 [64] to develop the experiments.

5.2. Results Analysis

Figure 6 shows the execution time for updating health records using client/server and the developed minimal blockchain-based healthcare models with increasing number of health records.

It shows that the execution time for client/server and blockchain models increase linearly with increasing health records. However, the execution time for the client/server model is less than that of blockchain. This is because of the consensus mechanism used in the blockchain for data validation and replication. The health record that has to be updated to the ledger is transmitted to all the hospitals having the copy of the ledger for validation. In addition, each peer node will transmit the block's hash to the other peers in the network for consensus before appending it to the ledger. On the other hand, in the client/server approach, the data update request is transmitted to the hospital where the patient data exists. Consequently, the execution time of the client/server is less compared to blockchain approach for health records update. On average, the client/server approach takes 8.5 times less time for updating health records compared to the blockchain platform. Figure 7 shows the performance of client/server and blockchain models in terms of the amount of data transferred to update health records versus increasing number of records. It shows that the amount of data transferred in the blockchain platform is more compared to the client/server network. This is because each health record update request is broadcasted to all the peer nodes in the network by the leader node generating more data transfer. In addition, each peer nodes broadcasts the block's hash to all other peers in the network increasing the data transfer. On average, blockchain model transfers 10 times more data compared to the client/server approach.

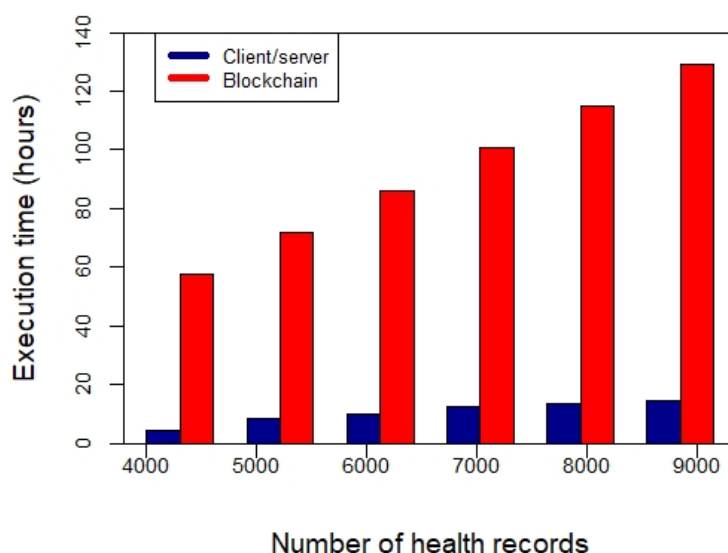


Figure 6. Execution time for health records update using client/server and blockchain with increasing number of health records.

Figure 8 shows the execution time of client/server and the developed minimal blockchain-based healthcare models for querying health records from the databases with an increasing number of health records. It shows the execution time of blockchain is significantly less than the client/server approach. This is because in client/server, the data are retrieved from the server where the record exists, while in blockchain the data are retrieved from the local copy of the ledger. The execution time in the blockchain is only due to transmission of data query request to all the nodes in the network and to add the request as a transaction in a block upon consensus. On average, blockchain is 11.7 times faster compared to the client/server approach for querying health records. Figure 9 shows the amount of data transferred by client/server and blockchain models for querying health records from the databases with an increasing number of health records. It shows the amount of data transferred by the blockchain platform is more compared to the client/server approach. This is because of the PBFT consensus protocol used by blockchain. On average, blockchain transfers 1.1 times more data compared to the client/server

approach for querying health records. However, the amount of data transferred by blockchain for ledger query (Figure 9) is less compared to the one for ledger update (Figure 7). This is because, for ledger update, a block includes a single health record to be updated, whereas, for ledger query, it includes a query request which is comparatively small in size.

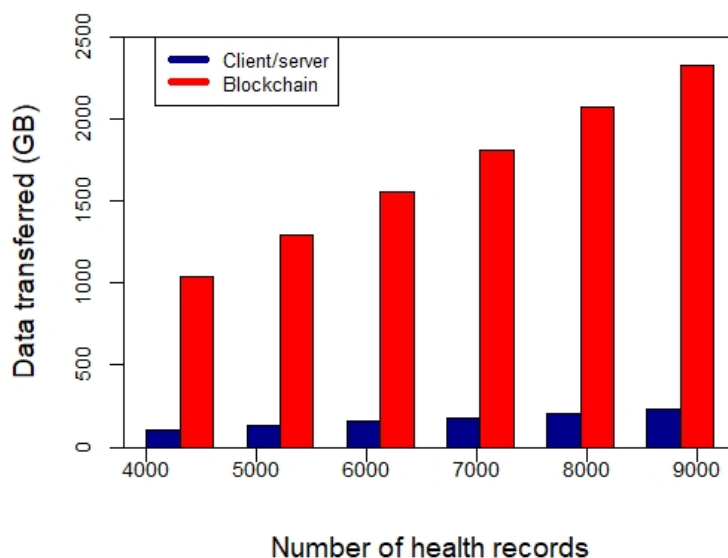


Figure 7. Amount of data transferred for health records update using client/server and blockchain with increasing number of health records.

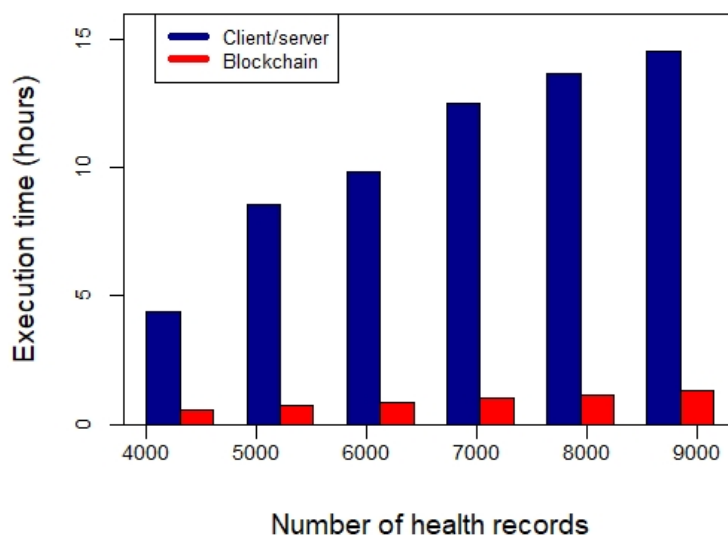


Figure 8. Execution time for health records query using client/server and blockchain with increasing number of health records.

Figure 10 shows the execution time of client/server and blockchain models for updating health records with an increasing number of hospitals. The relative performance is similar to that with an increasing number of health records (Figure 6). It shows that the blockchain model has more execution time than the client/server. On average, the client/server approach takes 13 times less time for updating health records compared to blockchain. Figure 11 shows the amount of data transferred

by client/server and blockchain approaches for updating health records with an increasing number of hospitals. It shows the execution time of blockchain is more than the client/server approach due to the consensus protocol used by the former. On average, the amount of data transferred by blockchain increases 10 times compared to the client/server approach with every 10 hospitals increased.

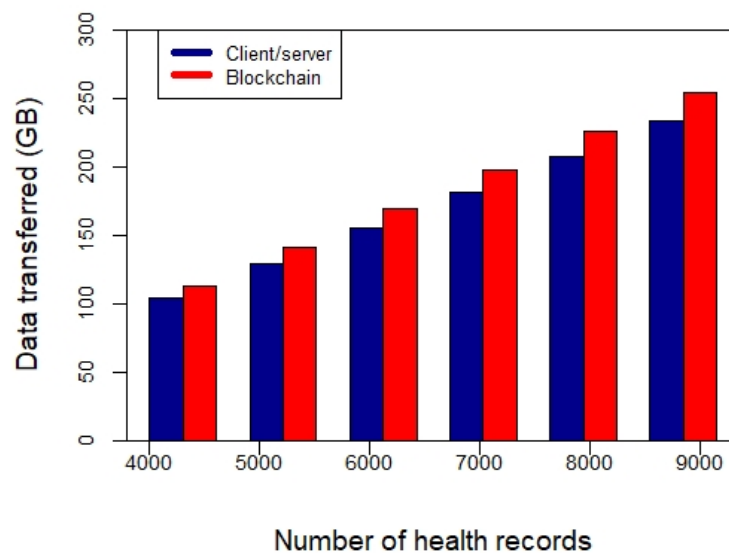


Figure 9. Amount of data transferred for health records query using client/server and blockchain with increasing number of health records.

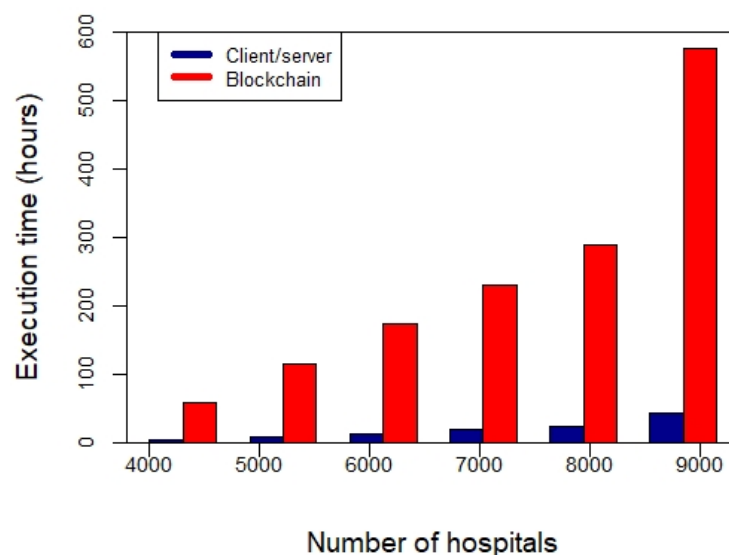


Figure 10. Execution time for health records update using client/server and blockchain with increasing number of hospitals.

Figure 12 shows the execution time for querying health records from the databases with an increasing number of hospitals. The relative performance is same when we increase the number of health records (Figure 8). It shows the execution time of blockchain is significantly less compared to that of the client/server approach. On average, blockchain is 8 times faster compared to the client/server approach for health records query. Figure 13 shows the amount of data transferred by

client/server and blockchain models for querying health records from the databases with an increasing number of hospitals. It shows that the amount of data transferred by the client/server model is constant. This is because the number of health records queried is constant irrespective of the number of hospitals. The query will be performed to the hospital having the required record. However, the amount of data transferred by the blockchain platform for querying health records increases with the number of hospitals. This is because of the exchange of messages between the hospitals due to PBFT consensus. On average, the amount of data transferred by blockchain is 1.1 times more compared to the client/server model for 10 hospitals.

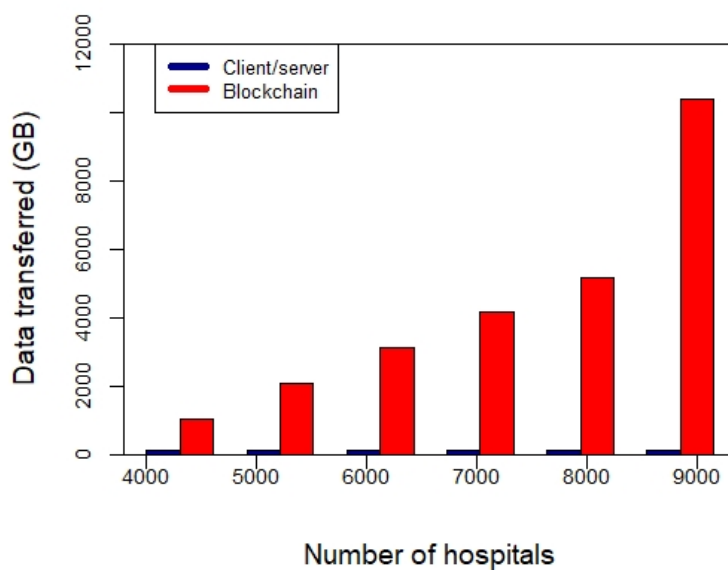


Figure 11. Amount of data transferred for health records update using client/server and blockchain with increasing number of hospitals.

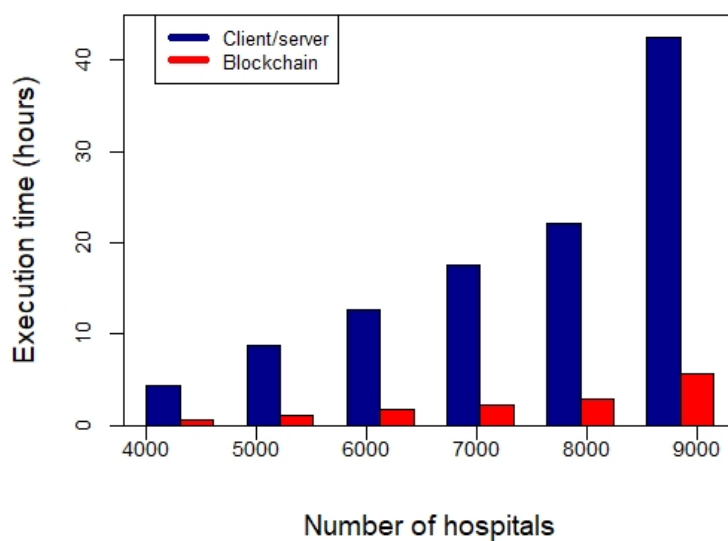


Figure 12. Execution time for health records query using client/server and blockchain with increasing number of hospitals.

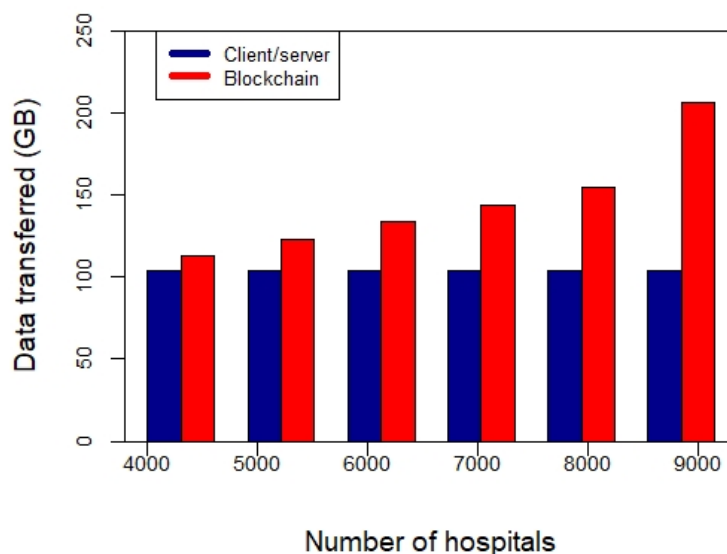


Figure 13. Amount of data transferred for health records query using client/server and blockchain with increasing number of hospitals.

Table 2 shows the performance of client/server and blockchain approaches in terms of execution time for ledger update and query with increasing number of health records and hospitals. It shows that blockchain outperforms client/server for ledger query with both increasing number of health records and hospitals. Table 3 shows the amount of data transferred of client/server and blockchain approaches for ledger update and query with increasing number of health records and hospitals. The client/server approach outperforms blockchain in all application scenarios.

Table 2. Execution time for client/server and blockchain with increasing health records and hospitals.

Increasing variable	Variable increasing factor	Average Increase in Execution Time (Hours)			
		Health Records Update		Health Records Query	
		Client/server	Blockchain	Client/server	Blockchain
Number of health records	+1000	2.03	14.36	2.03	0.14
Number of hospitals	+10	4.42	57.44	4.42	0.58

Table 3. Amount of data transferred for client/server and blockchain with increasing health records and hospitals.

Increasing variable	Variable increasing factor	Average Increase in Data Transfer (GB)			
		Health Records Update		Health Records Query	
		Client/server	Blockchain	Client/server	Blockchain
Number of health records	+1000	25.86	258.61	25.86	28.18
Number of hospitals	+10	0	1034.98	0	10.34

6. Conclusions

While many researchers investigated the application of blockchain for healthcare data management, however to our knowledge there is no evaluation of this new paradigm with the traditional client/server model. The client/server model suffers from the issue of data stewardship, data fragmentation, vulnerability, security and privacy. Blockchain paradigm has a strong potential to enhance health records management due to its immutability, security, privacy and data replication

features. In this paper, we presented a comparative analysis of the two models for healthcare data management.

To analyze the performance of the models under study for updating and querying health records, we developed a basic healthcare platform based on blockchain paradigm. The results of the experiments show that the blockchain paradigm can lead to significant improvements. This is in particular in a patient-centric approach where the patients and/or the physicians are constantly visiting the health records to construct a cohesive view from different hospitals for a better diagnosis or prognosis using machine learning and artificial intelligence algorithms. Our results show that the health records query for the blockchain platform is 11.7 times faster compared with the client/server model with increasing number of health records. However, the blockchain-based system model is more costly than the client/server system model considering the execution time and the amount of data transferred whenever the transaction involves an update of the health record. This is due to the consensus mechanism involved in the ledger update. One of the future research directions is to implement the developed platform to evaluate its privacy and security.

Author Contributions: Conceptualization, L.I.; methodology, L.I.; investigation, L.I. and H.M.; writing—original draft preparation, L.I. and H.M.; writing—review and editing, L.I.; supervision, L.I.; project administration, L.I. All authors have read and agreed to the published version of the manuscript.

Funding: Thanks to the Emirates Center for Energy and Environment Research of the United Arab Emirates University for supporting this work (Grant G00003304).

Acknowledgments: We would like to thank the anonymous reviewers for their invaluable feedback.

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

References

1. Jamoom, E.; Yang, N.; Hing, E. *Adoption of Certified Electronic Health Record Systems and Electronic Information Sharing in Physician Offices: United States, 2013 and 2014*; Technical Report 236, NCHS Data Brief; U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, National Center for Health Statistics: Hyattsville, MD, USA, 2016.
2. The HIPAA Privacy Rule. Available online: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (accessed on 5 March 2020).
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046> (accessed on 5 March 2020).
4. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 20 July 2020).
5. Ismail, L.; Hameed, H.; AlShamsi, M.; AlHammadi, M.; AlDhanhani, N. Towards a Blockchain Deployment at UAE University: Performance Evaluation and Blockchain Taxonomy. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu, HI, USA, 15–18 March 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 30–38.
6. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
7. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
8. 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]
9. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef] [PubMed]
10. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]

11. Who Owns Medical Records: 50 State Comparison. Available online: <http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison> (accessed on 5 March 2020).
12. Introduction-HealthVault Development. Available online: <https://docs.microsoft.com/en-us/healthvault/introduction/introduction> (accessed on 5 March 2020).
13. MTBC PHR: Personal Health Records for Patients. Available online: <https://phr.mtbc.com/phrdefault.aspx> (accessed on 5 March 2020).
14. OpenClinical e-Health Applications: MyPHR. Available online: http://www.openclinical.org/publicApp_myPHR.html (accessed on 5 March 2020).
15. Capzule PHR: Your Family Health Data in One App. (Personal Medical/Health Records). Available online: <https://www.capzule.com/> (accessed on 5 March 2020).
16. My Medical—The Personal Medical Record for You, The Patient. Available online: <http://mymedicalapp.com/> (accessed on 5 March 2020).
17. Individual Electronic Healthrecord-GenexEHR. Available online: <https://www.genexehr.com/individual-electronic-healthrecord> (accessed on 5 March 2020).
18. Saravanan, M.; Shubha, R.; Marks, A.M.; Iyer, V. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
19. 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; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
20. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inf. J.* **2019**, *25*, 1398–1411. [[CrossRef](#)]
21. Juneja, A.; Marefat, M. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In Proceedings of the 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Las Vegas, NV, USA, 4–7 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 393–397.
22. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [[CrossRef](#)]
23. Kleinaki, A.S.; Mytis-Gkometh, P.; Drosatos, G.; Efraimidis, P.S.; Kaldoudi, E. A blockchain-based notarization service for biomedical knowledge retrieval. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 288–297. [[CrossRef](#)]
24. Mytis-Gkometh, P.; Drosatos, G.; Efraimidis, P.; Kaldoudi, E. Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In *Precision Medicine Powered by pHealth and Connected Health*; Springer: Singapore, 2018; pp. 69–73.
25. Wu, H.; Shang, Y.; Wang, L.; Shi, L.; Jiang, K.; Dong, J. A Patient-Centric Interoperable Framework for Health Information Exchange via Blockchain. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 76–80.
26. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* **2018**, *42*, 152. [[CrossRef](#)]
27. Zhang, X.; Poslad, S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
28. Badr, S.; Gomaa, I.; Abd-Elrahman, E. Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Comput. Sci.* **2018**, *141*, 159–166. [[CrossRef](#)]
29. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* **2018**, *6*, 11676–11686. [[CrossRef](#)]
30. Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [[CrossRef](#)]

31. Brogan, J.; Baskaran, I.; Ramachandran, N. Authenticating health activity data using distributed ledger technologies. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 257–266. [\[CrossRef\]](#)
32. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.; de Albuquerque, V.H.C. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [\[CrossRef\]](#)
33. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [\[CrossRef\]](#)
34. Zghaibeh, M.; Farooq, U.; Hasan, N.U.; Baig, I. SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities. *IEEE Access* **2020**, *8*, 70030–70043. [\[CrossRef\]](#)
35. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 25–30.
36. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **2018**, *42*, 141. [\[CrossRef\]](#) [\[PubMed\]](#)
37. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. HealthSense: A medical use case of Internet of Things and blockchain. In Proceedings of the 2017 International conference on intelligent sustainable systems (ICISS), Palladam, India, 7–8 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 486–491.
38. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [\[CrossRef\]](#)
39. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.Y. Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [\[CrossRef\]](#)
40. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inf.* **2017**, *71*, 70–81. [\[CrossRef\]](#)
41. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* **2018**, *42*, 156. [\[CrossRef\]](#) [\[PubMed\]](#)
42. Aswin, A.; Basil, K.; Viswan, V.P.; Reji, B.; Kuriakose, B. Design of AYUSH: A Blockchain-Based Health Record Management System. In *Inventive Communication and Computational Technologies*; Springer: Singapore, 2020; pp. 665–672.
43. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [\[CrossRef\]](#)
44. Bitcoin Mining Consumes More Electricity a Year Than Ireland. Available online: <https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland> (accessed on 3 May 2020).
45. Bitcoin Energy Consumption Index. Available online: <https://digiconomist.net/bitcoin-energy-consumption> (accessed on 3 May 2020).
46. Scherer, M. Performance and Scalability of Blockchain Networks and Smart Contracts. Ph.D. Thesis, Umeå University, Faculty of Science and Technology, Department of Computing Science, Umeå, Sweden, 2017.
47. What is Practical Byzantine Fault Tolerance (pBFT)? Available online: <https://crushcrypto.com/what-is-practical-byzantine-fault-tolerance/> (accessed on 3 May 2020).
48. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [\[CrossRef\]](#)
49. Pseudonymity. Available online: <https://en.wikipedia.org/wiki/Pseudonymity> (accessed on 3 May 2020).
50. Healthcare Data Breach Statistics. Available online: <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (accessed on 3 May 2020).
51. Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain. Available online: http://www.calhospital.org/sites/main/files/file-attachments/dp___attachment_fbi_alert.pdf (accessed on 3 May 2020).
52. Health Sector Cybersecurity Coordination Center (HC3). A Cost Analysis of Healthcare Sector Data Breaches. Available online: https://content.govdelivery.com/attachments/USDHSCIKR/2019/04/16/file_attachments/1193648/HC3%20-%20HPH%20Breach%20Cost%20whitepaper.pdf (accessed on 28 May 2020).

53. The Breach of Anthem Health—The Largest Healthcare Breach in History. Available online: <https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref> (accessed on 24 June 2020).
54. Castro, M.; Liskov, B. Practical Byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating System Design and Implementation (OSDI), New Orleans, LA, USA, 22–25 February 1999; Unisys Association: Berkeley, CA, USA, 1999; pp. 173–186.
55. Hodge, J.G.; Kaufman, T.; Jaques, C. Legal Issues Concerning Identifiable Health Data Sharing Between State/Local Public Health Authorities and Tribal Epidemiology Centers in Selected US Jurisdiction. 2011. Available online: <https://cdn.ymaws.com/www.cste.org/resource/resmgr/PDFs/LegalIssuesTribalJuris.pdf> (accessed on 21 June 2020).
56. Health Information Privacy Law and Policy | HealthIT.gov. Available online: <https://www.healthit.gov/topic/health-information-privacy-law-and-policy> (accessed on 21 June 2020).
57. Data Protection Act 1998. Available online: <http://www.legislation.gov.uk/ukpga/1998/29/contents> (accessed on 21 June 2020).
58. The Human Rights Act 1998 | Department of Health. Available online: <https://www.health-ni.gov.uk/articles/human-rights-act-1998> (accessed on 21 June 2020).
59. The HIPAA Security Rule. Available online: <https://www.hhs.gov/hipaa/for-professionals/security/index.html> (accessed on 21 June 2020).
60. Merkle, R.C. A digital signature based on a conventional encryption function. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1987; pp. 369–378.
61. Ruiz, M.G.; Chaves, A.G.; Ibañez, C.R.; Mazo, J.M.G.; Giraldo, J.C.R.; Echavarría, A.P.; Díaz, E.V.; Restrepo, G.P.; Munera, E.N.M.; Loaiza, B.G.; et al. mantisGRID: A grid platform for DICOM medical images management in Colombia and Latin America. *J. Digit. Imaging* **2011**, *24*, 271–283. [CrossRef] [PubMed]
62. SHA-256 Cryptographic Hash Algorithm. Available online: <https://www.movable-type.co.uk/scripts/sha256.html> (accessed on 5 March 2020).
63. National Hospital Ambulatory Medical Care Survey: 2017 Emergency Department Summary Tables. Available online: https://www.cdc.gov/nchs/data/nhamcs/web_tables/2017_ed_web_tables-508.pdf (accessed on 5 March 2020).
64. ns-3 | A Discrete-Event Network Simulator for Internet Systems. Available online: <https://www.nsnam.org/> (accessed on 5 March 2020).



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

© 2020. This work is licensed under
<http://creativecommons.org/licenses/by/3.0/> (the “License”). Notwithstanding
the ProQuest Terms and Conditions, you may use this content in accordance
with the terms of the License.