applied sciences

MDPI

Article

Toward Patient-Centric Healthcare Systems: Key Requirements and Framework for Personal Health Records Based on Blockchain Technology

Ohud Aldamaeen *, Waleed Rashideh and Waeal J. Obidallah

College of Computer and Information Sciences, Imam Muhammad Ibn Saud Islamic University (IMSIU), Riyadh 11673, Saudi Arabia; wmrashideh@imamu.edu.sa (W.R.); wobaidallah@imamu.edu.sa (W.J.O.)
* Correspondence: osaldammaeen@sm.imamu.edu.sa

Abstract: Healthcare data are considered sensitive and confidential, and storing these sensitive data in traditional (i.e., centralized) databases may expose risks, such as penetration or data leaks. Furthermore, patients may have incomplete health records since they visit various healthcare centers and leave their data scattered in different places. One solution to resolve these problems and permit patients to own their records is a decentralized personal health record (PHR); this can be achieved through decentralization and distribution systems, which are fundamental attributes of blockchain technology. Additionally, the requirements for this solution should be identified to provide practical solutions for stakeholders. This study aims to identify the key requirements for PHRs. A design science methodology was utilized to meet the study objectives, and thirteen healthcare experts were interviewed to elicit the requirements and the previous studies. Thirty-three requirements are defined, and based on these, high- and low-level architectures are developed and explained. The result illustrates that the developed solution-based Hyperledger Fabric framework is a promising method for the achievement of PHRs that guarantee security aspects, such as integrity, confidentiality, privacy, traceability, and access control.

Keywords: access control; blockchain technology; data owner; identity management; personal health records

Citation: Aldamaeen, O.; Rashideh, W.; Obidallah, W.J. Toward Patient-Centric Healthcare Systems: Key Requirements and Framework for Personal Health Records Based on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 7697. https://doi.org/10.3390/app13137697

Academic Editor: Andrea Prati

Received: 3 May 2023
Revised: 14 June 2023
Accepted: 26 June 2023
Published: 29 June 2023

1. Introduction

Healthcare systems currently face the dilemma of having to share medical data or electronic records with more stakeholders to serve many goals while also maintaining data integrity and protecting patient privacy. One common issue is the scattering of patient data in several places due to the fact that patients visit different healthcare providers. Moreover, reconducting procedures, such as X-ray and computed axial tomography scans, have drawbacks, such as loss of money and health dangers on top of a noncomplete health record. Furthermore, storing sensitive data in centralized databases may expose risks, such as penetration or data leaks. One solution to resolve the above problems and allow patients to own and control their records is a decentralized personal health record (PHR). According to Hau et al. [1], PHRs can be achieved through decentralization and distribution systems, which are fundamental attributes of blockchain technology. Blockchain technology stores the data and provides a copy of these data on all the connected nodes to continuously verify the validity of any transaction. A healthcare system based on blockchain offers a decentralized approach to storing and managing medical data without violating privacy. This method breaks the data silos of centralized, traditional health information systems. It enables patients to assemble and own their records without violating privacy [2]. Utilizing a consortium blockchain for PHRs helps patients have access to their complete health history at any time and from anywhere at first glance, and it helps physicians to know a patient's full medical history before issuing any prescriptions. In addition, a PHR allows for a unified

source across numerous healthcare organizations after obtaining the patient's approval [3], thus reducing the cost paid by patients for a service (i.e., affordability) and saving time [4]. On the other hand, the disclosure of patient data through unauthorized access or data breaches remains a challenge as it is a threat to patient privacy. Moreover, according to Arndt [5], many legitimate healthcare providers earn profit from selling these data. Thus, patients must be aware of who has permission to view their data and the purposes for which it is used; on top of this, patients should be the ones who benefit first from these data. Several laws and regulations have been enacted, such as the Health Insurance Portability and Accountability Act (HIPAA) [6] and the General Data Protection Regulation (GDPR) [7], to enable the application of guidelines and compliance in the healthcare industry on how to manage, process, and safeguard personal data; the recent attacks on the healthcare industry demonstrate that the sector's data security has challenges, as hackers find it an easy target [8].

Motivation

According to Lee et al. [9], further research should be conducted that includes more than one healthcare institution since, in their study, the interviewees were recruited from a single medical institution (i.e., more research is called for in this field). This encouraged us to conduct this research in order to expand on the related studies and enrich the health management industry with a practical solution to increase patient satisfaction in line with industry benefits. According to a survey conducted by Chukwu and Garg [10], almost two-thirds of sixty-one studies proposed general models to illustrate how blockchain could be a promising solution for health records without offering a prototype or implementation. Moreover, Meier et al. [11] call for more studies based on design knowledge to explore and accelerate further solutions for health records based on blockchain. According to [12], due to cybersecurity concerns there is a need to provide more details regarding how users' data are managed in a blockchain. This research extended our previous proposal [13] twofold. The first was through a qualitative methodology, where we conducted interviews with various stakeholders from different healthcare industries. Second, we employed design science after the requirements were collected and proposed a solution based on Hyperledger Fabric, a blockchain framework, to illustrate how these could be applied. Our PHR solution is focused on achieving three objectives:

- Data ownership: to ensure patients own and control their data;
- Access control: to allow patients to grant, revoke, or deny access to their data to other healthcare service providers or network researchers;
- Auditability: to allow patients to rigorously know how their data are being used, giving them authority to revoke access to anyone who has been found to be in violation.

Thus, the main contributions of this research are as follows:

1. It proposes a solution for personal health records based on blockchain to give patients the power to own and benefit from their data.
2. It introduces Hyperledger Fabric to achieve access control; govern identities for peers and users; and provide user authentication, credential validation, signature generation, and verification.
3. It designs and develops a working prototype based on the defined requirements.
4. It engages stakeholders from the industry to understand the real needs and to identify the requirements for PHRs.
5. It evaluates the functionality of the system's performance using the Hyperledger Caliper tool.

This paper is organized as follows. Section 2 presents an overview of blockchain technology. Section 3 provides a literature review. Section 4 is the methodology, followed by the results, discussion in Section 5, and limitations in Section 6. Finally, the conclusions and future works are presented in Section 7.

2. Blockchain Technology Overview

Recently, blockchain technology and its applications have gained significant attention from governments, organizations, and academics around the globe [14]. Blockchain was first presented through Bitcoin in 2008 by Nakamoto [15] and was created to keep track of financial transactions. Blockchain can be defined as a "cryptographic, distributed peer-to-peer ledger system which operates via a number of nodes, all jointly responsible for the maintenance of a database" [16].

Transactions in a blockchain are digitally signed to ensure their validity and correctness. Each block is cryptographically connected via a "chain" to the next block; this provides immutable storage and prevents fraudulent transactions. A node in a blockchain can be either a physical or a virtual machine with an IP address assigned to it [17]. Each user in the network has a public key, which is used as a reference, and a private key for cryptographically signing messages. All transactions stored in the network are replicated and synchronized on all existing nodes [18].

The blockchain is a distributed ledger technology designed to guarantee security, privacy, integrity, and traceability [19]. All transactions on the blockchain are verifiable and safe due to the existence of consensus algorithms that ensure standard agreement across all nodes in the current ledger state. Consensus algorithms guarantee that any new block added to the ledger is the sole version upon which all nodes agree [19].

2.1. Blockchain Types

Blockchain requires an understanding of three basic types.

- Public blockchain

A public blockchain or a permissionless network allows anyone to join a network without restrictions. Once users are authorized, they are allowed to participate in transaction verification and mining. There are plenty of types of this network, such as Bitcoin and Ethereum [20,21].

- Private blockchain

A private blockchain, also known as a permissioned network, is only utilized by a single organization, and no one outside of this network can join. Examples of this platform include MultiChain and Hyperledger [20,21].

- Consortium blockchain

A consortium blockchain is sometimes considered a private blockchain. However, the main difference is that it allows many trusted organizations with shared interests to join the network and form a consortium. Examples of this type are R3 and Quorum [20,21]. Figure 1 illustrates the blockchain types.

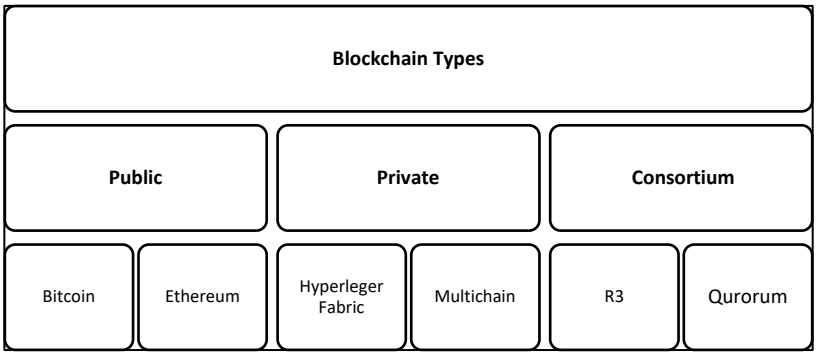

Figure 1. Blockchain types.

2.2. Hyperledger Fabric

Hyperledger Fabric is a distributed operating system that runs applications written in popular programming languages such as Go, Java, and Node.js [22]. Hyperledger Fabric is one kind of Hyperledger framework and was chosen for this study since it enables a private permissioned consortium blockchain. Hyperledger Fabric has a highly modular and configurable architecture and has critical features [23], such as the following:

- It is an open-source framework that permits work with open, widespread programming languages;
- It allows for the creation of private blockchains, which are crucial for supporting sensitive data;
- It does not require a mining process;
- It establishes a decentralized trust network of known participants instead of a public network of anonymous participants.

A Hyperledger Fabric network comprises a group of peers and orderers, which is an essential component of the network, and other elements, such as channels, policies for governance, applications, and a membership service for member identities.

3. Related Work

3.1. Access Control and Data Ownership

Electronic health records (EHRs) and PHRs allow physicians and healthcare providers to access and review their patients' health histories electronically. Various studies have been pursued to allow patients to control, own, and share their data. Zhuang et al. [24] proposed a system with two models based on a private Ethereum network to allow patients to own their data. First, there is a linkage model on the healthcare center's side that links EHRs to the blockchain to create a touchpoint for patient visits. Second, there is the request model, where patients provide permission for a clinic's physician and then add them to the authorized list. A patient also has the option to reveal what information the physician can view and can choose the data they wish to reveal. However, the system has scalability constraints. Zaabar et al. [25] developed a system to manage patient data from reports or IoT devices; the solution is based on Hyperledger Fabric and Composer. The solution focuses on collecting data from IoT devices to monitor a patient's vital signs, allowing the physician make the right decision at the right time. The patient has complete control of their EHR, and the physician must request permission to view it. Similarly, Pawar et al. [26] proposed a blockchain-based personal health information management system that allows users to have complete control over their data and the sharing of their data from their medical IoT devices. The system focuses on an adapter component that collects data from the backend of a wearable health device and sends it to the blockchain for storage rather than a provider's cloud storage. Another work, by Balistri et al. [27], proposed a high-level architectural solution for collecting and sharing health data while assuring immutability and data privacy. Following GDPR compliance, each patient has the right to be forgotten in terms of their data. Another solution for cross-institution and medical data sharing with highly secure data sharing was proposed by Tang et al. [28]. The system is built on the Ethereum framework and has two sorts of access based on incentives to allow patients to benefit from sharing their data. Non-incentive access is normal access provided to a physician, who can then view a patient's record. The incentive model is for researchers or marketing companies using these data for non-medical purposes. Uddin et al. [29] designed architecture for EHRs to ensure secure and private communication across various stakeholders utilizing Hyperledger Fabric. The proposed solution gives a patient access control over their record. The solution provides a general overview of how patients will manage their reports and how blockchain will be utilized. However, a deeper look is needed to address the real requirements for stakeholders and what kind of permissions and restrictions they must have. Another work, by Antwi et al. [30], designed and implemented scenarios based on a Hyperledger Fabric consortium after determining the general requirements for EHRs. The authors present experiments and illustrate how the system complies with the GDPR, achieving

security, privacy, and confidentiality by storing all data on-chain and providing access control. Considering the user's perspective, Meier et al. [11] developed three principles that should be considered when developing solution-based PHRs. First, the data structure should be unified in order to be easily integrated into the existing ecosystem. Second, the implementation should have a safe, reliable, and traceable infrastructure to prevent unauthorized access; finally, it should have an easy-to-use access control mechanism. The authors continued their work by developing an operational prototype based on a private blockchain and a Hyperledger Fabric framework. The authors recommended considering these principles in future works and utilizing consortium blockchain and stakeholder engagement. Other studies engaged stakeholders to understand their needs. Dubovitskaya et al. [31] developed an EHR data-sharing framework based on Hyperledger Fabric, where cancer patients can share their data and give access to physicians, who are constrained by time. The storage of large amounts of data is off-chain to avoid scalability issues. However, the study does not cover emergency access. Moreover, only one orderer was applied, and this was considered a single point of failure. Another solution integrates cloud computing within the blockchain. For instance, Albahli et al. [32] proposed a generic EHR model by mixing private and public blockchains so that patients can share their data. However, scenarios or prototypes based on real frameworks should be addressed to support such claims. Another work, by Toshniwal et al. [33], presented a high-level architecture for sharing data among healthcare stakeholders after patient permission is provided. The authors illustrated a proof of concept based on a private Ethereum blockchain. Another work, by Leeming et al. [34], presented a general reference architecture for PHRs. According to the authors, the architecture was designed after analyzing the current application of health records, and they illustrated how patients can have access control by adopting blockchain technology. However, the requirements were not illustrated for either the stakeholders or the patients, and the type of framework that should be utilized was not given.

From another angle, in the traditional emergency system, patients cannot provide access permission to emergency personnel to access their PHR. In some cases, a patient may transfer their record from healthcare centers where no medical record belongs. Few studies have been conducted to overcome this issue. Rajput et al. [35] proposed a simple framework for a patient emergency access control system that defines permission access rules through Hyperledger Fabric. Patients can determine access to their data in emergency conditions by setting an authorization access control policy for their data through a developed smart contract. Thus, in an emergency, the medical staff does not need to contact a patient's relatives or wait for a third party to approve access to their data. In contrast, the patient determines and defines an access control policy for their data by enabling an emergency physician to access their data for a limited time to ensure patient privacy.

Based on the storage of off-chain data in a decentralized file system, in [36] a healthcare data sharing system was proposed to overcome the performance and scalability issues of centralized databases. The study mainly focused on the performance analysis of a network considered for an emergency case of a patient, since traditional and off-chain-based cloud databases need to be much faster and scalable. The authors proposed a blockchain-based architecture containing three types of smart contracts: registry contracts for system protection from malicious users, data contracts for records storage, and permission contracts for access permission. The experiment showed better results compared to a traditional approach. However, the mechanism for how emergency conditions will be performed was not clarified in the architecture or even described.

3.2. Health Records and Patient Incentives

The incentive mechanism encourages patients to contribute their medical data for research, marketing, or other benefits and to receive incentives such as cryptocurrency. This mechanism is distinct from the blockchain system's incentive itself. According to Stafford and Treiblmaier [37], an incentive mechanism is valuable for patients since they

are empowered to monetize their private data through EMR applications. Gan et al. [38] presented a solution for patients to benefit from their data by obtaining a reward for sharing it with any third party; the proposed implementation method used a private blockchain network and the Ethereum framework. Another study was conducted by Mohammed Yakubu and Chen [39] to allow DNA donors to profit from shared genomic data in addition to having access control on a private blockchain. This solution is driven by the profits that organizations receive from selling these data, while donors receive nothing. Faber et al. [40] proposed a general architecture system for patient identity, data management, and access control. In addition to empowering patients to be the owners of their data, it allows patients to monetize the sharing of their data with businesses. A patient can receive a reward in two ways: first, the patient can take the initiative to share their data; second, they can respond to requests by confirming their permission to share. The patient only receives a reward once when sharing their data, and they cannot receive a reward when sharing multiple times, unless there is an update to their data.

3.3. Health Records and Stakeholder Engagement

The stakeholders' engagement should be considered when they are targeted as users. Beinke et al. [41] conducted interviews to collect requirements for EHRs based on blockchain. Thirty-four requirements were identified, both from previous studies and from stakeholders, and a five-tier architecture-based blockchain was designed as a future guide for EHRs based on decentralized systems. Nevertheless, the authors did not specify which framework these requirements and prototypes should be applied to. A survey on blockchain as a solution for managing health information was conducted by Hau et al. [1]. Patients and physicians were targeted to understand their attitudes regarding managing patient data. The patients showed a positive impression toward applying this technology to enhance their lives, as compared to the physicians, who showed a negative impression. As the research employed a quantitative method, the authors called for more research utilizing another method, such as interviews, to better understand the real needs and to obtain more explanations. Another interview-based study was conducted by Stafford and Treiblmaier [37] with stakeholders to obtain their views on the potential for blockchain to provide access and control to EMRs. The healthcare providers did not appear enthusiastic about EHRs because they are not financially viable and because they treat patients as clients. Moreover, there is a lack of awareness of blockchain and its potential in healthcare. The study does not reflect the industry's current situation, and its findings cannot be generalized. In addition, the study recommends future research to focus on understanding the current limitations and problems of user satisfaction with existing healthcare applications and the possibility of replacing them with blockchain applications.

4. Methodology

As mentioned earlier the aim of this study was to develop a PHR solution to the existing patient and centralized system dilemma. To achieve this, a practical methodology was needed. The authors chose the design science (DS) method [42]. The DS method addresses human-related dilemmas [43] and contributes to the generation of knowledge for the scientific community. DS is a practical methodology for the information systems field due to the fact that it is in its nature to solve more problems in this area than in other areas such as the social sciences [44]. Moreover, it is appropriate as a base for developing a blockchain-based PHR architecture that researchers in information systems and computer science commonly use [45]. The first activity of the framework was to explicate the problem; this activity aimed to precisely formulate the initial problem, justify its significance, and identify its root causes. A literature review was conducted to determine the related works.

A search for academic publications was conducted in information systems and healthcare databases, such as Sage, Emerald, IEEE Xplore, Springer, ProQuest, PubMed, ScienceDirect, Wiley, JMIR, Hindawi, MDPI, IEEE, Web of Science, and Google Scholar. The results include related works and their research problems. Additionally, to preserve the

rigor and quality of this research, conference proceedings, working papers, and book chapters were not considered. Defining requirements was the second activity; this aimed to find and define an artifact that could overcome the identified problem and elicit requirements for that artifact. The data collection methods were essential for achieving the research objectives. Interviews with stakeholders were conducted through purposeful sampling to gather and accurately identify and recruit various information-rich interviewees [46,47]. Only those with over four years of experience were selected because such participants would properly understand how health records were used in their working environment.

The researcher briefly introduced the participants to the research objectives and to how they would benefit and contribute to enriching the research. For ethical considerations, the researcher asked the participant's permission before recording the interview, and the responses ranged between approval and rejection. Ethical principles, including respect for the person's privacy, integrity, and confidentiality, were guaranteed. According to [48], confidentiality is critical to having honest and free discussions during an interview. A total of 13 interviews were conducted with participants from the public and private sectors in the Kingdom of Saudi Arabia, and their experience was varied. Table 1 presents the participants' information. The interviews lasted approximately 40 min on average and included face-to-face and remote interviews.

Table 1. Stakeholder interviews.

Interviewees' Information			
No.	**Position**	**Experience**	**Healthcare Provider Sector**
1.	IT manager	15	Private
2.	Medical records manager	6	Private
3.	Information and medical records director	21	Government
4.	Medical director and implementer of KFMC's electronic health record system	14	Government
5.	Physician and patient safety and quality manager	20	Private
6.	Physician and medical director	12	Private
7.	Clinical application specialist (ERM, ESM, HIM, charge services, and reporting) and executive manager	28	Government
8.	HIS and EMR manager	14	Government
9.	IT director	13	Private
10.	IT and HIS manager	21	Private
11.	Medical records manager	10	Government
12.	Deputy medical director (acts as the medical manager)	18	Government
13.	Medical records system administrator	7	Private

Thematic or qualitative content analysis was used to analyze the data [49]. Next, the interview transcripts were entered into Atlas.ti software version 9, which is used for qualitative data analysis [50], to help manage, organize, and discover richer insights. Three additional interviews were conducted to verify the results, and no new codes were created. The data and code saturation was reached in the tenth interview, where information and codes began to be repeated, and no new codes were generated. The third activity was to design and develop artifacts to fulfill the collected requirements, including the artifact's functionality and structure [42]. Unified modeling language (UML) has been used in designing different artifacts through the Lucidchart development tool. The high-level system architecture was illustrated and explained. The proposed Fabric architecture enables private permissioned blockchains where various healthcare stakeholders and users are registered and connected using channels to preserve privacy, confidentiality, access control, and scalability. The fourth activity was the demonstration, which assisted in convincing the audience of the validity of the idea behind the PHR solution. Moreover, it illustrated how the developed artifact can be utilized to address the problem in a single illustrative or real-world case [42]. Below is a summary of the overall architectural solutions design tools:

1. Web and mobile applications: a frontend web application for administrators, healthcare centers, and physicians and mobile apps for patients;
2. Node API server: a RESTful API (application programming interface) that uses HTTP requests to GET, PUT, POST, and DELETE data to the blockchain. It enables external components to access the blockchain;
3. Hyperledger Fabric network: a blockchain backend platform;
4. Interplanetary file system (IPFS): a peer-to-peer decentralized storage service that stores vast PDF files such as X-rays with the proper security access, which reduces the load on the blockchain and enhances performance [51].

Finally, an evaluation phase determined how well the developed prototype works [52]. It was a twofold evaluation: analytical, to study the fit of the PHR-based blockchain in the technical architecture, and descriptive, featuring detailed scenarios to illustrate the solution's utility [53]. Moreover, the Hyperledger Caliper tool was used to test and evaluate the functionality of the proposed system. Hyperledger Caliper is an open-source performance assessment method that focuses on benchmarking Hyperledger blockchains and was developed by the Linux Foundation [54,55]. The performance evaluation was examined using three metrics:

Transaction throughput: number of successful transactions per second (TPS);
Transaction latency: amount of time for transaction initialization and actual execution (i.e., response time);
Success rate: number of successful transactions overall.

Figure 2 illustrates a summary of the design science framework.

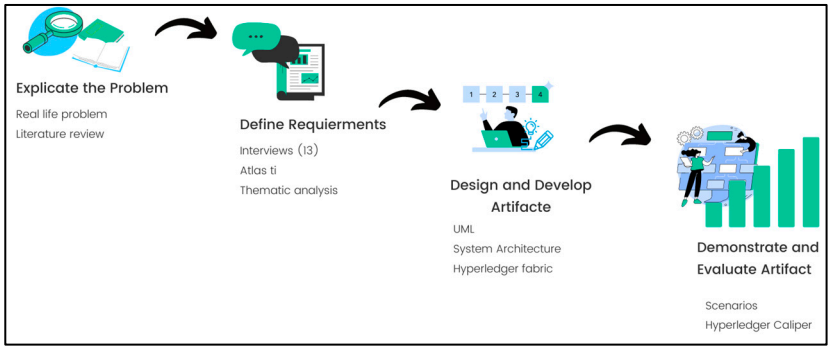

Figure 2. Summary of the design science methodology.

5. Results and Discussion

This section presents the results and discussion of the study. The data collection, analysis, and system design and development were performed according to the study's objectives. Before demonstrating the system's requirements, it is worth identifying the stakeholders of the system to clarify where each requirement falls. The stakeholders were divided into four categories, as shown below:

- Primary stakeholders: patients are the pivotal actors and primary beneficiaries of their records as the owners and data controllers at the first level;
- At the same level, primary stakeholders are also physicians, therapists, and those who provide advice and treatment to the patient in addition to that of pharmacies and laboratories, and who add the results of tests and other processes to a health record;
- Next, secondary stakeholders include insurance organizations who are responsible for medical approvals, relatives authorized by the patient on behalf of their health record, and employees responsible for administrative matters;
- Finally, tertiary stakeholders include government or private agencies, researchers, and medical institutions.

Figure 3 illustrates the stakeholders.

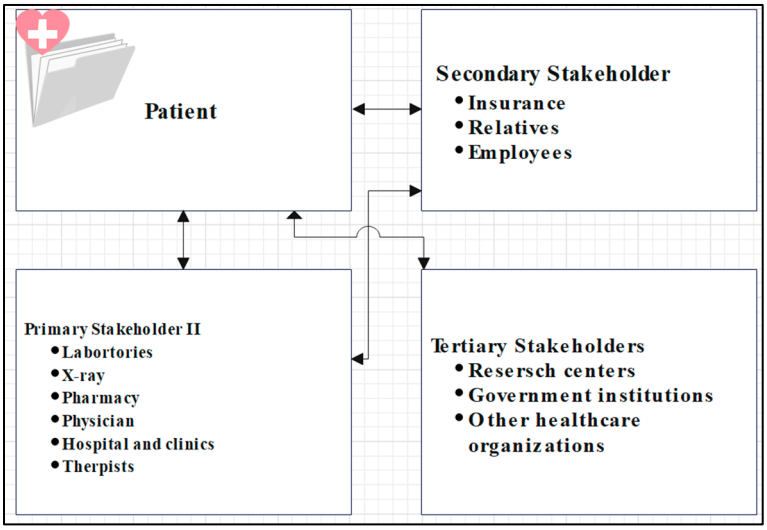

Figure 3. PHR stakeholders, adapted from [41].

The first section illustrates the requirements collected from the academic literature review and the interviews with PHR stakeholders. These requirements are categorized as functional, nonfunctional, and system design requirements.

5.1. Functional Requirements

Functional requirements are essential tasks that the system should accomplish in order to perform tasks. For patient functional requirements, two themes were identified.

5.1.1. Identity Management and Data Ownership

The first theme of functional requirements is identity management and data ownership. It is necessary and critical for patients to own their medical data and to have sufficient information about their health situation and to preserve their privacy [56]. The section below illustrates the codes for this theme.

- Provide access control

To protect a patient's privacy, patients should be the owners of their data and have full access and control based on policies regarding, e.g., those who should have access to their data, such as physicians, researchers, and relatives [1–3,16,21]. Permission must be obtained from the patient when anyone tries to view any section of their record. According to Expert 9, "The patient must provide permission for which type of report the physician must see".

- Share data with researchers and receive incentives

According to a study [16], patients are willing to provide researchers with their data without revealing their identity (i.e., the option to hide); this will contribute to helping researchers obtain medical data more smoothly and quickly without impacting patient privacy. If the patient agrees to provide access to their PHR to researchers or another party, the patient can be incentivized to reveal such data. According to [37], an incentive mechanism is valuable for patients since they can monetize their private data through applications [5,26,34,35].

- Emergency and relatives' access

Emergency access to a patient's record is a critical requirement of PHRs when a patient is unconscious [57]. Even in many of the research solutions presented for patient health records using blockchain, this requirement has been overlooked. The medical staff may require knowledge of the patient's medical history, where quick decisions must be made or documented in the PHR. Patients can grant access to their data by enabling an emergency

physician to access their data for a limited time to assure patient privacy [11,36,57]. Expert 6 stated, "For example, if the patient arrives at Emergency or in a state of unconsciousness . . . I can see the complete history, as this makes a difference in the physician's decision making". Another aspect enables relatives to have access to PHRs; this requirement adds value for patients who cannot manage their records effectively, such as the elderly [41]. According to Expert 7, "The elderly represent a large segment of society because they do not know how to manage their PHR". Expert 12 states, "Nevertheless, this should be for a certain period . . . there should be a method to enable the patient to cancel the authorization of other people and not leave it permanently".

5.1.2. PHR Content

The second theme is the content of the PHR, which means the essential aspects that should be in a patient's record to support their healthcare journey.

- Medical support and appointment reservation

Medical support is another requirement which is necessary to enhance healthcare services; this supports includes communicating with the physician, providing recommendations or raising awareness regarding a patient's condition, health education, chatting with medical support, and sending tips. Moreover, some cases may require immediate contact by the treating physician. According to Expert 1, "Even if the patient needs urgent consult, the physician can open the record and know the patient's situation". This is in addition to the ability to reserve an appointment, reschedule, and view all reports with the option to copy, according to Experts 3, 8, and 9.

- Have all patient details, family history, allergies, and complete medical history

Incomplete health records may lead to mistreatment, putting patients' lives at risk. Knowing the current patient's medical history is critical; for example, it is necessary to know the sensitivity to medicines or foods and to have them with them whenever needed; so, if a patient forgets or goes to another healthcare center, it is documented in the PHR and clear to the physician or expert. Another aspect is having a survey on family disease. According to Expert 1, "When the patient gets a new record, it would be better to answer simple questions about genetic or family diseases, so when the physician opens the record, this information will be visible to him".

5.1.3. PHR and Stakeholders

This theme illustrates common interests among all stakeholders.

- Unified medical standards and regulations

The system should have unique record numbers across all participating healthcare centers that are different from the patient IDs. As Expert 7 illustrates, "There must be a mechanism to give a unified number to each patient, and then we build on this file. This number can be used to direct access to the patient's record, even in emergency situations". This, as a result, will allow a healthcare center to share data and transfer a patient to another healthcare center or physician. According to Expert 12, "If the healthcare center cannot treat the patient, the healthcare center can transfer the patient to another healthcare center participating in the blockchain network, and the patient can permit other physicians to view reports to take additional consultations on their condition".

5.1.4. Healthcare Provider Administration Issues and PHRs

This theme illustrates the healthcare providers' requirements that should be considered from their side when designing PHRs.

- Keep PHR for patient use and have another for healthcare center administrative use

There are several benefits that a PHR provides to a patient; however, a healthcare center needs to access PHRs without obtaining patient approval. According to Expert 1,

"We in the health records department follow the patient's record and make sure all data are entered completely and correctly after they leave . . . for inpatient, we make sure that the test form is passed to the physician to monitor the patient's condition appropriately" This is called a health services foster; so, waiting for a patient to give a healthcare center approval will negatively impact the work on medical records. Moreover, physicians should have the ability to modify PHR reports to correct wrong information for healthcare centers. According to Expert 1, "It does not make sense to get back to the patient and ask him to allow us to make modifications to their records . . . there is an example that happens daily. We raise insurance claims, so we do modifications as insurance agencies requests for more clarification, and we add more details about his condition to know if the insurance approves the claim or rejects [it]. So, the patient pays the costs, and sometimes the insurance does not respond until a patient leaves or is discharged". This should be for administrative tasks, but patients must not be able to edit or delete reports. "The patient should not be able to change some results or add or remove reports. The patient should only be able to block or allow a physician to check his reports".

- The section for physician documentation is not visible to a patient without a release option

The system should have a release option for a physician for sensitive reports. As Expert 4 explains, "There is something we call investigation release and results release, for example, if a woman has a pregnancy test, and the result comes out. The physician has the option to allow the analysis to appear for the patient; this is called results or lab release". In addition, the system should also have a release option for physicians for sensitive reports; as Expert 4 stated, "... another person went to the physician with serious symptoms or for a patient with psychological symptoms indicating that he could commit suicide. The physician here writes these special notes . . . the physician has a choice whether he releases so it is clear to another physician who treats the patient, but it is not visible to the patient".

5.2. System Design Requirements

It is recommended that the system design requirements are in the system so that the patient and physician have more options.

- Location features for health recommendation and notification services

Several features, such as notification and geographical location features, can be added to the system to improve patient healthcare services, for instance, notifications [58] and geographical location features. Expert 4 says, "If a patient has asthma and the weather is dusty, the patient is supposed to know this information. So, the system could send an alert to take a sprayer or change his place, or even if a patient is in a high area, which may cause shortness of breath."

- Accessibility features and the right to be forgotten

Because some patients may not be able to utilize the app properly, a guide should be considered. Patients also suggest improving accessibility, such as for those with visual impairments [11]. Another aspect is when a patient wants to remove their record, as the patient has the right to be forgotten in terms of their data, in compliance with the GDPR [7].

- Two sections for inpatient and outpatient details

According to the conducted interviews, almost all healthcare centers have separate sections for inpatient and outpatient treatment; these sections have different procedures. However, this needs to be conducted correctly for all stakeholders. As Expert 7 explains, "When you open the patient's record, the system should automatically open it to a window like a bifurcation . . . for example, if the patient is in an inpatient clinic, a bed icon appears, and if in an outpatient clinic, it shows another icon, and the visit itself, if I open it, shows me the name of the treating physician with each visit, the medical licenses, even the external medical prescriptions".

5.3. Nonfunctional Requirements

Nonfunctional requirements do not address functionality but refer to system operation specifications and capabilities, i.e., environmental requirements [42].

- Mobility and decentralized storage

Mobile health is a rapidly growing field and an essential requirement in healthcare application domains. As patients become more mobile these days, they desire the same portability for their health records [59,60]. Another requirement is that decentralized storage can facilitate faster access to medical data in a protected manner [61] since there is no single point of failure, and it splits the records storage from a single server into multiple distributed nodes in the network. In addition, the storage of large files, such as X-rays, will impact the network's performance.

- Performance, scalability, and availability

Performance evaluation plays an essential role in the area of blockchain research, in particular PHRs; thus, it is critical to assure usability in practice [62]. New solutions should be assessed in a meaningful way to illustrate their efficiency and effectiveness, as well as the performance benefits and drawbacks of the new release [54]. "The application's performance must be guaranteed for all transactions carried out to be attractive for the user groups" [41]. In addition, the PHR should be consistent and available to deliver timely support and treatment options to the patients [63,64].

- Security and privacy

Currently, security and privacy among healthcare organizations remain challenges [65]. Data leaks and the distribution of patient medical records can have serious consequences, such as risks to patients' privacy through the selling of the data on the black market and malicious attacks that can harm a patient's reputation and finances [60]. Thus, the system should be secure and traceable. In addition, a one-time password is required when the user signs into the system. According to Expert 12, "There must be several layers of security, such as having a fingerprint or face ID; it is feasible to send the OTP, but it will not be like the patient's fingerprint or face... It is required because it may be possible to steal the patient's device and try to log in and get the code". Privacy is also critical, and this requirement is achieved by applying access control through Hyperledger Fabric.

- Interoperability

In healthcare, interoperability generally focuses on data sharing among business organizations [66]. Patient-driven interoperability occurs when a patient's data are made available via specific standards [67]. With this approach, the patients approve the exchange of health data with trusted institutions as supervisors. Thus, the data formats should comply with consistent standards [67–70]. According to Experts 2 and 3, there must be a unification of medical data standards for all healthcare centers. Each healthcare center follows a different school in terms of reading and classifying the data. In addition, nonunified medical data standards lead to the low interoperability of medical information systems among healthcare providers [2].

- User friendliness and efficiency

The system should allow users to complete their tasks efficiently, and it should have a user-friendly graphical interface [71]. Therefore, a user-friendly interface will enhance the usage of the system so that patients can make reservations and physicians can perform their work easily [71]. As Expert 6 illustrates, "The system should be easy to use. Now I waste some time due to the difficulty of navigating between pages; automatic saving and filling fields are essential". Expert 2 says, "It should be efficient and fast. I mean, when data are retrieved, there should not be a hiccup". Table 2 illustrate summery of PHR requirements.

Table 2. Summary of PHR requirements.

No.	Requirement	Reference	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13
		Functional Requirements													
A	Identity Management and Data Ownership														
1.	The system must allow the patient to manage their identity and be the owner of their data.	[1–3,16,24]													
2.	The system should provide access control (accept/reject/deny) for patients regarding their PHR.	[1,2,16,24]									*				
3.	The system should allow patients to approve/deny access to their data for clinical research purposes.	[11]													
4.	The system should allow patients to hide identity and sensitive data.	[11,57]									*				
5.	The system should allow patients to receive incentives if they agree to share data with other parties.	[37,41,56]								*					
6.	The system should provide emergency access to PHRs based on patient preferences.	[11,35]						*							
7.	The system should provide relatives with access.	[41]										*		*	*
B	PHRs and Stakeholders														
8.	The system should allow a physician to transfer a patient to another physician or healthcare center.	-												*	*
9.	The system should have a unified record number across all healthcare centers.		*	*				*							*
10.	The system should be able to share data with another provider.	-				*						*	*		
11.	The system must not allow a patient to edit or delete reports.	-									*				
C	PHR Content														
12.	The system should have a survey of family diseases.	-	*		*										
13.	The system should have all patient details and medical histories.	[41]	*	*	*		*	*	*	*		*	*	*	
14.	The system should allow patients to view all reports and to have the ability to copy them.	-			*					*					*

Table 2. *Cont.*

No.	Requirement	Reference	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13
		Functional Requirements													
15.	The system should have medical support for chatting and tips or contact information for physicians.	–			*	*	*	*		*				*	
16.	The system should have a reservation system for appointments.	-			*						*				
D	Healthcare Provider Administration Issues and PHRs														
17.	The system should have a release option for physicians for sensitive reports.	-				*			*						
18.	The system must allow a healthcare center to modify false information in PHR reports.	-	*							*		*	*		*
19.	The system should have sections for physician documentation that are not visible to the patient.	-		*		*	*	*					*		
20.	The system should keep PHRs for patient use and have another copy for a healthcare center for administrative use.	-	*												
		Nonfunctional Requirements													
1.	The system should support controlling the access of channel information based on the user's identity (data privacy, protection, and confidentiality).	[11,19,27,61,67]									*			*	
2.	The system should be interoperable and scalable among stakeholders.	[60–64,66]													
3.	The system should be usable, allowing users to complete their tasks efficiently.	[54]		*				*							
4.	The system should have the availability of infrastructure services that are core to the blockchain system's operations.	[65]													
5.	The system should provide security and transaction traceability.	[19,52,58]													
6.	The system should have smart contract capabilities to validate transactions, i.e., the execution of decentralized applications.	[19,52,58,59]													

Table 2. *Cont.*

No.	Requirement	Reference	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13
		Nonfunctional Requirements													
7.	The system should provide two-factor authentication or fingerprint authorization.	-			*							*		*	*
8.	The system should support mobility and decentralized data storage.	[51,52,54,58]													
		System Design Requirements													
1.	The system should provide notification services.	[58]													
2.	The system should provide a right-to-be-forgotten feature.	[27]													
3.	The graphical interface of the system should be user friendly.	[71]													
4.	The system should have a location feature for health recommendations.	-													
5.	The system should have two sections for inpatient and outpatient details.	-													

E, refers to expert. *, refers to mentioned requirement by expert.

The stakeholders show a positive view toward PHRs; the first side is health risk avoidance. Duplicated procedures are one of the drawbacks of scattered healthcare systems. One of the repeated procedures is having X-ray and CT scanning, which is more dangerous for patient health. According to Expert 11, "It is not good for the patient to do a CT scan in one or two days; there must be a long time between the first and the latter because the human body bears a certain amount of radiation from the radiology equipment, and another hospital asked for another CT scan, so there would be a danger to the patient that he was doing two rays in one day". Thus, blockchain-based PHRs will maintain patient safety. Moreover, PHRs link with healthcare providers to achieve a unified view of the patient's record. According to Expert 8, "One of the problems of current systems is that the patient's data is scattered on different databases, which makes it difficult for the doctor to access them". However, according to Expert 8, "with the PHR based on a blockchain system, these problems will be solved as all data is in one place while maintaining data security and controlling who has its right of access".

On the other hand, according to Experts 1 and 5, not all PHR aspects can be applied since they conflict with our standards, CBAHI standards, medical institutions, and international health standards. However, some points must be taken into consideration while designing PHRs. As Expert 5 illustrates, "the patient is not authorized to see the entire record, only specific things because this is an international standard; for example, there are genetic diseases that affect 50% of people, we must sit with the patient and tell him that details about the result". To do so, the proposed system considers this aspect by allowing physicians to write private data that are only shown to physicians and that can be added to patient reports later.

Based on the interviews, the stakeholders suggest recommendations before applying to the decision-makers for PHRs. According to Expert 10, "The system must be unified for all hospitals. Not every hospital has its system; a legislative body must manage this implementation instead of wasting budgets on incompatible systems or medical data". Expert 6 adds, "Another recommendation for decision-makers is there must be a legislature

for blockchain applications to illustrate a clear path for its implementation". PHR allows unified sources across several medical facilities after obtaining the patient's permission [3].

5.4. Design of the Proposed System

This section illustrates the proposed solution's high-level architecture, followed by a general system implementation scenario and detailed low-level scenarios.

5.4.1. The High-Level Architecture of the Proposed System

The section below illustrates the high-level architecture and implementation details of Hyperledger Fabric as a solution.

The Logical Structure of Hyperledger Fabric

1. Presentation layer: the patient can access their PHR from a mobile app or web browser and interact with a Fabric blockchain network through a system development kit (SDK).
2. Data access layer: the SDK provides a simple application programming interface (API) that encapsulates all access to the ledger by allowing an application to interact with Fabric. The system provides a security layer so that the system's members can access their related documents and information based on their role.
3. Logic layer: this layer represents the functions of the chaincode for different members, which are healthcare centers, patients, physicians, etc. In addition, CouchDB and the ledger store the healthcare center's information and the transaction history on the Hyperledger Fabric blockchain to maintain immutability and security. Each member can request access to the PHR, but they cannot view the record unless the patient grants them access.
4. Data storage layer: the system solution contains data that are off-chain and data that are on-chain to maintain security and efficiency simultaneously; these are:
    - Off-chain: this stores a user's basic information through the health provider, including their mobile numbers, email addresses, and hashed passwords, in a regular secure database to provide them with the ability to delete and remove their accounts from the system at any time;
    - Interplanetary file system (IPFS): a peer-to-peer decentralized storage service that stores vast PDF files such as X-rays with the proper security access, which will reduce the load on the blockchain and enhance performance [51].

Figure 4 illustrates the logical layers.

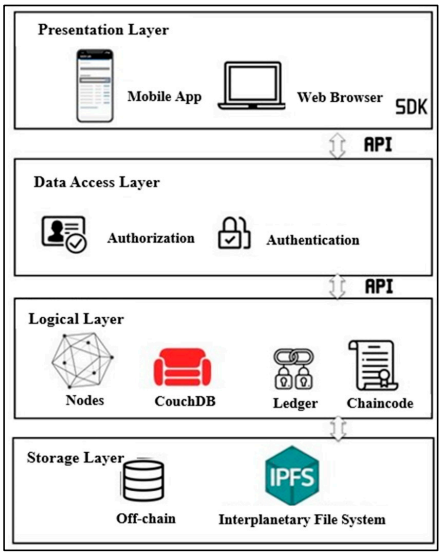

Figure 4. Logical layers of the solution.

System Implementation Details

The Hyperledger Fabric framework provides fine-grained access control. At the beginning of a consortium network, there could be two or more healthcare center and network members, who are patients, physicians, researchers, etc. Each member has specific reading, creating, updating, and deleting permissions. All stakeholders (healthcare centers, patients, physicians, insurance, researchers, etc.) need to be identified by the network administrator or the so-called authority management through a membership service provider (MSP). The MSP governs the identities of all nodes in the system (clients, peers, and OSNs) and is responsible for issuing node credentials for authentication and authorization with the help of a Fabric certificate authority (Fabric CA). The MSP manages identities and permissioned access for network participants and allows an identity to be trusted and recognized by the rest of the network. Once all the members are authorized, they can access the system securely and privately. Authorized users can access the system through the Hyperledger Fabric software version 2.2 development kit (SDK), which allows applications to interact with a Fabric blockchain network. The SDK provides a simple application programming interface (API) that encapsulates all access to the ledger by enabling an application to interact with Fabric, verifying identities, communicating with chaincode queries, or receiving ledger updates. Once the authorized users log in, they submit a proposal containing the identity to the endorser nodes; the endorser cryptographically signs a message, called an endorsement, and sends it back to the client in a proposal response. The client collects endorsements based on the endorsement policy of the chaincode and passes it to the OSN to order them into groups of blocks with cryptographic signatures of the ordering peers and broadcasts these blocks to the committing peers as a final validation step before changes are made to the ledger. Once this is finished, the block will be written into the ledger. Figure 5 illustrates the system's implementation.

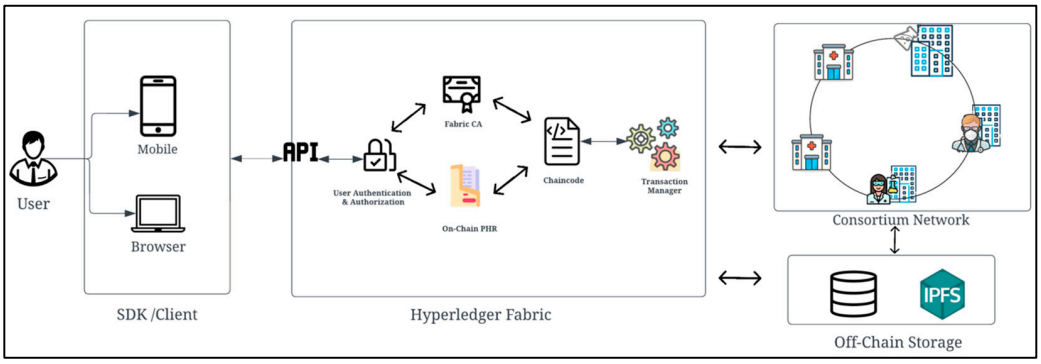

Figure 5. System implementation process.

5.4.2. Implementation and Configuration

The system's implementation, configuration, and development are illustrated in the following sections.

Environment Setup

After all the pre-requested development tools are installed, the system will start a test network with the following:

- One orderer;
- Four organizations with one peer per organization;
- One CouchDB instance per peer;
- CA server for the peers and orderer;
- One chaincode per organization.

The Hyperledger Fabric framework was installed and configured on the Ubuntu operating system. Figure 6 shows the installation of the Hyperledger, and Figure 7 shows the installed Docker containers. Docker containers simplify the running and deployment of

Hyperledger Fabric's different tools. After the installation process, the network and consensus protocol configurations are followed by channel creation, as shown in Figure 8. The third part is the Hyperledger Fabric system's SDK, as explained in the high- and low-level architectures and scenarios. This part deals with the execution of the chaincode through which the transactions of the PHR system are operated and then stored in the ledger.

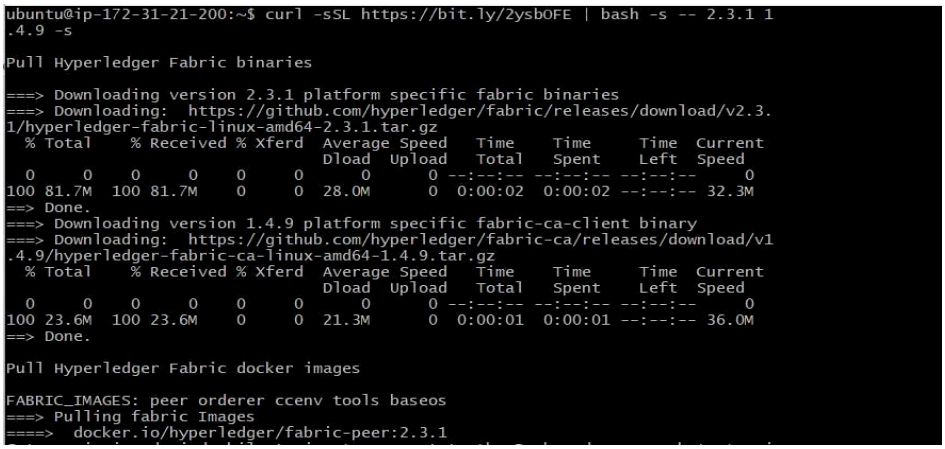

Figure 6. Hyperledger Fabric binaries.

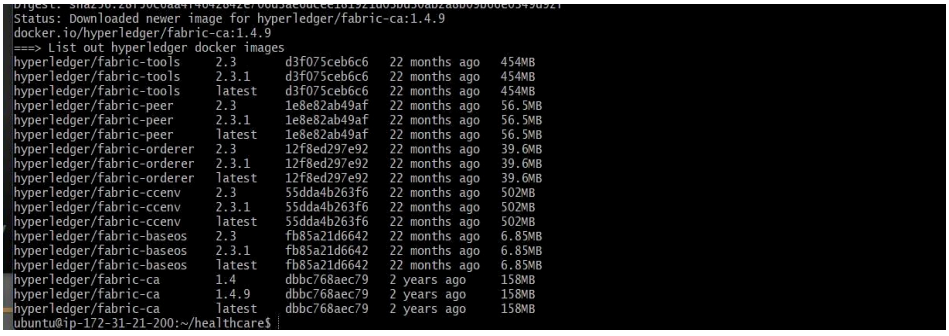

Figure 7. List of installed Hyperledger Fabric tools in Docker containers.

Figure 8. Chaincode deployment in channel and policy.

Implementation Overview

The PHR system was developed for mobile applications to ensure that it can be with patients who are on the go. For decentralization, our scheme stores medical data using CouchDB rather than a semi-honest and curious cloud server; this further protects the privacy of the medical data. In addition, the IPFS allocates a unique hash for each file.

PHR

As mentioned earlier, a vital requirement of the blockchain-based PHR is the provision of different levels of control to different types of users, which means that participants can be restricted to reading, creating, updating, and/or deleting rights. With the different

permissions and roles, the number of users accessing the patients' data is significantly reduced, reducing the risk of a data breach [30]. The healthcare center is authorized to add physicians and patients to the system. The network administrator has full permission over the network, i.e., is allowed to add organizations and view all participants. They also manage researchers, check their identity, and approve them. Figure 9 illustrates the administrator page to approve or add a researcher.

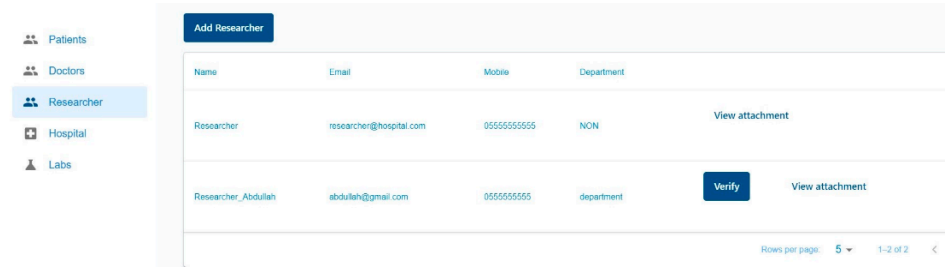

Figure 9. Administrator page.

Figure 10 illustrates a PHR profile, which includes a patient's details, wallet, and the option for whether they would like to appear to researchers for the sharing of their data. Another requirement is access control; Figure 11 shows the access control, where patients can approve or deny access to PHRs. In addition, there is a place for appointment reservations where patients can reserve appointments with a physician, a laboratory, etc. As shown in Figure 12. Relatives' access is restricted to a specific period of time, and the patient's relatives need to approve the request, which is shown in the profile, as illustrated in Figure 13. Once approved, the relatives will appear in the patient profile. For emergency access, the patient will appear in the emergency section. Patients determine whether physicians can access basic information, allergies, or full details, as shown in Figure 14. Moreover, access to the patient's profile is restricted according to an amount of time that is determined by the patient, as shown in Figure 15.

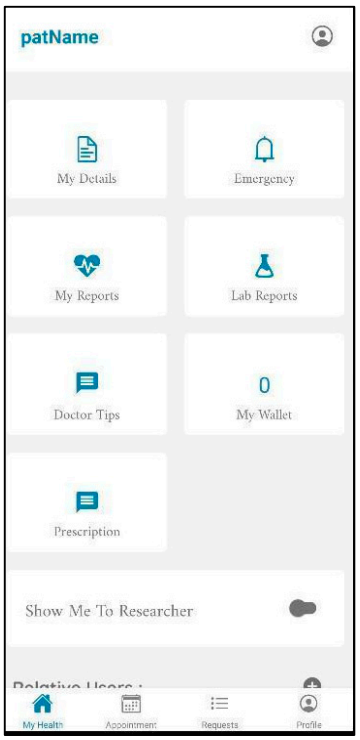

Figure 10. Patient profile.

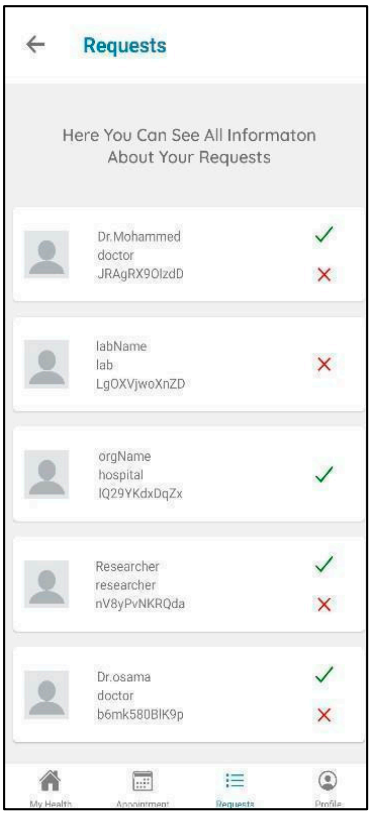

Figure 11. Access control.

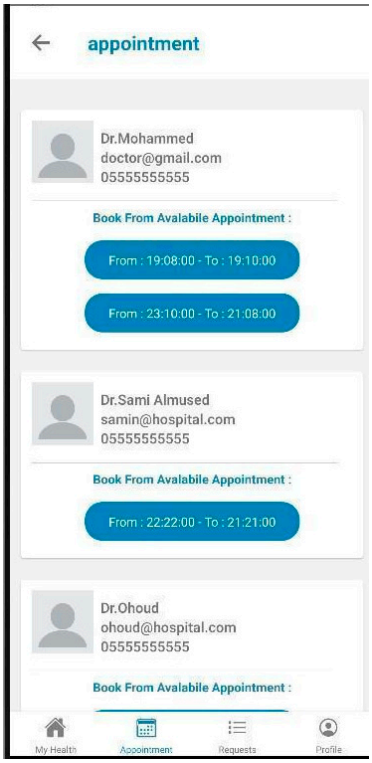

Figure 12. Appointment reservation.

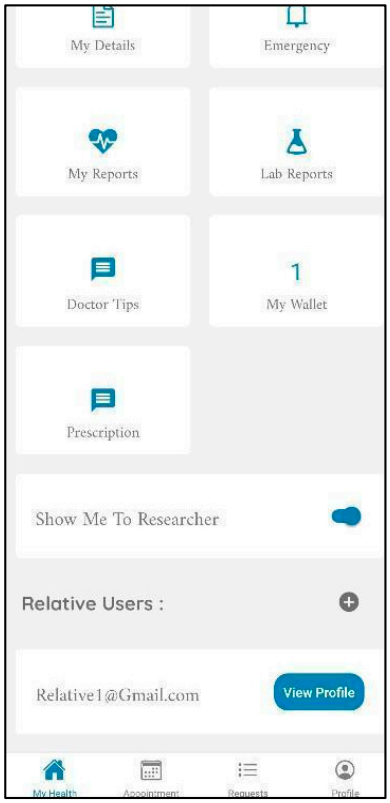

Figure 13. Relatives' Access.

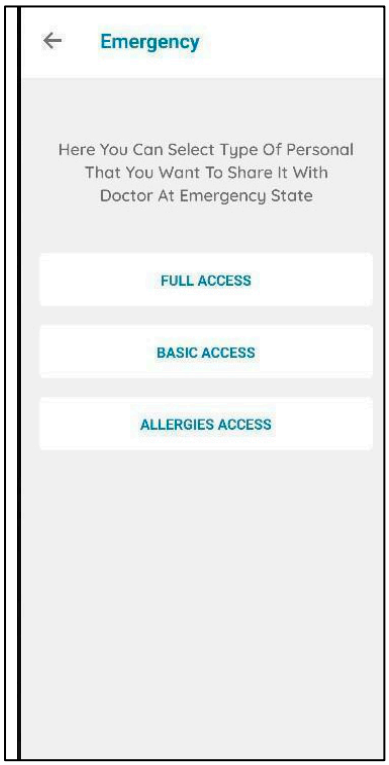

Figure 14. Emergency access.

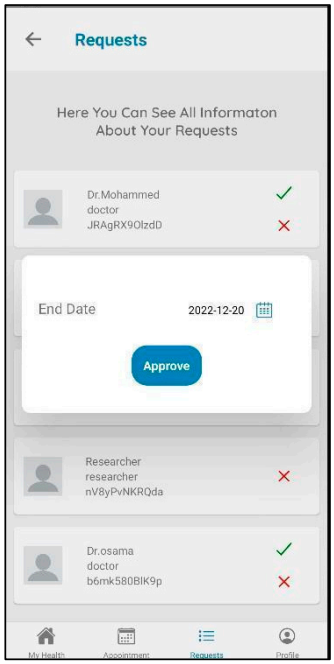

Figure 15. Time restriction.

Researchers

After a researcher is verified and approved by the administrator, the researcher requests access to a PHR after a patient decides to show their data via selecting the option to share their data in their profile. Moreover, patients have the choice to hide or reveal their identity, and they can accept a request to access their data with the ability to hide their identity, as shown in Figure 16 Once a patient agrees to a researcher's request, the researcher will pay the patient using a normal credit card or cryptocurrency, as shown in Figure 17. Once the payment is made, the researcher can download the file, and the patient receives compensation.

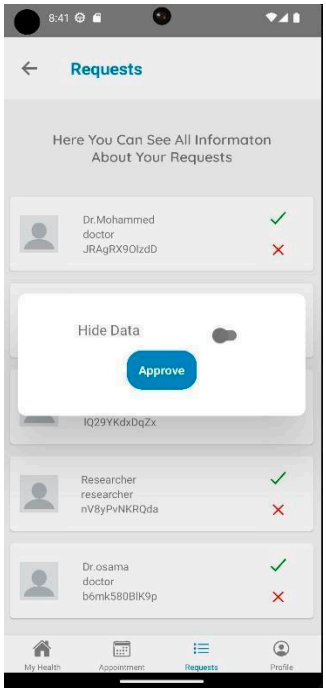

Figure 16. Hide data.

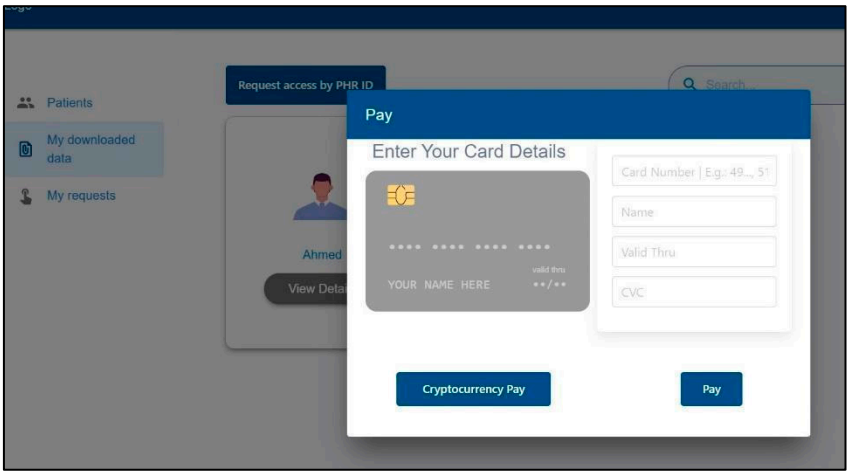

Figure 17. Researcher payment.

Physician

Once a patient arrives at a clinic, a physician will request that the patient provide them with access to their PHR. At this moment, the patient will have the option to accept or reject the access request, as well as to determine the time limit. Once it is accepted, the physician can review the PHR, write a report, add observations, and write tips, as shown in Figures 18 and 19.

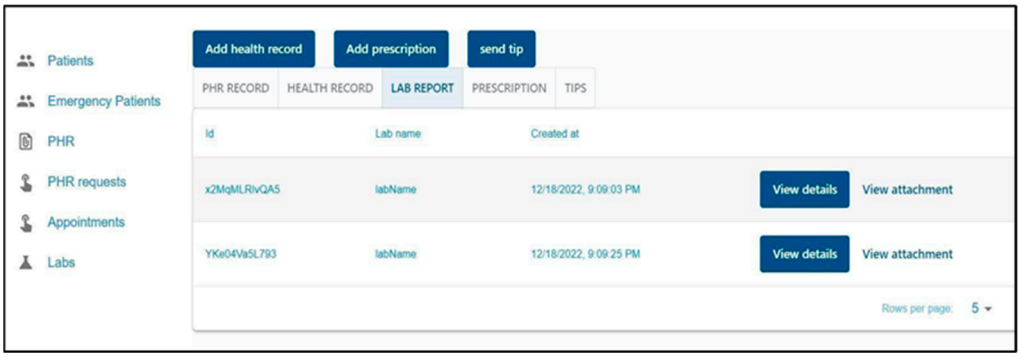

Figure 18. Physician page.

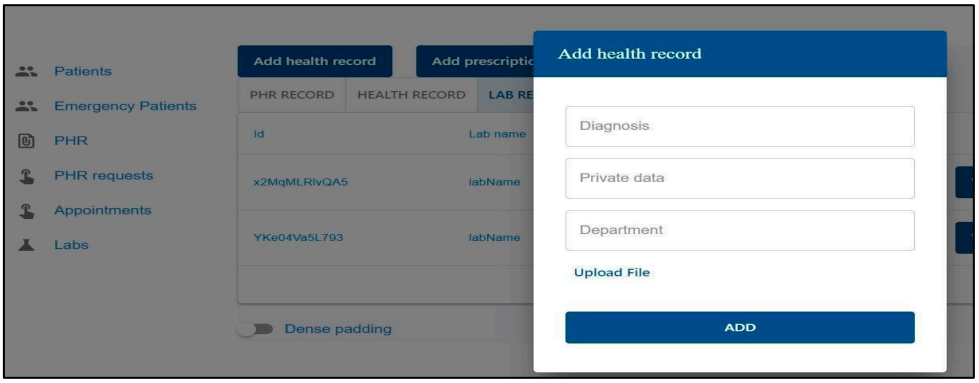

Figure 19. Physician enters data.

6. System Evaluation

The proposed system was evaluated; the evaluation was conducted with Amazon Web Services (AWS) EC2 (2.2xlarge) on a computer with an e core CPU, 32 GB RAM, running Ubuntu 22.04 LTS using the Hyperledger Caliper tool version 0.3.2. The performance

metrics test was threefold: transaction throughput, latency, and send rate. The success rate and throughput were measured in TPS and the latency in seconds. The test benchmark was to execute a chaincode to query access to a PHR. The system was tested in five test rounds submitted at fixed rates of 100, 200,300,400, and 500. There are two types of transactions specified by Caliper: query and open transactions [72]. Query transactions perform a simple read from the state CouchDB, while open transactions perform one read and one write operation per transaction. The result of the evaluation was successful, with a 100% success rate and 0 fails.

Figure 20 presents a summary of the system's latency. The average latencies were 0.02 s for all rounds. This resulted in an overall average latency of 0.01 s, a maximum overall latency of 0.03, and a minimum overall latency of 0.01 s. Thus, the amount of time for the transaction initialization and actual execution was less than 1 s, which is a good latency metric.

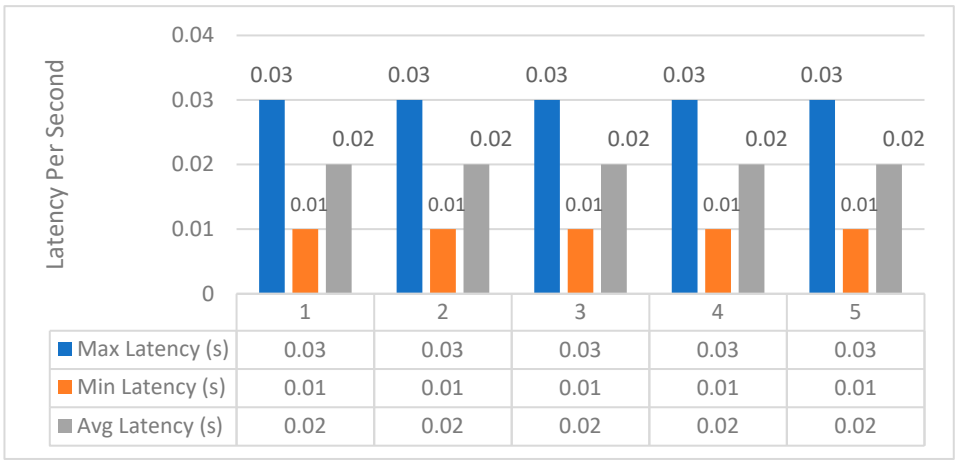

Figure 20. Summary of the query latency.

Figure 21 presents a summary of the system throughput. As mentioned earlier, five rounds were run from 100 to 500 transactions. The overall number of successful TPS was approximately the same for each round, and it slightly decreased as more transactions were sent. The overall average throughput was 262.56 per second.

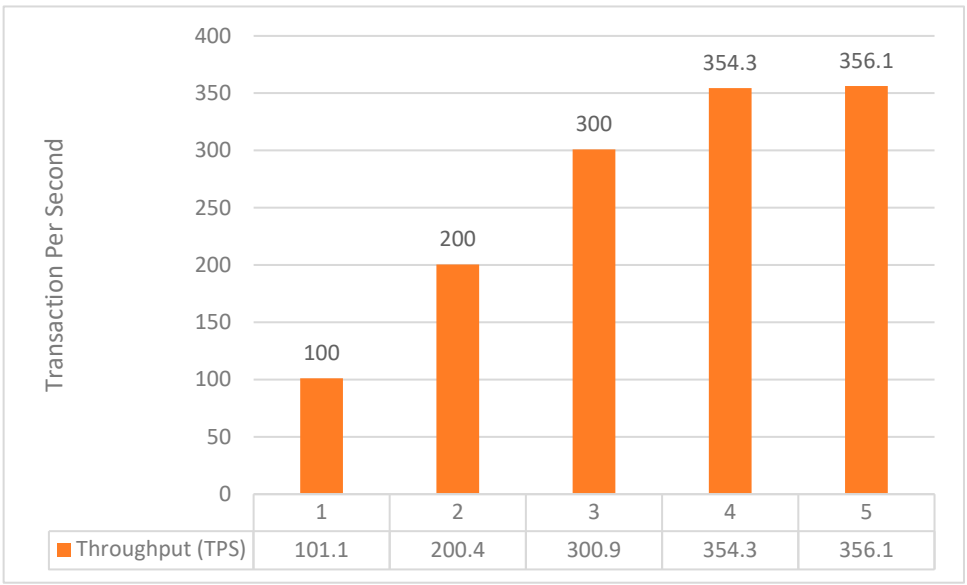

Figure 21. Summary of the query throughput.

Figure 22 presents a summary of the open latency. The average latencies were 0.74 s for round 1; 1.56 for round 2; and 2.21, 3.01, and 3.43 for rounds 3, 4, and 5, respectively. This resulted in an overall average latency of 2.19 s, a maximum overall latency of 4.082, and a minimum overall latency of 0.832 s. Figure 23 illustrates a summary of the open throughput. It can be seen that the throughput on the open function was lower than on the query function. The throughputs on all rounds were almost equal for all rounds at approximately 36 TPS. It can be seen that both the throughput and the latency increase with the increasing number of synchronized transactions. Moreover, this also indicates that the system reached its maximum ability to handle and queue the remaining transactions for the following processing [72]. Overall, the constant stability of the throughput indicates Hyperledger's reliability and availability [73].

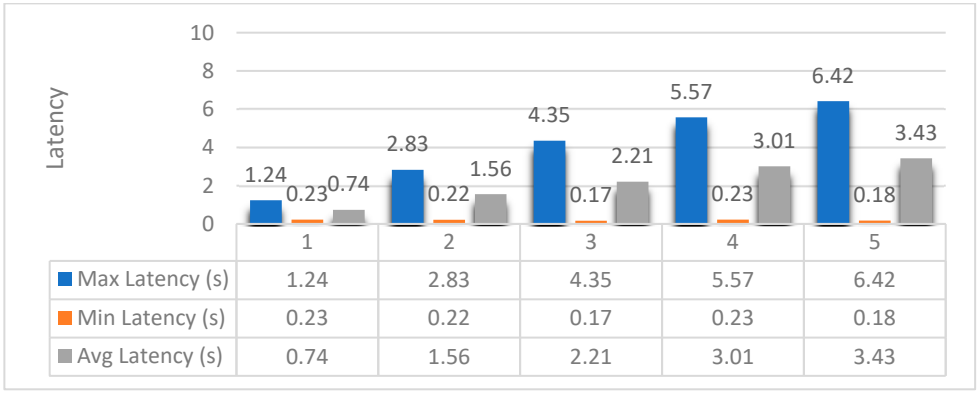

Figure 22. Summary of the open latency.

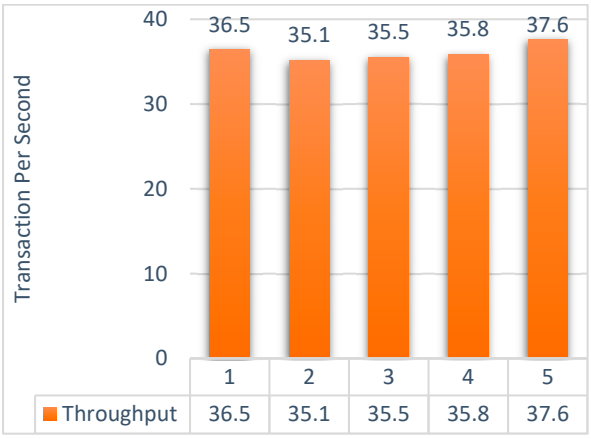

Figure 23. Summary of the open throughput.

In summary, all the transactions were successful, with a 100% success rate. It is important to note that the hardware configuration, blockchain network design, consensus algorithms, complexity, and operation of the chaincode affect the throughput, latency, and send rate of a blockchain-based system's performance [74]. Thus, these findings could vary depending on the test environment [54], as shown below in the comparison.

6.1. Comparison with an Empirical Study

This section compares the performance of this study to that of the study in [73]; the performances were similar, using the same benchmarks with the same number of rounds; however, they had different configurations and a different number of organizations. Table 3 illustrates the differences. Only the same number of rounds and transactions were considered.

Table 3. Performance environment and specifications.

Performance Environment and Specifications		
No.	This Study	Khan et al. (2022) [73]
Configuration	AWS EC2 (2.2 × large) with an 8 core CPU, 32 GB RAM, and running Ubuntu 22.04 LTS	Intel Xeon®, 2.6 GHz with a 12 core CPU, 16 GB RAM, 500 GB disk space, and running Ubuntu 18.04 LTS
Algorithm	RAFT	RAFT
Originations	4 Organizations	2 Organizations
Peers	1 Peer each	1 Peer each

6.2. Latency

The first comparison benchmark was latency. Figure 24 illustrates the query transactions, where the blue bars represent Kahn et al.'s study, and the orange bars represent this study. The latency of the query transaction was less than one millisecond for all rounds. In contrast, in the other study, the first round was only 1 s less, and it increased as the transactions increased, with approximately 1 s for each round.

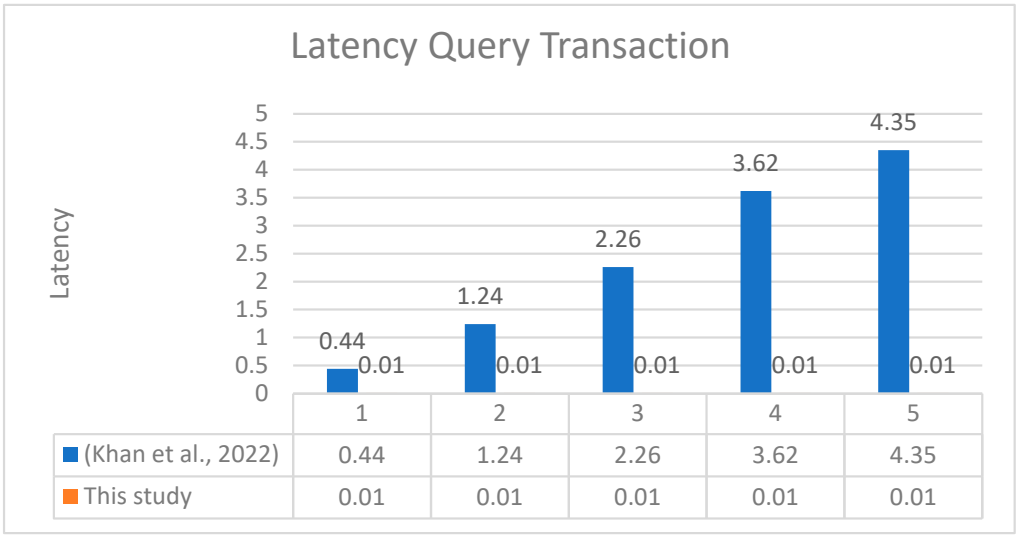

Figure 24. Latency query transactions [73].

On the other hand, Figure 25 illustrates the open transactions. Our study demonstrated less than 1 s in the first round, and this slightly increased by less than a second as long as the transactions increased, reaching 3.43 in the fifth round. In Kahn et al.'s study, the first two rounds demonstrated more than 2.50 s, and this increased until reaching 7.78 in the fifth round. In summary, our study's overall open and query latency transactions were lower than those of Khan et al.'s study for all rounds.

6.3. Throughput

First, for the open throughput, it was noticed that both this study and Khan et al.'s study showed a decrease in the transactions per second in all rounds. Our study excelled over Khan et al.'s study, with slight differences in the TPS in the first three rounds and at two seconds in the fourth round and fifth round. The overall TPS for our study was between approximately 35 and 37 TPS, while for Khan et al.'s study it was between 31 and 32 TPS. Figure 26 illustrates a summary of the open throughput.

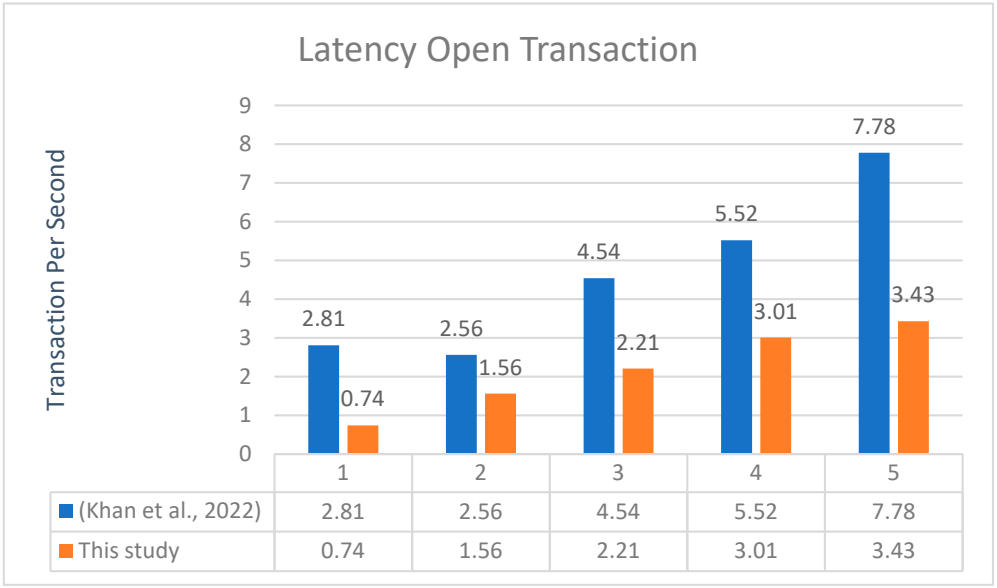

Figure 25. Latency open transactions [73].

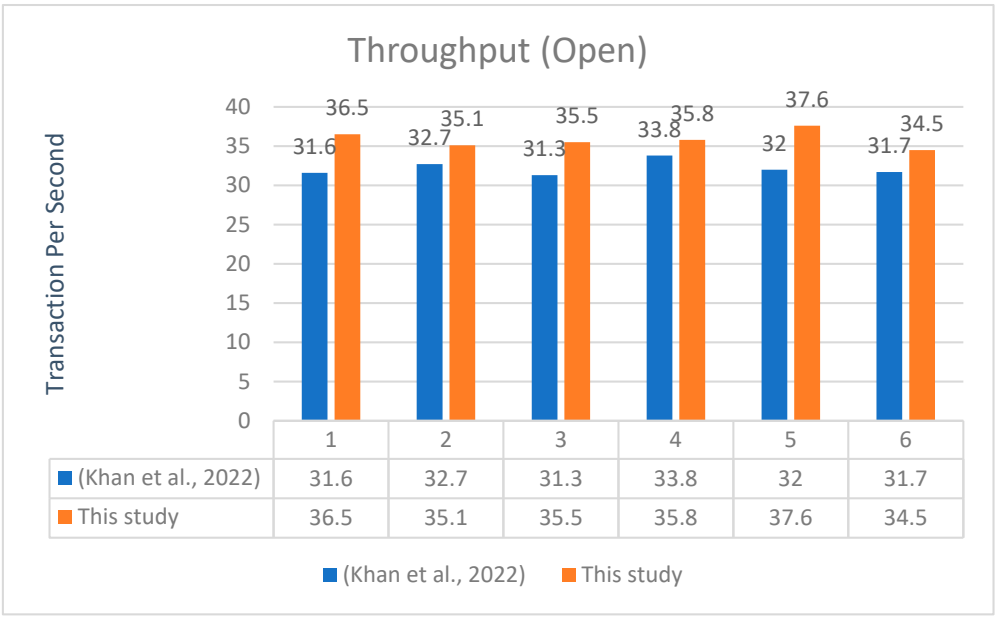

Figure 26. Summary of the open throughput [73].

For the query throughput, the results show a large difference between this thesis and Khan et al.'s study. It was approximately higher for the open transactions; however, in this study, the throughput of the query transactions was higher than almost all transactions sent if the first three rounds had no delay, and it decreased in the fourth and fifth rounds with 354.3 TPS and 356.1, respectively. Figure 27 illustrates a summary of the query throughput.

Table 4 illustrates an overview of the different performances (i.e., throughput and latency) under various evaluation environments and systems [73,75]. The comparison consisted of 1000 transactions, utilizing Hyperledger Caliper and Hyperledger Fabric, and considered the query and open transaction functions.

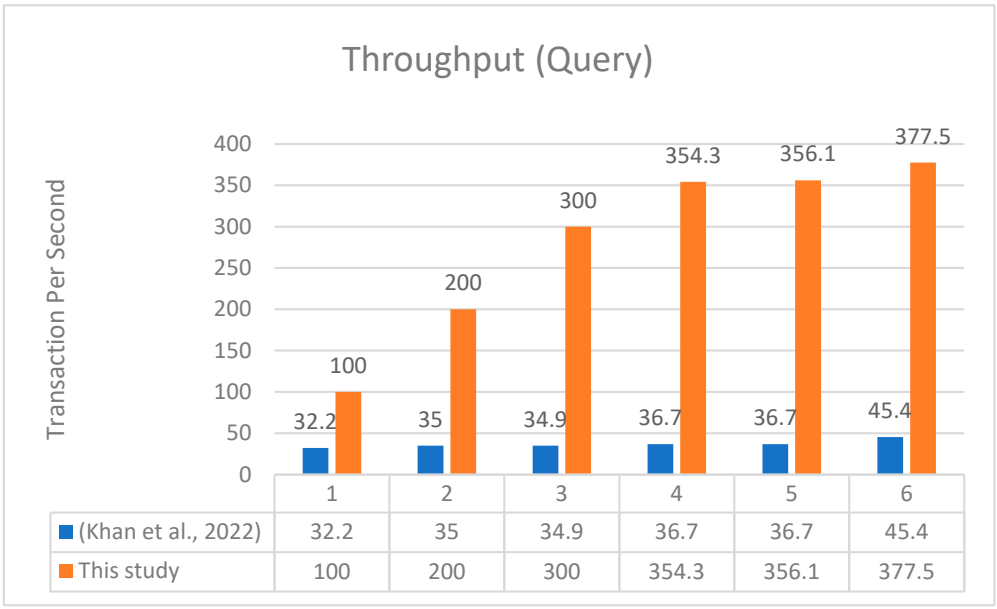

Figure 27. Summary of the query throughput [73].

Table 4. Overview of the performances of the different studies.

Author	Fabric Version	Latency		Throughput		Test Environment
		Query	Open	Query	Open	
Nasir et al. (2018) [75]	Fabric 0.6	5.18	5.18	19.26	155	HPC server in Hertz, Xeon® CPU E5-2690, 2.60 GHz, 24 core CPU, 64 GB RAM, and running Ubuntu 16.04 LTS
	Fabric 1.0	1.37	5.18	461	185	
Khan et al. (2022) [73]	Fabric 2.2	6.74	19.66	45.4	31.7	Intel® Xeon®, 2.6 GHz with 12 core CPU, 16 GB RAM, 500 GB disk space, and running Ubuntu 18.04 LTS
This study	Fabric 2.2	0.01	7.86	377.5	34.5	AWS EC2 (2.2 × large), 8 core CPU, 32 GB RAM, and running Ubuntu 22.04 LTS

6.4. Limitations

As this research focused on PHRs, some requirements were discarded since they were related to the differences between PHRs and EHRs, as elaborated in Section 1, which were as follows:

Functional requirements:

- Management of invoices and payments;
- Unified medical data standards and regulations;
- Sharing data with another health provider;
- Keeping PHRs for patient use and having another copy for healthcare centers' administrative use.

System design requirements:

- Accessibility features;
- Location features for health recommendations;
- Two sections for inpatient and outpatient details.

Additionally, system interoperability is required for EHRs for sharing information; however, since we used a consortium blockchain, we were not sharing data among stakeholders; they requested to access patient data to view details.

7. Conclusions

As the current centralized systems are not designed to facilitate the effective management of patients' data across various institutions, this results in the loss of easy access to

their records, incomplete medical histories, and the disclosure of data without their knowledge via internal fraud, breaches caused by cyberattacks, and other forms of unauthorized access. This study proposed a solution for patient identity management, data ownership, and access control by applying a Hyperledger Fabric framework, which is a blockchain-based distributed ledger. Stakeholders in the industry were engaged to understand the real needs and to identify the requirements for PHRs. In addition to the requirements identified in previous studies, this research investigated fifteen new requirements that had not been found in the previous studies. Next, we designed and developed a prototype based on the collected requirements to elaborate the solution's utility by illustrating the high- and low-level architectures of the implementation process based on defined requirements with scenarios and demonstrations of the providing of patients with the power to own and benefit from their data, which was achieved after we applied DS and Hyperledger Fabric to access control over identity for peers and users, authentication, and verification. The proposed system was tested using Hyperledger Caliper. The results showed a 100% success rate in functionality when testing the gaining of access to a PHR. Moreover, the system received a 100% transaction success rate. Among the interviews, it was discovered that there was a lack of awareness of blockchain and its potential in the current healthcare industry in Saudi Arabia. There was also misinterpretation of some aspects of PHRs and EHRs, resulting in confusion between them, as illustrated in Section 6.4 (Limitations). Our proposed system could be a first step for healthcare providers who intend to adopt this technology based on a private blockchain and to utilize our framework, which considers highly sensitive data and focuses more on applications that put the patient at the center.

A part of this research was presented and published at the 5th International Conference on Future Networks and Distributed Systems [13]. Our contributions were twofold: major and minor, as listed below:

7.1. Major Contributions

1. Proposed a solution for personal health records based on blockchain to give patients the power to own and benefit from their data;
2. Introduced Hyperledger Fabric to achieve access control and govern identity for peers and users, user authentication, credential validation, signature generation, and verification;
3. Designed and developed a working prototype based on the defined requirements;
4. Engaged stakeholders from the industry to understand the real needs and to identify the requirements for PHRs;
5. Evaluated the functionality of the system's performance using the Hyperledger Caliper tool.

7.2. Minor Contributions

Introduced a mechanism to allow patients to be incentivized to share their data with researchers, facilitated researchers in accessing patient data in a more straightforward manner, and connected patients with researchers directly.

Author Contributions: O.A.: data curation, writing—original draft preparation, visualization, validation, and investigation; W.R.: methodology, visualization, writing—review and editing, and supervision; W.J.O.: methodology, visualization, writing—review and editing, and supervision. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University for funding and supporting this work through the Graduate Student Research Support Program.

Institutional Review Board Statement: Nor applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Acknowledgments: The researchers would like to thank all stakeholders for their cooperation as this research would not be complete without their input.

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

References

1. Hau, Y.S.; Lee, J.M.; Park, J.; Chang, M.C. Attitudes toward blockchain technology in managing medical information: Survey study. *J. Med. Internet Res.* **2019**, *21*, e15870. [CrossRef]
2. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* **2018**, *43*, 5. [CrossRef] [PubMed]
3. Li, C.; Dong, M.; Li, J.; Xu, G.; Chen, X.; Ota, K. Healthchain: Secure EMRs Management and Trading in Distributed Healthcare Service System. *IEEE Internet Things J.* **2020**, *8*, 7192–7202. [CrossRef]
4. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2021**, *34*, 11475–11490. [CrossRef]
5. Arndt, R.Z. How Third Parties Harvest Health Data from Providers, Payers and Pharmacies. Modern Healthcare. 2018. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=129027739&site=ehost-live&scope=site (accessed on 1 October 2020).
6. Office of the Federal Register. *Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 110*; U.S. Government Printing Office: Washington, DC, USA, 1996; pp. 1936–2103.
7. Viorescu, R. 2018 Reform of Eu Data Protection Rules. *Eur. J. Law Public Adm.* **2017**, *4*, 27–39. [CrossRef]
8. Argaw, S.T.; Bempong, N.E.; Eshaya-Chauvin, B.; Flahault, A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Med. Inform. Decis. Mak.* **2019**, *19*, 10. [CrossRef] [PubMed]
9. Lee, K.; Lim, K.; Jung, S.Y.; Ji, H.; Hong, K.; Hwang, H.; Lee, H.-Y. Perspectives of patients, health care professionals, and developers toward blockchain-based health information exchange: Qualitative study. *J. Med. Internet Res.* **2020**, *22*, e18582. [CrossRef]
10. Chukwu, E.; Garg, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* **2020**, *8*, 21196–21214. [CrossRef]
11. Meier, P.; Beinke, J.H.; Fitte, C.; Brinke, J.S.T.; Teuteberg, F. Generating design knowledge for blockchain-based access control to personal health records. *Inf. Syst. E-Bus. Manag.* **2021**, *19*, 13–41. [CrossRef]
12. Gimenez-Aguilar, M.; de Fuentes, J.M.; Gonzalez-Manzano, L.; Arroyo, D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Gener. Comput. Syst.* **2021**, *124*, 91–118. [CrossRef]
13. Aldamaeen, O.; Rashideh, W.; Alalawi, S.; Obidallah, W. Personal health records: Blockchain-based identity management and data ownership. In Proceedings of the 5th International Conference on Future Networks & Distributed Systems, Dubai, United Arab Emirates, 15–16 December 2021; pp. 87–92. [CrossRef]
14. Zhu, Q.; Loke, S.W.; Trujillo-rasua, R.; Jiang, F.; Xiang, Y.; Trujillo-Rasua, R. 20 Applications of Distributed Ledger Technologies to the Internet of Things: A Survey. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
15. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: www.bitcoin.org (accessed on 29 January 2022).
16. Despotou, G.; Evans, J.; Nash, W.; Eavis, A.; Robbins, T.; Arvanitis, T.N. Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study. *Digit. Health* **2020**, *6*, 2055207620924949. [CrossRef] [PubMed]
17. Thwin, T.T.; Vasupongayya, S. Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *Secur. Commun. Netw.* **2019**, *2019*, 8315614. [CrossRef]
18. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
19. Daraghmi, E.Y.; Daraghmi, Y.A.; Yuan, S.M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]
20. Kuo, T.T.; Rojas, H.Z.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478. [CrossRef]
21. Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain technology the identity management and authentication service disruptor: A survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735–1745. [CrossRef]
22. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the 13th EuroSys Conference, Porto, Portugal, 23–26 April 2018; Volume 2018. [CrossRef]
23. IBM. What is Hyperledger Fabric? IBM. 2021. Available online: https://www.ibm.com/topics/hyperledger (accessed on 30 September 2022).
24. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.P.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [CrossRef]

25. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [CrossRef]
26. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. eHealthChain—A blockchain-based personal health information management system. *Ann. Telecommun. Telecommun.* **2021**, *77*, 33–45. [CrossRef]
27. Balistri, E.; Casellato, F.; Giannelli, C.; Stefanelli, C. BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express* **2021**, *7*, 308–315. [CrossRef]
28. Tang, X.; Guo, C.; Choo, K.-K.R.; Liu, Y.; Li, L. A secure and trustworthy medical record sharing scheme based on searchable encryption and blockchain. *Comput. Netw.* **2021**, *200*, 108540. [CrossRef]
29. Uddin, M.; Memon, M.S.; Memon, I.; Ali, I.; Memon, J.; Abdelhaq, M.; Alsaqour, R. Hyperledger fabric blockchain: Secure and efficient solution for electronic health records. *Comput. Mater. Contin.* **2021**, *68*, 2377–2397. [CrossRef]
30. Antwi, M.; Adnane, A.; Ahmad, F.; Hussain, R.; Rehman, M.H.U.; Kerrache, C.A. The case of HyperLedger Fabric as a blockchain solution for healthcare applications. *Blockchain Res. Appl.* **2021**, *2*, 100012. [CrossRef]
31. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. *J. Med. Internet Res.* **2020**, *22*, e13598. [CrossRef] [PubMed]
32. Albahli, S.; Khan, R.U.; Qamar, A.M. A blockchain-based architecture for smart healthcare system: A case study of Saudi Arabia. *Adv. Sci. Technol. Eng. Syst.* **2020**, *5*, 40–47. [CrossRef]
33. Toshniwal, B.; Podili; Reddy, R.J.; Kataoka, K. PACEX: PAtient-Centric EMR eXchange in Healthcare Systems using Blockchain. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; Volume 2019, pp. 954–960. [CrossRef]
34. Leeming, G.; Cunningham, J.; Ainsworth, J. A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. *Front. Med.* **2019**, *6*, 171. [CrossRef]
35. Rajput, A.R.; Li, Q.; Ahvanooey, M.T. A blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthcare* **2021**, *9*, 206. [CrossRef]
36. Shuaib, K.; Abdella, J.; Sallabi, F.; Serhani, M.A. Secure decentralized electronic health records sharing system based on blockchains. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *34*, 5045–5058. [CrossRef]
37. Stafford, T.F.; Treiblmaier, H. Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1340–1362. [CrossRef]
38. Gan, C.; Saini, A.; Zhu, Q.; Xiang, Y.; Zhang, Z. Blockchain-based access control scheme with incentive mechanism for eHealth systems: Patient as supervisor. *Multimed. Tools Appl.* **2021**, *80*, 30605–30621. [CrossRef]
39. Yakubu, A.M.; Chen, Y.P.P. A blockchain-based application for genomic access and variant discovery using smart contracts and homomorphic encryption. *Futur. Gener. Comput. Syst.* **2022**, *137*, 234–247. [CrossRef]
40. Faber, B.; Michelet, G.C.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A Blockchain-based Personal Data and Identity Management System. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019; Volume 6, pp. 6855–6864. [CrossRef]
41. Beinke, J.H.; Fitte, C.; Teuteberg, F. Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study. *J. Med. Internet Res.* **2019**, *21*, e13585. [CrossRef]
42. Johannesson, P.; Perjons, E. *An Introduction to Design Science*; Springer: Cham, Switzerland, 2014; pp. 1–197. [CrossRef]
43. Hevner, A.; Chatterjee, S. *Design Research in Information Systems*; Springer: Boston, MA, USA, 2010; Volume 22.
44. Venable, J.R.; Pries-Heje, J.; Baskerville, R.L.; Venable, J.R.; Pries-Heje, J.; Baskerville, R. Choosing a Design Science Research Methodology. *ACIS 2017 Proc.* **2017**, *2*, 112. Available online: https://aisel.aisnet.org/acis2017/112 (accessed on 31 August 2022).
45. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A design science research methodology for information systems research. *J. Manag. Inf. Syst.* **2014**, *24*, 45–77. [CrossRef]
46. Barbour, R.S. Checklists for improving rigour in qualitative research: A case of the tail wagging the dog? *BMJ* **2001**, *322*, 1115–1117. [CrossRef]
47. Palinkas, L.A.; Horwitz, S.M.; Green, C.A.; Wisdom, J.P.; Duan, N.; Hoagwood, K. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Adm. Policy Ment. Health Ment. Health Serv. Res.* **2013**, *42*, 533–544. [CrossRef]
48. Wiltfang, G.L.; Berg, B.L. Qualitative Research Methods for the Social Sciences. *Teach. Sociol.* **1990**, *18*, 563. [CrossRef]
49. Bauer, J. Význam průkazu RAS mutací pro anti-EGFR protilátky v léčbě 1. linie metastazujícího kolorektálního karcinomu. *Onkology* **2013**, *7*, 260–261.
50. ATLAS.ti | The Qualitative Data Analysis & Research Software—ATLAS.ti. Available online: https://atlasti.com/ (accessed on 20 August 2022).
51. Benet, J. IPFS—Content Addressed, Versioned, P2P File System. *arXiv* **2014**, arXiv:1407.3561.
52. Hevner, A.; Chatterjee, S. Design Science Research Frameworks. In *Design Research in Information Systems*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 23–31. [CrossRef]
53. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q. Manag. Inf. Syst.* **2004**, *28*, 75–105. [CrossRef]

54. Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access* **2020**, *8*, 126927–126950. [CrossRef]
55. Hyperledger Caliper. Caliper. Hyprtledger. 2018. Available online: https://www.hyperledger.org/blog/2018/03/19/measuring-blockchain-performance-with-hyperledger-caliper (accessed on 12 June 2021).
56. Fatokun, T.; Nag, A.; Sharma, S. Towards a blockchain assisted patient owned system for electronic health records. *Electronics* **2021**, *10*, 580. [CrossRef]
57. Rajput, A.R.; Li, Q.; Ahvanooey, M.T.; Masood, I. EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. *IEEE Access* **2019**, *7*, 84304–84317. [CrossRef]
58. Hongwei, L.; Xinhui, W.; Sanyang, L. A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data. *Optim. Methods Softw.* **2016**, *19*, 125–136.
59. Sinha, S.R.; Park, Y. Dealing with Security, Privacy, Access Control, and Compliance. In *Building an Effective IoT Ecosystem for Your Business*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 155–176. [CrossRef]
60. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
61. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
62. Thwin, T.T.; Vasupongayya, S. Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation. *Int. J. Netw. Distrib. Comput.* **2020**, *8*, 139–151. [CrossRef]
63. Dodevski, Z.; Filiposka, S.; Mishev, A.; Trajkovik, V. Real time availability and consistency of health-related information across multiple stakeholders: A blockchain based approach. *Comput. Sci. Inf. Syst.* **2021**, *18*, 927–955. [CrossRef]
64. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
65. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]
66. Rahurkar, S.; Vest, J.R.; Menachemi, N. Despite The Spread of Health Information Exchange, There Is Little Evidence of Its Impact on Cost, Use, and Quality of Care. *Health Aff.* **2015**, *34*, 477–483. [CrossRef]
67. Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef] [PubMed]
68. 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]
69. George, M.; Chacko, A.M. MediTrans—Patient-centric interoperability through blockchain. *Int. J. Netw. Manag.* **2021**, *32*, e2187. [CrossRef]
70. Tandon, A.; Dhir, A.; Islam, N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
71. 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]
72. Kuzlu, M.; Pipattanasomporn, M.; Gurses, L.; Rahman, S. Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 536–540. [CrossRef]
73. Khan, D.; Jung, L.T.; Hashmani, M.A.; Cheong, M.K. Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises. *Sensors* **2022**, *22*, 915. [CrossRef]
74. Pajooh, H.H.; Rashid, M.A.; Alam, F.; Demidenko, S. Experimental Performance Analysis of a Scalable Distributed Hyperledger Fabric for a Large-Scale IoT Testbed. *Sensors* **2022**, *22*, 4868. [CrossRef] [PubMed]
75. Nasir, Q.; Qasse, I.A.; Talib, M.A.; Nassif, A.B. Performance analysis of hyperledger fabric platforms. *Secur. Commun. Netw.* **2018**, *2018*. [CrossRef]