systems

MDPI

Article

Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric †

Álvaro Díaz * and Héctor Kaschel

Electrical Engineering Department, Faculty of Engineering, University of Santiago of Chile (USACH), Av. Víctor Jara Nº 3519, Estación Central, Región Metropolitana, Santiago 9170124, Chile; hector.kaschel@usach.cl

* Correspondence: alvaro.diaz.m@usach.cl; Tel.: +569-91237030

† This paper is an extended version of our paper published in Diaz, A.; Kaschel, H. Scalable Management Architecture for Electronic Health Records Based on Blockchain. In Proceedings of the 2022 IEEE International Conference on Automation/XXV Congress of the Chilean Association of Automatic Control (ICA-ACCA), Curicó, Chile, 24–28 October 2022; pp. 1–7.

Abstract: Communication and information technologies have accelerated the implementation of electronic medical records, but at the same time, have put patient privacy, information security and health data at risk. An alternative to address the problem of security and privacy of medical data is the use of blockchain. Scalability has become one of the biggest challenges facing the development of blockchain-based electronic health records (EHRs). The purpose of this article is to implement and test a scalable blockchain-based EHR management system. For this reason, we present a scalable blockchain-based EHR management architecture. In this paper, we propose an EHR management model based on entities and user roles, adapt, and then implement with Hyperledger Fabric in a two-channel configuration. We develop a prototype in Fabric using a one-and two-channel configuration. We then designed and conducted an experiment to verify the performance of the proposed scheme in terms of scalability improvement. This scalable blockchain-based EHR management solution, such as the Hyperledger Fabric platform, offers a viable alternative to address scalability issues, as well as to protect patient's privacy and the security of their medical data.

Keywords: blockchain; chaincode; electronic healthcare records (EHRs); Hyperledger Fabric; scalability

Citation: Díaz, Á.; Kaschel, H. Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. *Systems* **2023**, *11*, 346. https://doi.org/10.3390/systems11070346

Academic Editor: Paolo Visconti

Received: 12 April 2023
Revised: 18 June 2023
Accepted: 30 June 2023
Published: 6 July 2023

1. Introduction

Electronic health records (EHR) are a health information system used to store, manage, and share clinical data about patients. These systems have been an important part of the healthcare landscape for many years and have seen tremendous growth in recent years. This is largely due to the digitization of healthcare systems, which has increased the need to collect and share large amounts of data. EHRs have been used to improve the quality of patient care by enabling healthcare providers to access important clinical information at the right time [1–3]. Electronic health records (EHRs), in addition to contributing to the management of data for medical diagnosis and treatment, also offer several advantages to the world of medical research. These include [4]:

- Easier to collect and analyze clinical data on a large scale. EHRs generally store a large amount of clinical data, which facilitates data collection for large research studies.
- Increased data accessibility. EHRs make data more accessible, making data collection easier for researchers.
- Increased data accuracy. EHRs store accurate and consistent clinical information, which improves data quality for analysis.

However, public disclosure of such sensitive personal data poses serious threats to the privacy and security of patients and healthcare providers. Hence, we foresee the need for new technologies to address the privacy and security issues of personal data

in healthcare applications. Blockchain is one of the most promising solutions, as it provides transparency, security, and privacy through decentralized, consensus-based data management on distributed peer-to-peer computing systems [5,6].

Blockchain is a database technology that allows storing information reliably and securely using a combination of distributed consensus procedures with cryptographic techniques. The concept used in the blockchain is the distributed ledger, which represents an ordered and consistent chain of financial transactions distributed across multiple nodes in an untrusted peer-to-peer network [7,8].

The most relevant key elements of blockchain technology related to security and privacy are [9–11]:

- Cryptography: Cryptography is fundamental in blockchain to ensure data security. Robust cryptographic algorithms are used to protect the integrity of information and ensure the confidentiality of transactions.
- Distributed consensus: Blockchain systems are based on distributed consensus, which means that all parties in the network must agree on the validity of transactions. This prevents data manipulation and malicious attacks. Among the most commonly used methods are PoW (proof of work), PoS (proof of stake) and BFT (Byzantine Fault Tolerance).
- Identification and authentication: Identification and authentication of blockchain network participants are essential to maintain security and privacy. Mechanisms, such as cryptographic keys and digital signatures, ensure transaction authenticity and data integrity.
- Decentralized network: One of the key features of blockchain is its decentralized nature. In a decentralized network, information is stored on multiple nodes, making it difficult to manipulate or gain unauthorized access to data.
- Selective privacy: Although blockchain is inherently transparent due to its public record structure, selective privacy techniques can be implemented to protect certain sensitive data. This is achieved through the use of techniques, such as encryption of sensitive data or the use of smart contracts that control access to information.
- Auditing and transparency: Auditing is an important property of the blockchain. When a transaction is made, the current block records the transaction with a timestamp. It records a history of all transactions. Then a system participant tracks the actions of previous events. This feature is beneficial for individuals or medical organizations that need to obtain tamper-proof account records [12].

Blockchain is a technology that offers many advantages for ensuring patient privacy in electronic health records (EHRs) [1,13]. These include:

- Enhanced data security. The blockchain offers enhanced security by storing clinical data in a distributed network that cannot be manipulated by third parties.
- Increased transparency. The blockchain allows users to monitor the use of their data, which helps ensure that data is not misused.
- Increased privacy. The blockchain allows users to control who can access their data. This can help prevent data abuse and data breaches.

Blockchain has advantages with sensitive data, such as electronic health records. With blockchain, data transactions are cryptographically secured and verified, making it nearly impossible to alter or manipulate data without detection. The decentralized nature of blockchain ensures that there is no single point of failure, which reduces the risk of data breaches and cyberattacks. That said, scalability is an important issue and is what this paper addresses.

Within the main areas of blockchain application in healthcare systems, we can distinguish healthcare information management, supply chain management (widespread in the pharmaceutical industry), biomedical research and education, remote patient monitoring (collection of biomedical information using a mobile device or body area sensors) and healthcare data analysis [9,13].

Blockchain-based EHR systems present scalability challenges due to the distributed nature of the blockchain. This means that many nodes are needed to process and validate each transaction, which in turn limits the number of transactions per second (TPS) that can be processed [7]. This means that it is difficult to meet the demand for the use of electronic health record (EHR) systems as data networks grow.

To address this problem, blockchain developers have been working to improve consensus processes so that they can process more transactions per second. This includes techniques such as using alternative consensus algorithms, implementing auxiliary channels to speed up transactions, and using compression techniques to reduce the size of the blockchain.

In our first paper on the topic, "Scalable Management Architecture for Electronic Health Records Based on Blockchain" [3], we proposed and described a blockchain-based electronic health records management model with scalability features. The proposed model was analyzed and compared with other EHR management architectures based on decentralized systems.

The studies presented in [9,10,14] indicate that the Ethereum blockchain and Hyperledger Fabric are the most widely used in the integration of EHR in decentralized systems. Although the Ethereum blockchain is widely used for the operation of smart contracts, since 2021, due to the rise of DeFi (Decentralized Finance), its cryptocurrency has presented a significant increase in its monetary value. This increase in value has significantly affected network speed, costs, and transaction performance [15]. There are other blockchains, such as Polygon, Cardano, or Binance Smart Chain, whose transaction costs and latencies are considerably lower. However, we chose to use blockchains that are not associated with crypto assets because, in the long run, transaction costs and speed are affected [3]. On the other hand, Hyperledger Fabric is a permission-based blockchain that uses a modular architecture and provides high levels of confidentiality, robustness, scalability, and adaptability. In permission-based blockchains, the nodes are known, identified, and cryptographically authenticated, and the number of transaction-validating nodes is allocated in a way that allows for minimizing the processing time of the consensus mechanism [16,17]. While there are several other permissioned blockchain platforms, such as Corda, Ripple, and Ethereum Enterprise, we selected Hyperledger Fabric to implement the proposed model due to its modular architecture, flexibility, and support backed by a large developer community.

The objective of this work is to implement and test a scalable EHR management system based on Hyperledger Fabric private blockchain. We address the issue of blockchain scalability in EHR by proposing a multi-channel-based scheme. For this purpose, we establish a base test blockchain deployed on Hyperledger Fabric. We compare the performance of the network composed of one channel and the enhanced network version composed of two channels with the same number of organizations and peers. We perform the performance tests with Hyperledger Caliper.

The main contributions of this paper include the following:

1. We present the implementation of the blockchain-enabled healthcare framework and the design of the prototype deployed in the context of real roles for network members.
2. We provide novel aspects of the working methodology.
3. We present a performance analysis of the healthcare prototype deployed in a test system.

The remainder of this paper is structured as follows: Section 2 presents the methods used in the article, Section 3 summarizes the review of related work on EHR or medical record document implementation via blockchain, and Section 4 presents the proposed architecture of the EHR management system using Hyperledger Fabric blockchain. Section 5 describes the implementation of the test system for performance measurement using Hyperledger Caliper, then in Section 6, the test result and performance of the proposed System are analyzed. Finally, Section 7 presents the conclusions and future work for this proposal.

2. Methods

In this section, we describe the methodology for the development of this work, which is divided into four stages:

- In the first part, we conceptualize the blockchain-based EHR management model. At this stage, we describe the conceptual model of the entity-based EHR management system, which we developed with scalability features.
- We performed the adaptation of the model to the Hyperledger Fabric blockchain platform. In this part, we adapt the features of the proposed model to the elements that make up the Hyperledger Fabric blockchain platform.
- We implemented test prototypes. In this item, we generate two test prototypes: the first one built with a traditional Hyperledger Fabric blockchain architecture and the second one built with the scalability elements of the proposed model.
- Finally, we present the performance testing stage of the proposed model. At this point, we perform two testing frameworks using the Hyperledger Caliper tool: the first one we apply to the traditional prototype and the second one we apply to the prototype with the scalability elements of the proposed model. We then compare and analyze the performance results.

In the analysis, we also include the comparison of our proposed model with others existing in the literature. The methodology is summarized in the schematic in Figure 1.

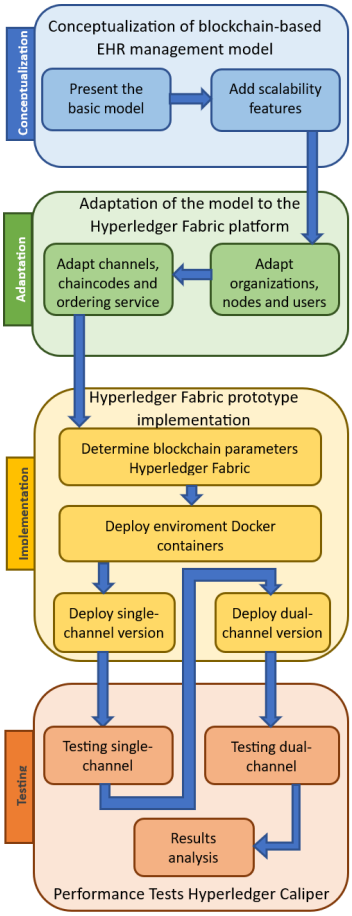

Figure 1. Summary diagram of the methodology of this paper.

3. Related Work

Several proposals for electronic health records implemented on blockchain using different blockchain architectures, approaches and networks have been published in recent

years. Below, we present a review of some of these proposals that relate most closely to our proposed scheme.

In work developed by Pradhan, N.R. et al. [8] present a prototype EHR based on a Hyperledger Fabric 2.0 blockchain platform with the RAFT consensus method. The study demonstrated that the system is able to successfully compare the performance of Hyperledger Fabric RAFT, Kafka and Ethereum blockchain platforms. In addition, the prototype offers a multi-host configuration. Patient information is also stored outside the blockchain. For testing, a complete prototype is used relying on docker swarm for the multi-host network configuration, and benchmarking is deployed under Hyperledger Caliper. The most satisfactory performances are obtained with the RAFT consensus method.

The proposed work by Wadud et al. [18] presents a remote patient monitoring scheme under a BSN (Body Area Sensor Network) architecture. The working model of the blockchain is implemented under the concept of Patient Centered Agent (PCA), which provides a secure data flow for the patient. The private blockchain used is Hyperledger Fabric implements a hybrid consensus method that combines Proof of Integrity (PoI) and Proof of Validity (PoV) to protect the privacy and integrity of data when retrieved from a blockchain-based cloud database. The platform also uses a storage manager that combines a public and a private storage system of records. The scheme is performance tested for access and retrieval of data stored on the network.

Fernandes et al. in [19] propose an EHR management architecture that is formed by four interconnected components: the clients, the blockchain, a storage platform and Certification Authorities (CA) based on Hyperledger Fabric. The architecture includes a multi-chain scheme and is analyzed according to three scenarios of interaction between the patient and a healthcare facility. The analysis results support that the multi-chain format performs better for EHR sharing and is more scalable.

Abunadi, I. and Kumar, R.L. [20] propose a blockchain security framework (BSF) to ensure efficient and secure electronic health record (EHR) retention. This framework provides a competent and secure means for physicians, patients, and insurance agents to access medical information while protecting patient data. The objective of this paper is to examine how the proposed framework meets the security needs of physicians, patients, and third parties, as well as resolving security and confidentiality issues in the healthcare sector. Experimental results demonstrate that BSF-EHR achieves secure data sharing among users.

In their work, Cernian, A. et al. [21] present the proposal of a system called PatientDataChain, designed, implemented, and experimentally validated using blockchain technology. This innovative data exchange and sharing solution is secure, flexible and reliable, taking advantage of an enabling context for its creation. With this approach, enhanced data confidentiality and privacy are ensured while providing secure access to patient's medical records.

The MedBloc platform, presented by Huang, J. et al. [22], suggests a secure EHR system based on blockchain technology, which allows patients and healthcare professionals to access and share medical records easily, securely and privately. In the context of the New Zealand healthcare system. To protect the privacy of patients and their health information. The platform is evaluated, and the results indicate that the use of a permissioned blockchain as a Hyperledger Fabric significantly improves network latency and throughput. These features make the proposed system more efficient and scalable.

In this research, Ndzimakhwe, M. et al. [23] discuss the opportunities for Hyperledger Fabric (HLF) in the healthcare industry, addressing the knowledge base gap by developing personalization approaches that enable ease and efficiency of EHR adoption for the healthcare environment. The focus is on prioritizing users by exploring methods of using blockchain technology. The results identify that Hyperledger Fabric, an open-source project, can be used to build a novel method of EHR storage, providing a customizable proof-of-concept network to meet the needs of various projects, including medical record storage. After reviewing a significant group of available blockchain types, it is concluded that Hyperledger Fabric meets the needs of healthcare systems, offering a distributed and secure environment.

Mukherji, A. and Ganguli, N. [24] present a framework that combines IPFS (Interplanetary File System) off-chain storage technology with the security, speed, and low cost of Hyperledger Fabric. This framework enables the authentication of important documents, such as medical records, diagnoses, scans, and prescriptions via blockchain with permissions, while mass data storage is performed on the IPFS platform. The results were benchmarked against the Ethereum blockchain and demonstrated higher performance in terms of latency, storage capacity and transaction costs. These factors also contribute to the scalability of the system.

The works presented in [5,25] analyze and propose a blockchain-based Hyperledger Fabric architecture for different EHR systems. The proposed EHR blockchain system is based on the creation of a ledger network by Peer nodes from various organizations. To ensure privacy and security of communication between the different stakeholders in the network, specific channels are created. The identification and registration of patients and other stakeholders are performed through unique digital certificates issued by Fabric Architecture's membership service provider (MSP). The business logic is handled by different chaincodes that execute EHR transactions in the network. The promising advantages of private blockchain technologies in matters of security, regulatory compliance, compatibility, flexibility, and scalability are demonstrated by experimental results.

Randolph, J. et al. [26] presents a proposed blockchain technology-based platform to address the current limitation in the context of teleradiology, specifically in the exchange of medical images and automatic notification of critical results. This platform uses blockchain technology to provide a secure and trusted environment for the exchange of sensitive medical information and to ensure patient privacy and confidentiality. The proposed platform is expected to improve workflow efficiency by eliminating the need for intermediaries and benefit patients by eliminating the need to store medical images in hard copies.

The aspects of improved quality of service, increased data privacy and security, and low blockchain implementation costs are the issues addressed in [27,28]. Being that in [27], secure EHR management is based on the Hyperledger blockchain, unlike in [28], the authors propose a hybrid approach of offloading and sharing data for healthcare by using edge cloud and Ethereum network blockchain.

In [29], Atreyapurapu et al. describes key technical aspects of deploying a Hyperledger Fabric blockchain in the EHR context. The test network works with two organizations and one peer each.

In [30], Singh et al. propose a patient-centric design of a decentralized blockchain-based EHR management system using javascript-based smart contracts. Experiment results with benchmarking using Hyperledger Caliper evidence significant improvement in throughput and latency.

In [31], Mahore et al. presents a modular entity-based EHR management model under the Hyperledger Fabric blockchain. The design focuses mainly on data security and access control, and privacy preservation.

The studies presented in [14,32] perform a comprehensive analysis of the implementation of blockchain in EHR, aspects such as the level of decentralization, privacy preservation, security, interoperability, and scalability are examined.

While there are many articles on blockchain study and implementation for EHR, there are few proposals that address the issue of scalability of these systems in the healthcare context. For this reason, we believe that the proposed Hyperledger Fabric blockchain with the use of multichannel contributes to the improvement of scalability in her, which is supported by experimental results. Table 1 summarize the related work.

In our article, we plant the following main research questions:

(1) How can a scalable blockchain-based EHR management model be obtained?
(2) Does the dual-channel architecture allow for improved scalability of a blockchain Hyperledger Fabric for the implementation of an EHR management system?

Table 1. Related work on blockchain-based approaches for the EHR system.

Reference	Year	Approach	Features	Limitation
Pradhan et al. [8]	2022	RAFT ordering services with on-chain and off-chain storing scheme	Transaction traffic analysis and performance optimization using HL Caliper.	Fault tolerance, scalability
Wadud et al. [18]	2020	Patient Centered Agent (PCA)	Remote monitoring, good latency performance and de-centralization	Data storage, interoperability
Fernandes et al. [19]	2020	Multi-chain EHR storage management	Multi-channel architecture	Storage hardware, scalability
Abunadi et al. [20]	2021	Blockchain Security Framework (BSF)	Low latency and decentralization	Scalability
Cernian et al. [21]	2020	PatientDataChain Modex Blockchain Database	Interoperability, standards compliance, user interface.	Blockchain proprietary database
Huang et al. [22]	2022	MedBloc	Security, interoperability, and reliability	Latency and scalability
Ndzimakhwe et al. [23]	2023	Patient-centered EHR management.	Interoperability, user interface	Scalability
Mukherji et al. [24]	2020	Linked storage with IPFS	Higher performance in terms of latency, storage capacity and transaction costs	Processing capacity
Uddin et al. [25]	2021	Secure and Efficient Solution for Electronic Health Records	Analysis implementation Hyperledger Fabric arquitecture for EHR	Scalability, data standarization, adoption, costs of operating.
Randolph, J. et al. [26]	2022	Blockchain-based medical image sharing and automated critical-results notification platform	Image management model improves efficiency and safety	Autentification, security
Sammeta et al. [27]	2022	Hyperledger blockchain enabled secure medical data management with deep learning (HBESDM-DLD) model	High security data manager	Implementation limitations
Nguyen et al. [28]	2021	Data Offloading and Sharing for Smart Healthcare with Blockchain	Reduced time latency, energy consumption, and better memory usage	Scalability, costs of operating
Atreyapurapu et al. [29]	2022	Hyperledger Fabric with Docker containers	Methodology for implementing a hyperledger Fabric network	No consensus method specified
Singh et al. [30]	2021	Patient-centric, novel design, Hyperledger Fabric	Reduced time latency, throughput	Consensus method, scalability
Mahore et al. [31]	2019	Secure and Privacy Focused EHR management, hyperledger fabric framework	Data security and access control, privacy preservation	Latency and scalability

4. Proposed Architecture

4.1. Conceptual Scheme of the Model

In this article, we propose an EHR management scheme focused on entities with organizational or institutional roles. Each organization interacts in a decentralized data system that is the blockchain. Network users generate transactions, share and store data, and can read or modify it according to permissions granted within a set of rules that operates within the decentralized network. For these rules to be put into practice, the blockchain needs to have smart contracts. Each user must belong to one or more of these organizations and can have more than one user role within the same institution.

The way this model is proposed allows users not to interact directly on the network but within a framework that allows them to manage and provide security and privacy in the use of their data. This scheme also allows the management of authorization certificates for the granting of public and private keys.

The entities are characterized by type, but each of them has its own identity within the network. For example, a hospital-type entity can be determined to have certain attributes and characteristics. Then, for a given hospital to be integrated into the network, it must be clearly identified through an identifier code that will differentiate it from other hospitals. Each organization also has specific types of users with people roles. Users enrolled in the institution interact directly with the EHRs. The administrative system determines the access permissions to the EHR according to the institution to which the user belongs and

the roles he/she has within the institution. The proposed model has the flexibility to create new organizations or institutions that adapt or adjust to the reality of the region where the system is applied. Figure 2 shows an outline of the proposed architecture.

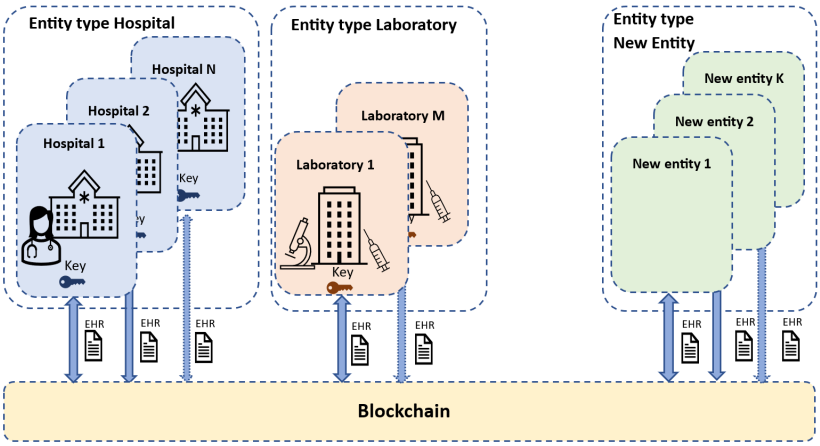

Figure 2. Conceptual scheme of the proposed management model.

As organizations are added, network performance is clearly affected. An organization, such as a hospital or healthcare facility, for example, brings many users to the network. Our proposal addresses the scalability issues by implementing the use of sub-chains within the blockchain structure. These sub-chains would integrate some participating organizations of the network, which manage medical data more efficiently and privately. An example of the sub-chain concept is shown in Figure 3.

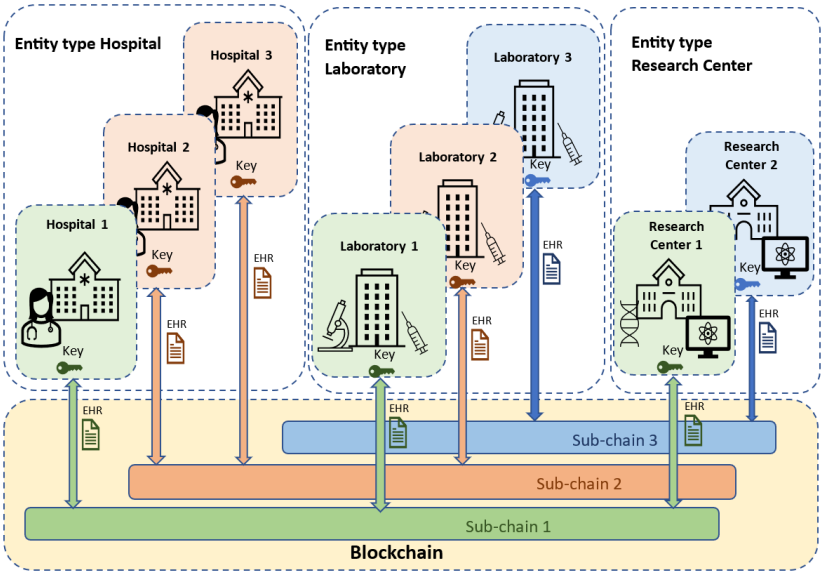

Figure 3. Example scheme of the concept of sub-chains for the proposed model.

4.2. Blockchain Hyperledger Fabric

Hyperledger Fabric is an open-source blockchain platform designed for enterprise use. It is developed to enable users to create scalable and secure blockchain applications. This platform uses introduces a novel architecture and determines where transactions are processed by executing smart contracts (known as chaincode) written in Go, Java or JavaScript programming languages. It was developed by the Hyperledger Foundation, a consortium of technology companies led by IBM. Hyperledger Fabric offers unique features, such as private data collections, secure Docker containers, a host-based consensus model and a flexible programming framework [33].

Before being able to visualize the overall architecture, it is necessary to understand the typical elements of a Hyperledger Fabric network and specifically those used for the proposed implementation. These elements are described below:

- Peer: Corresponds to the nodes that make up the network organizations. They are responsible for storing and distributing all the information. These are the elements that inform the orderer nodes of the network so that they can configure the transacted blocks [34].
- Orderer: One of the most important elements of the network. It is in charge of configuring the blocks according to the selected criteria and distributing them to their peers. They can belong to one or several organizations, having to reach the desired consensus. All transactions relating to the network configuration pass through them. Computers also apply basic access control for channels, restricting who can read and write data to them and who can configure them [35].
- Consensus: it is the existing mechanism in the blockchain to validate the blocks. Regarding the Fabric architecture, there have been three different algorithms throughout its history [34]. Initially, Solo was developed, an algorithm that allowed the existence of a single orderer node in charge of transacting the blocks it creates. At the same time, the Kafka algorithm emerged as an alternative, being a Byzantine fault-tolerant algorithm where one node will do all the transactions. This algorithm complicated its deployment and maintenance over time. As an evolution to these two, Raft consensus arises [36].
- Raft: is a consensus method in force since version v1.4.1 of HLF; Raft is a crash fault-tolerant ordering service (CFT) implementation based on the etcd library of the Raft protocol. It is based on a leader and follower model, where a leader node is elected (per channel), and its decisions are replicated by the followers. Raft ordering services should be easier to configure and manage than Kafka-based ordering services, and its design allows organizations to contribute nodes to a distributed ordering service.
- Channel: the means of communication between network participants [37]. In this case, it is a form of private communication that allows data isolation and confidentiality. This layer is responsible for the transmission of information between network participants and for ensuring data integrity. It also makes it possible to establish a series of criteria or permissions to encapsulate the data being transmitted. As it is a resource that allows communication between two or more organizations, it is the key element to providing the permissions for this type of network. In the case of keeping certain information private, it is possible to create a channel outside the rest to which only certain organizations have access. This property is what demonstrates the possibility of the coexistence of several Blockchains in the same network since a channel is, in essence, an independent Blockchain.
- Certification Authorities (CA): They correspond to a typical element of public key infrastructures (PKI), which are responsible for issuing digital certificates. This layer is responsible for authenticating that the participants or actors in the communication are whom they say they are. Websites usually have a digital certificate provided by a trusted CA to verify that the website being visited is trusted [38].
- Membership Service Provider (MSP): Collects the totality of cryptographic methods used to interact with the network. Each organization must have an MSP, which contains its cryptographic information, such as its keys or the CA that issued its certificate. Clients use these credentials to authenticate their transactions, and peers use them to authenticate transaction processing (endorsements) results [38].
- Chaincode: This is how smart contracts are known in Hyperledger Fabric. A smart contract is a code invoked by a client application external to the blockchain network that manages access and modifications to a set of key-value pairs in the current state of the network through transactions. In Hyperledger Fabric, smart contracts are packaged as chaincode. Then the chaincode is installed on the peers and then defined and used in one or more channels [38].

4.3. Proposed Model

To determine the proposed model, the types of organizations and quantities are defined. The model is oriented to use its structure as the basis of the test prototype to implement with Hyperledger Fabric.

Each organization interacts in a decentralized data system. For the scheme, we implemented four organizations viz: Hospital, Laboratory, Research Center, and Health Insurance Provider. Each of these organizations has a generic character and does not represent a particular institution. Thus, each organization has different types of users: for the Hospital; the users are patients, doctors, nurses, and paramedics, among others. For the Laboratory, the users are laboratory technicians, radiologists, and biotechnologists, among others. For the Research Center, the users are scientific researchers and systems analysts. Finally, in the Health Insurance Provider, the users are consultants, vendors, and insurance administrators. A schematic of the proposed architecture is shown in Figure 4.

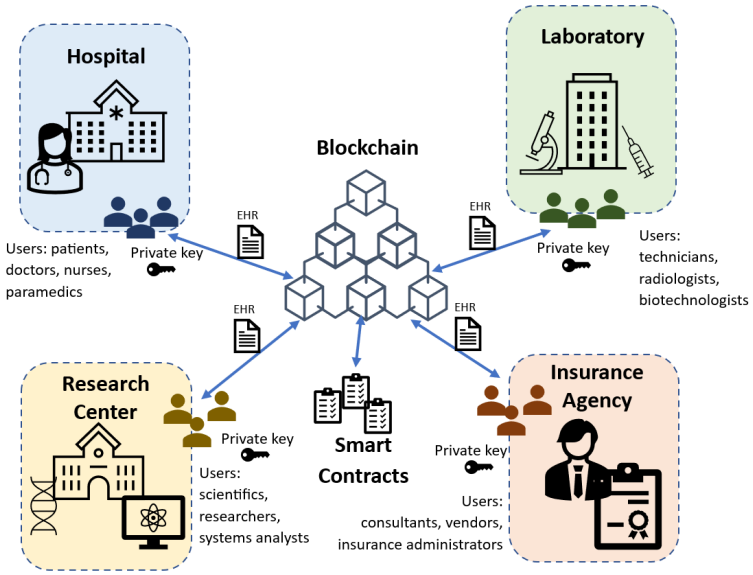

Figure 4. Scheme of the proposed architecture using four organizations: Hospital, Laboratory, Research Center, and Insurance Agency.

5. Implementation and Testing

5.1. Implementation Setup

To implement and test the proposed blockchain network model performance, we need to make some adaptations to the context of the Hyperledger Fabric architecture. The Hyperledger Fabric blockchain also uses the concept of organizations, so at this point, the adaptation is immediate. In the case of peers, these do not have direct correspondence with our model since it does not use this concept of nodes. However, they are useful for organizing groups of users or administrative subdivisions that the organization has. The concept of sub-channels is completely adapted to the structure of channels offered by the Hyperledger Fabric architecture. We can implement several channels within the same network. In this way, we adapt our EHR management model fully to the standard Hyperledger Fabric architecture.

We dispose of a Hyperledger Fabric design with four organizations: Org1 represents the Hospital, Org2 corresponds to the Laboratory, Org3 symbolizes the Research Center, and Org4 represents the Insurance Agency. In HLF, the network requires a domain name which will be health.cl, the initial adaptation scheme (a single channel called EHRChannel and a peer node) of the proposed model to the Hyperledger Fabric architecture is shown in Figure 5.

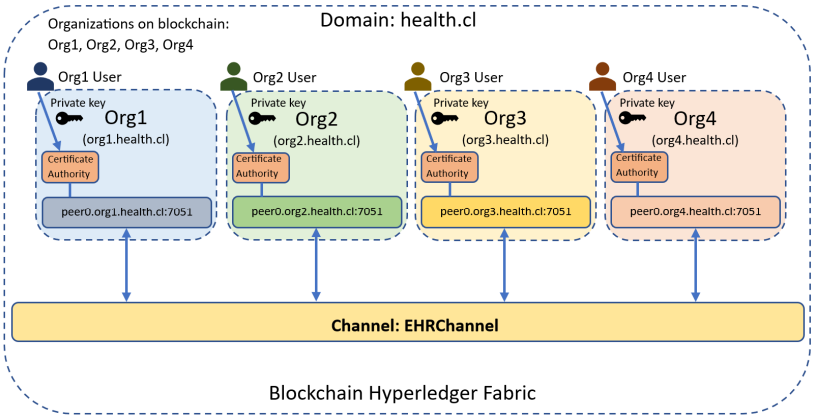

Figure 5. Adaptation of the proposed model to the Blockchain Hyperledger Fabric architecture. Each organization has its own Certification Authority [39].

The next implementation configuration steps are the deployment of orderer peers and multiple channels.

For the execution of the proposed scheme, we deploy the orderer peers per organization and not as a separate group. This alternative way of implementing the network is possible using the RAFT consensus. A striking advantage of this RAFT-based ordering service configuration is that each organization can have its own ordering nodes participating in the service. This provides a higher level of decentralization that is not available in the traditional mode. The difference between these two forms is shown in Figure 6.

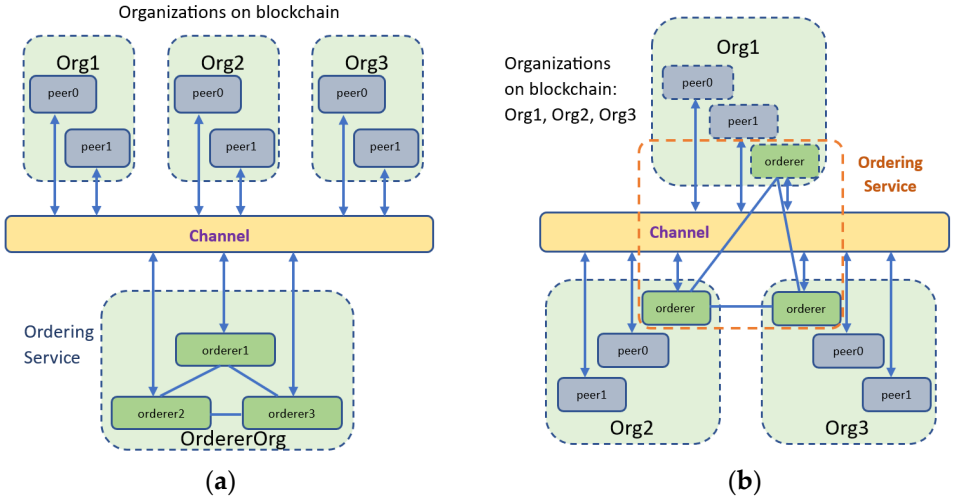

Figure 6. Example of implementation (three organizations with two peers each) formats of the ordering service in a blockchain Hyperledger Fabric. (**a**) A traditional format where all orderers peers form a new organization; (**b**) An alternative format where each organization has its own orderers nodes.

It is important to point out that for the purposes of the implementation of our network, the order services will serve the organizations that are part of its consortium, i.e., those that are linked by the same channel. If, for example, more organizations are added to the network, they can become part of an existing consortium, and the orderer brought by the new organization will be integrated into the order service of the consortium it joined.

From the configuration point of view in the Hyperledger Fabric platform, we configure the ordering node itself as OrdererEndpoints in the 'configtx.yaml' file in the 'Organizations' section. The detail of this configuration for organizations 1 and 2 is shown in Appendix A.

On the other hand, in the 'Profiles' section of the 'configtx.yaml' file, we specify the organizations that are part of each consortium. In the case of our network, the first consortium is formed by the organizations Org1, Org2 and Org3, while the second consortium

is formed by Org1, Org2 and Org4. The orderer services will participate in the RAFT instance of the consortium to which they belong. This does not interfere with the other consortium even if there are organizations that belong to both consortia (case of Org1 and Org2). The detailed configuration of the network profiles is presented in Appendix B. The channel profiles are EHRChannel1 and EHRChannel2, corresponding to the two channels of our proposed network. The detailed configuration of the channel profiles in the file 'configtx.yaml' is shown in Appendix C. If, for example, a patient in a hospital requires to schedule a medical examination in the laboratory whose cost is covered by the health insurance, the organizations Org1 (hospital), Org2 (laboratory) and Org4 (insurance agency) belonging to the consortium 2 and connected to the channel EHRChannel2 will be interacting. EHR transactions will be regulated through the smart contracts associated with the EHRChannel2 channel operating independently from the transactions occurring in the EHRChannel1 channel. If, on the other hand, a medical science researcher requires the clinical data of a patient in the hospital, the organizations Org1 (hospital) and Org3 (research center) belonging to consortium 1 will be interacting. In this case, the transactions and permissions are subject to the smart contracts of the EHRChannel1 channel and without the intervention of the I data of the EHRChannel2 channel. This type of interaction aims to deliver more privacy to hospital patients while alleviating the load of transactions that occurs between the different organizations interacting with the blockchain.

The experiment developed in this study aims to determine the performance of the proposed network compared to a traditional network deployment but under the same environment and capacity conditions. We consider the traditional network as a network working with a single channel (single channel, network A, Figure 7) and the proposed network is implemented with two channels (dual channel, network B, Figure 8). The working conditions for the experiment are as follows:

- Both networks (A and B) have the same number of organizations and peers per organization.
- The chaincode structure is the same for both networks.
- The endorsement policies are the same for both networks.
- We deploy both networks on the same virtual machine or host with the same hardware resource conditions, but not simultaneously so that the resource consumption of one blockchain does not influence the performance of the other.

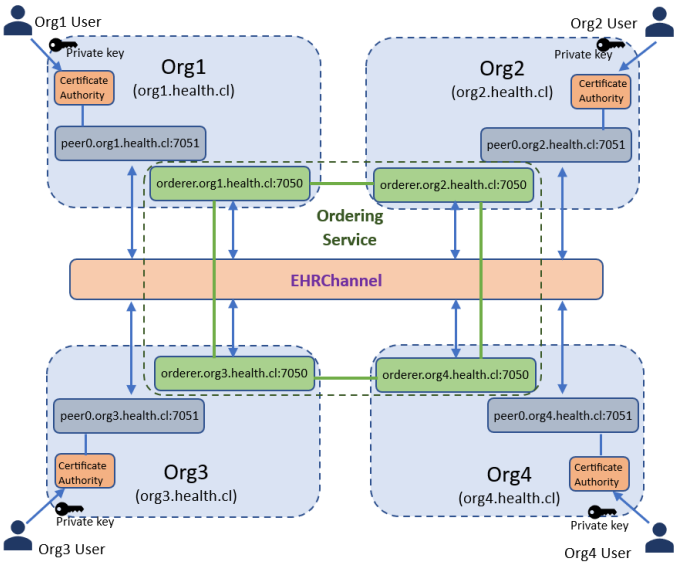

Figure 7. Testing traditional blockchain by implementing a single channel.

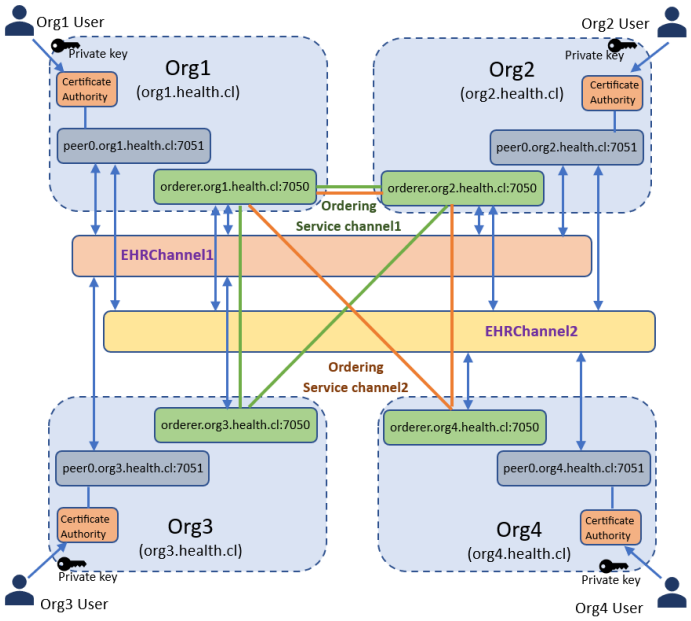

Figure 8. Test blockchain implementing a dual channel. Org1 and Org2 operate on channel EHRChannel1 and channel EHRChannel2. The green connection represents the ordering service for EHRChannel1, and the orange connection represents the ordering service for EHRChannel2.

We dispose of a personal computer Intel i7 CPU with 8GB in RAM to work with. We implemented a virtual machine to run the Ubuntu Linux operating system to run the experiment. The requirements for the working environment are shown in Table 2.

Table 2. Requirements for implementation and testing.

Software/Platform	Version	Description
Ubuntu Linux 20.04 64bit (2GB RAM)	20.04 64 bit	Operative System VM
Visual Studio Code	1.761	Code Editor
Docker	23.0.1	Container
Docker Compose	1.24.0	Container
Portainer	2.16.2	Management Container
NodeJS	14.13.1	Hyperledger Caliper
NPM	6.14.8	Hyperledger Caliper
Hyperledger Fabric	2.2.0	Blockchain
Apache CouchDB	3.1	World State
Goland	1.2	Chaincode programming
Javascript	1.8.5	Callback programming
Hyperledger Caliper	0.3.2	Blockchain Benchmark

5.2. Setup Hyperledger Caliper

Hyperledger Caliper is a performance-testing tool for blockchain. It is designed to allow users to measure the performance of a specific blockchain network in a variety of scenarios. This tool provides a methodology for testing the performance of any blockchain network, including Hyperledger Fabric [40].

The Hyperledger Caliper service consists of generating a workload against a specific system under test (SUT) and continuously monitors its responses. Hyperledger Caliper's methodology for testing the performance of a Hyperledger Fabric blockchain network includes the following steps:

- Set up the test environment. This includes setting up a local blockchain network and configuring the nodes. For our case, an environment for network A (single channel) and an environment for network B (dual channel) are configured.

- Configure the testing parameters. This includes specifying the number of nodes in the network, the number of transactions, the size of the blocks, etc.
- Execute the tests. This includes running Hyperledger Caliper benchmarking on the configured test network. The commands to launch Hyperledger Caliper for network B are shown in Listing 1.
- Analyze the results. This includes collecting data from the tests, such as average network response time, number of transactions per second (TPS), and commit time, among others.
- Document the results. This includes documenting test results for further analysis.

Listing 1. Launch Hyperledger Caliper Network B.

```
npx caliper launch master \
    --caliper-workspace . \
    --caliper-benchconfig benchmarks/scenario/config.yaml \
    --caliper-networkconfig networks/health-network-local.yaml \
    --caliper-flow-only-test \
    --caliper-fabric-gateway-usegateway \
    --caliper-fabric-gateway-discovery
```

Hyperledger Caliper does not include any particular reference implementation, but it is up to each developer to create a workload module for each test round. This means that users must generate transaction content and submit it to be executed by Caliper. Each round can have a different workload implementation, so it will be easy to separate the behavior of each round. Workload modules are used, which are basically Node.JS modules that export a given API or function [41,42].

Given its modular design, Hyperledger Caliper separates two important processes:

- The master process that connects to the SUT (and sometimes initializes) coordinates the execution of the test rounds and handles the generation of the performance report based on the statistics of the observed transactions.
- The worker processes perform the actual workload generation independently of each other. The workers execute the callbacks that are parametrically coupled to the SUT chaincodes.

A benchmark test consists of repeatedly executing named test callback files over a series of rounds, where the duration of each round is controlled, and the load is driven during these rounds by (potentially multiple) clients that are, in turn, controlled through a rate control mechanism [43,44]. For the case of our tests, we implement three workers performing 1000 transactions in two rounds (Create Rate and Query Rate). We determine the tests for fixed Send Rate of 25, 50, 100 and 200 TPS. The process schematic for Hyperledger Caliper is shown in Figure 9.

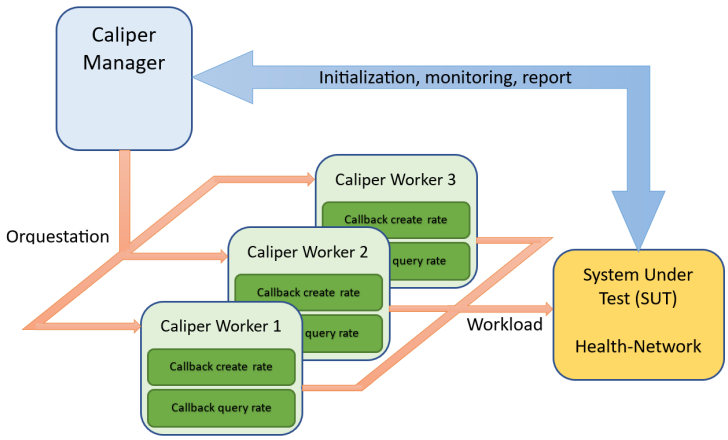

Figure 9. The process scheme for benchmarking with Hyperledger Caliper.

5.3. Results of the Experiments

Hyperledger Caliper displays performance results per round. Each round consists of 1000 transactions. We apply tests for a sending rate of 25, 50, 100 and 200 TPS. In the first phase of the experiment, we take the log of the rounds corresponding to the Create Rate and Query Rate Callbacks of the single-channel network. Table 3 shows the results of the Create Rate round with transaction rates of 25, 50, 100 and 200 TPS. In the first column of Table 2, we specify the number of successful transactions per specified send rate (column 2). The columns that follow correspond to the measurement of maximum latency, minimum latency, average latency, and throughput per specified sending rate. Tables 3–5 have the same structure.

Table 3. Throughput Create Rate single channel network.

Succ	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
960	25	5.04	0.83	1.82	21.8
984	50	5.47	0.88	2.36	43.1
966	100	5.83	0.91	2.88	78.6
976	200	5.94	0.97	3.62	148.7

Table 4. Throughput Query Rate single channel network.

Succ	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
992	25	2.01	0.04	0.18	23.3
1000	50	2.31	0.07	0.20	50.0
1000	100	2.48	0.07	0.31	83.2
994	200	3.02	0.08	0.52	167.1

Table 5. Throughput Create Rate dual-channel network.

Succ	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
987	25	4.26	0.71	1.56	25.0
993	50	4.70	0.74	2.10	48.5
988	100	4.92	0.78	2.31	87.4
997	200	5.03	0.85	3.12	164.4

Table 4 below shows the results for the Query Rate round of the single channel network. Table 4 shows that for the rates of 50 and 100 TPS, there are 100% of successful transactions. In general, the Query Rate round presents lower latency values and better throughput than the Create Rate round.

Table 5 shows the performance result of the Create Rate round for the dual-channel blockchain design. In Table 5, we verify that, in general, the latency and throughput values are higher than the Create Rate round of single-channel design.

Table 6 displays the result for the Query Rate round of the dual-channel network. In Table 6, we observe that, for the sending rates of 50, 100 and 200 TPS, 100% of successful transactions are achieved. Additionally, for the sending rates of 25 and 50 TPS, the throughput is maximum. Finally, we verify that, in general, the Query Rate round of the dual-channel blockchain has lower latencies and better throughput than the Query Rate round of the single-channel design.

Table 6. Throughput Query Rate dual-channel network.

Succ	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
997	25	1.72	0.03	0.15	25.0
1000	50	1.96	0.06	0.17	50.0
1000	100	2.10	0.07	0.24	94.4
1000	200	2.51	0.07	0.44	186.2

Throughput and average latency are parameters that directly affect the performance of a blockchain network [45] and, therefore, also influence the scalability of the system. The graph in Figure 10 shows the comparison of the throughput of the Create Rate round for the single-channel and dual-channel cases. In the graph, we verify that, in general, for the Create Rate round, the performance of the two-channel blockchain is superior for all sending rates (TPS). We also observe that for the 25 TPS send rate, the performance is maximum in the dual-channel design.

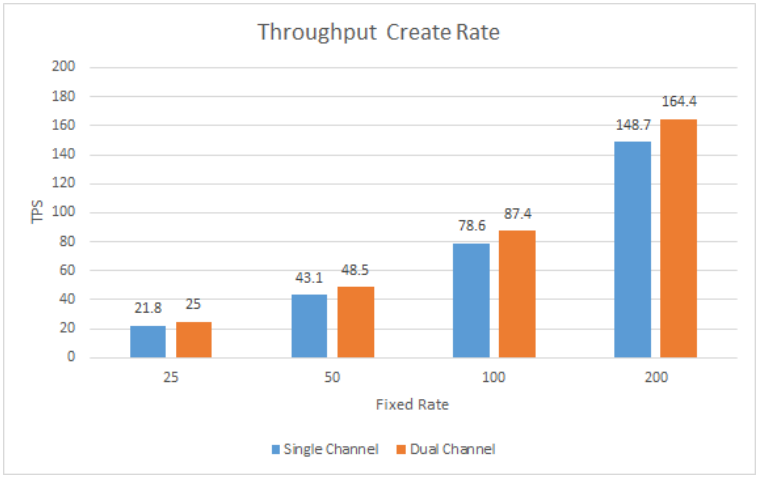

Figure 10. Create Rate round throughput, comparison between single channel and dual channel.

The graph in Figure 11 compares the Throughput Query Rate between single-channel and dual-channel. In this graph, we observe that, in general, for the Query Rate round, the performance of the dual-channel blockchain is superior except for 50 TPS, where the performance remained at the maximum point.

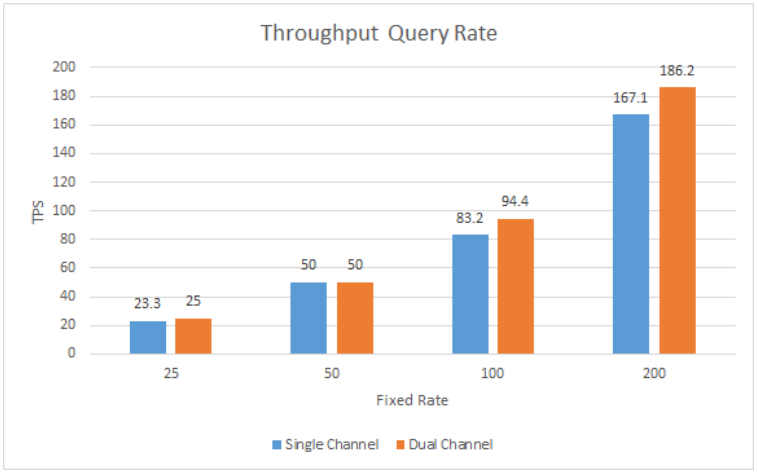

Figure 11. Query Rate round throughput, comparison between single channel and dual channel.

The graph in Figure 12 compares the average latency of the Create Rate round between the single-channel and dual-channel blockchain prototypes. In this graph, we observe that for all submission rates, the average latency is lower for the dual-channel blockchain.

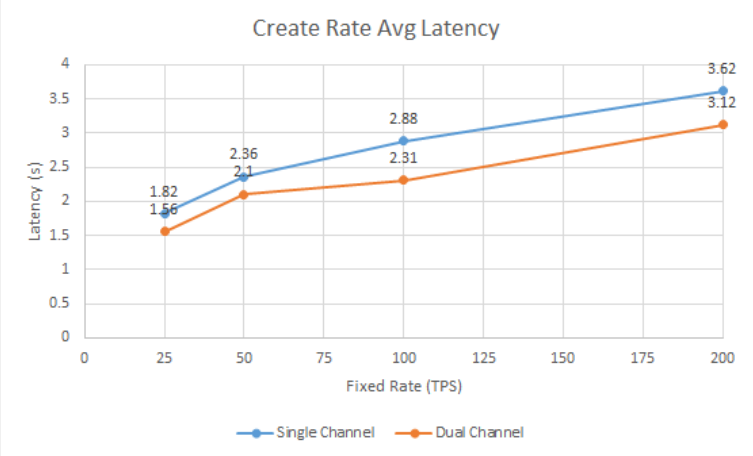

Figure 12. Average latency of the Create Rate round, comparison between single channel and dual channel.

The graph in Figure 13 compares the average latency of the Query Rate round between a single-channel and dual-channel blockchain. In this graph in Figure 13, we observe that the decrease in the average latency of the dual-channel blockchain is more significant for the 100 and 200 TPS sending rates, while for the 25 and 50 TPS sending rates, the difference in the average latency between the one-channel and two-channel network is only 0.03 milliseconds.

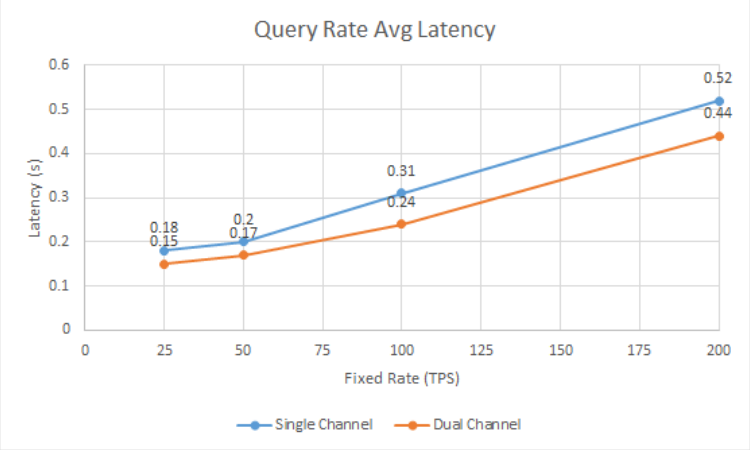

Figure 13. Average latency of the Query Rate round, comparison between single channel and dual channel.

6. Analysis and Discussion

In this section, we analyze the performance of our proposed system with respect to decentralization, security and privacy, latency, and scalability. Overall, the data observed in the throughput parameters in Tables 3–6 indicate that there is a perceptible improvement in the performance of the two-channel network over the single-channel network. The improvements are present in all sending rates (25, 50, 100 and 200 TPS) and for both submitted rounds (Create Rate and Query Rate), with the exception of the 50 TPS case for the Query Rate round where the maximum throughput is reached in the two blockchain formats.

In terms of performance review, latency is the time elapsed from the time a transaction proposal is sent by the smart contract until it is posted to the general ledger. It is observed that latencies (Max, Min and Avg) in transactions decrease when the dual channel network

is used. The probabilities of successful transactions are also beneficial in the dual channel network measurements.

In Table 7, we present a summary of the network performance improvement percentages when relating the single-channel and dual-channel cases for each round. We observe that, in general, the percentage improvement in blockchain performance when implementing dual-channel is not high. The most important performance improvement occurs at 20 TPS in the Create Rate round, where a value of 14.7% is reached.

Table 7. Summary of the network performance improvement round Create Rate and round Query Rate.

Send Rate (TPS)	Round Create Rate [%]	Round Query Rate [%]
25	14.7	7.3
50	12.5	0
100	11.2	13.5
200	10.6	11.4

In the case of the Create Rate round, performance improvements decrease as the transaction rate increases. This occurs because all peers share hardware resources since the nodes all run on the same machine. Processing and memory usage becomes more inefficient for higher transaction rates. This effect is not as noticeable for the Query Rate round, but there is a drop in performance improvement from 100 TPS to 200 TPS. Additionally, in the case of the Query Rate round, for 25 TPS and 50 TPS, the percentage improvements are the lowest because the throughput that happened with the single channel network is high. In the case of the 50 TPS sending rate, there is no improvement possible because the throughput is the maximum for one and two channels.

The average latency comparison plots shown in Figures 12 and 13 indicate that, for both Query Rate and Create Rate rounds, latency times are lower when comparing the dual-channel scheme with respect to the single-channel scheme for all data load rates. The most significant improvements occur in the Create Rate round, where the decrease in latency is around 0.5 s. This decrease remains almost constant for all upload rates for the Create Rate round, so it can be deduced that either the TPS does not significantly influence the latency or also the hardware capacity is effective.

An important strategy to achieve a better decentralization of the network is the use of orderer nodes per organization. In none of the related works studied is the use of the separate ordering service per organization verified. In our framework, the user with the patient role defines the access permission rules (read, write, update, delete) and the time for sharing his EHR using smart contracts on the blockchain. The smart contract is executed on the blockchain if the data requesters meet the conditions to access the health data. Data privacy is improved by using multiple channels on the blockchain. The latency of our proposed system is compared with similar systems studied in the review of related works. We use metrics whose measurement methods and conditions are also similar to ours. In reference [30], it is observed that the average latency in Query operations has values of 0.12, 0.44 and 3.51 for Send Rate (TPS) of 50, 100 and 200, respectively. Our proposed system presents average latency of 0.17, 0.24 and 0.44 for Send Rate of 50, 100 and 200 TPS, respectively, clearly showing better timing performance. Reference [44], we verified the average latency of the 1 org 1 peer case whose minimum value a is 3.13 s at 50 TPS. However, in our proposed system we compare it with the Create Rate operation, which presents an average latency of 2.10 s at 50TPS. Regarding throughput, in reference [44], the throughput with a Send Rate of 200TPS is 124TPS, while our proposed framework reaches 164.4. For Send Rates of 50 and 100 TPS, the throughputs are similar to ours. In reference [31], the performances are similar to our proposed system for Query but in the case of Write, we compare it with Create Rate, for which our performance is slightly higher. To deliver a comparative analysis, we have evaluated existing blockchain-based EHR manager systems [22,30,31,44] considering their experimentation methodologies. Table 8 shows the comparison of the dual-channel blockchain model with several related works

with respect to various technical characteristics. We selected the parameters that influence the performance and scalability of the system during our analysis. We used two options: Y-yes (available) and N-no (not available). The comparison results show that the dual-channel blockchain model performs better than these related works and offers a promising solution for improving current electronic health record management applications.

Table 8. Comparative analysis of the proposed framework with related work systems.

Features	[22]	[30]	[31]	[44]	Our Proposed Model
Throughput (TPS)	Y	Y	N	Y	Y
Scalability	N	N	N	N	Y
Decentralization	Y	Y	N	N	Y
Latency	N	Y	N	Y	Y
Privacy	Y	Y	Y	Y	Y

This type of comparative study to evaluate performance and scalability issues of blockchains in organizational and business processes is gaining more and more importance [46]. Our motivation leads us to design experimental practices to approach blockchain-based EHR management environments more realistically. Variants, such as testing with several smart contracts, dynamic entry or exit of peers in the process, and progressive transaction loading rate, are some elements contemplated for future testing and analysis.

7. Conclusions and Future Work

In this paper, we propose a novel EHR management design based on blockchain Hyperledger Fabric aimed at improving scalability. We present the multichannel Hyperledger Fabric system as a viable alternative to implement in an EHR management system. The tests performed on the prototypes allow us to quantitatively validate the efficiency in terms of performance and scalability of the blockchain. The work methodology allows to delivery of a detailed implementation from the conceptual scheme of the management system, adaptation to the Fabric architecture, implementation of RAFT consensus, and distributed orderer nodes up to the performance tests with Caliper.

The results obtained from the performance improvements of the blockchain using two channels point out that they are achieved, but they are of low magnitude, around 10%, with a maximum of 14.7%. These values have two interpretations:

- For high TPS rates (100 and 200), the performances obtained are low and are mainly conditioned by the shared use of hardware resources. An important variation in future tests is the distribution of nodes in different machines to obtain performances closer to a production environment. In addition, look for other scalability improvement alternatives complementary to multichannel.
- For low TPS rates (25 and 50), we have two cases: in the Create Rate round, we can see improvements of over 12%. In the case of the Query Rate round, good performances (over 90%) can be seen both with the single-channel network and with the dual-channel network.

The transaction effectiveness parameters are significantly improved for dual-channel so that in a total of the four Query Rate rounds (4000 transactions), there are only three failures (99.925% effectiveness).

The limitations of the EHR management system are directly related to the limitations of Hyperledger Fabric, whose consensus method is not fault tolerant. However, this limitation is not critical since, in a healthcare system; all participants must be properly verified to operate in the network. An important point to take into account when designing and implementing the EHR management system based on blockchain dual-channel is to be careful that at least one organization of the health system must participate in two channels, thus avoiding leaving organizations completely isolated from the rest of the health system.

In the future, we propose to work with a multi host testing prototype with hardware resource control (use of virtual machines) to evaluate how hardware capabilities influence blockchain performance. Evaluate the enablement of more channels in combination with more participating organizations in the network. We also intend to extend the work, empirically addressing the problem of EHR management document storage in a Hyperledger Fabric scheme. Another important aspect that we intend to address in the future is the use of real EHR datasets available from some open medical research repositories. The use of real data will also require the implementation of a friendly user interface.

Author Contributions: Conceptualization, Á.D.; methodology, Á.D. and H.K.; software, Á.D.; validation, Á.D. and H.K.; formal analysis, Á.D. and H.K.; investigation, Á.D. and H.K.; resources, Á.D. and H.K.; data curation, Á.D.; writing—original draft preparation, Á.D.; writing—review and editing, Á.D. and H.K.; visualization, Á.D.; supervision, H.K.; project administration, Á.D. and H.K.; funding acquisition, Á.D. and H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the University of Santiago of Chile (USACH), DICYT Project, Code 062113KC Vicerrectoría of Research, Development, and Innovation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Faculty of Engineering of University of Santiago of Chile. Acknowledgments DICYT Project, Code 062113KC, Vicerrectoria of Research, Development, and Innovation.

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

Appendix A

```
################################################################################
#   Section: Organizations
################################################################################
Organizations:

    - &Org1
        Name: Org1MSP
        ID: Org1MSP
        MSPDir: crypto-config/peerOrganizations/org1.health.cl/msp
        Policies:
            Readers:
                Type: Signature
                Rule: "OR('Org1MSP.admin', 'Org1MSP.peer', 'Org1MSP.client')"
            Writers:
                Type: Signature
                Rule: "OR('Org1MSP.admin', 'Org1MSP.client')"
            Admins:
                Type: Signature
                Rule: "OR('Org1MSP.admin')"
            Endorsement:
                Type: Signature
                Rule: "OR('Org1MSP.peer')"
        AnchorPeers:
            - Host: peer0.org1.health.cl
              Port: 7051
        OrdererEndpoints:
            - orderer.org1.health.cl:7050

    - &Org2
        Name: Org2MSP
        ID: Org2MSP
        MSPDir: crypto-config/peerOrganizations/org2.health.cl/msp
        Policies:
            Readers:
                Type: Signature
                Rule: "OR('Org2MSP.admin', 'Org2MSP.peer', 'Org2MSP.client')"
            Writers:
                Type: Signature
                Rule: "OR('Org2MSP.admin', 'Org2MSP.client')"
            Admins:
                Type: Signature
                Rule: "OR('Org2MSP.admin')"
            Endorsement:
                Type: Signature
                Rule: "OR('Org2MSP.peer')"
        AnchorPeers:
            - Host: peer0.org2.health.cl
              Port: 7051
        OrdererEndpoints:
            - orderer.org2.health.cl:7050
```

Figure A1. Health-Network Org1 and Org2 Setup.

Appendix B

```
################################################################################
#   Profile
################################################################################
Profiles:
    FourOrgsOrdererGenesis:
        <<: *ChannelDefaults
        Orderer:
            <<: *OrdererDefaults
            Organizations:
                - *Org1
                - *Org2
                - *Org3
                - *Org4
            Capabilities:
                <<: *OrdererCapabilities
        Consortiums:
            SampleConsortium1:
                Organizations:
                    - *Org1
                    - *Org2
                    - *Org3
            SampleConsortium2:
                Organizations:
                    - *Org1
                    - *Org2
                    - *Org4
```

Figure A2. Health-Network Profiles.

Appendix C

```
EHRChannel1:
    Consortium: SampleConsortium1
    Application:
        <<: *ApplicationDefaults
        Organizations:
            - *Org1
            - *Org2
            - *Org3

        Capabilities:
            <<: *ApplicationCapabilities

EHRChannel2:
    Consortium: SampleConsortium2
    Application:
        <<: *ApplicationDefaults
        Organizations:
            - *Org1
            - *Org2
            - *Org4
```

Figure A3. Channels Profiles.

References

1. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE Access* **2019**, *7*, 118943–118953. [CrossRef]
2. Shahnaz, A.; Qamar, U.; Khalid, A. Using Blockchain for Electronic Health Records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
3. Diaz, A.; Kaschel, H. Scalable Management Architecture for Electronic Health Records Based on Blockchain. In *Proceedings of the 2022 IEEE International Conference on Automation/XXV Congress of the Chilean Association of Automatic Control (ICA-ACCA), Curicó, Chile, 24–28 October 2022*; IEEE: New York, NY, USA, 2022; pp. 1–7. [CrossRef]
4. Dagliati, A.; Malovini, A.; Tibollo, V.; Bellazzi, R. Health informatics and EHR to support clinical research in the COVID-19 pandemic: An overview. *Brief. Bioinform.* **2021**, *22*, 812–822. [CrossRef] [PubMed]
5. 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]
6. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
7. Tandon, A.; Dhir, A.; Islam, A.N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
8. Pradhan, N.R.; Singh, A.P.; Verma, S.; Kavita; Kaur, N.; Roy, D.S.; Shafi, J.; Wozniak, M.; Ijaz, M.F. A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed. *Sensors* **2022**, *22*, 3449. [CrossRef]

9. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. [CrossRef]
10. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
11. Tavares, B.; Correia, F.F.; Restivo, A. A survey on blockchain technologies and research. *J. Inf. Assur. Secur.* **2019**, *14*, 118–128.
12. 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] [PubMed]
13. Praveen, G. The Impact of Blockchain on the Healthcare Environment. *J. Inform. Electr. Electron. Eng.* **2021**, *2*, 1–11. [CrossRef]
14. Mohan, M.S.; Sujihelen, L. A Study on Blockchain and the Healthcare System. In *Proceedings of the 5th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 3–5 June 2021*; IEEE: New York, NY, USA, 2021; pp. 518–521. [CrossRef]
15. Abreu, A.W.d.S.; Coutinho, E.F.; Bezerra, C.I.M. Performance Evaluation of Data Transactions in Blockchain. *IEEE Lat. Am. Trans.* **2022**, *20*, 409–416. [CrossRef]
16. Sonkamble, R.G.; Bongale, A.M.; Phansalkar, S.; Sharma, A.; Rajput, S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics* **2023**, *12*, 1015. [CrossRef]
17. 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]
18. Wadud, A.H.; Bhuiyan, T.M.A.-U.; Uddin, A.; Rahman, M. A Patient Centric Agent Assisted Private Blockchain on Hyperledger Fabric for Managing Remote Patient Monitoring. In *Proceedings of the 11th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 17–19 December 2020*; IEEE: New York, NY, USA, 2020; pp. 194–197. [CrossRef]
19. Fernandes, A.; Rocha, V.; da Conceicao, A.F.; Horita, F. Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In *Proceedings of the 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil, 16–20 March 2020*; IEEE: New York, NY, USA, 2020; pp. 130–138. [CrossRef]
20. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. *Sensors* **2021**, *21*, 2865. [CrossRef] [PubMed]
21. Cernian, A.; Tiganoaia, B.; Sacala, I.; Pavel, A.; Iftemi, A. PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records. *Sensors* **2020**, *20*, 6538. [CrossRef]
22. Huang, J.; Qi, Y.W.; Asghar, M.R.; Meads, A.; Tu, Y. Sharing medical data using a blockchain-based secure EHR system for New Zealand. *IET Blockchain* **2022**, *2*, 13–28. [CrossRef]
23. Ndzimakhwe, M.; Telukdarie, A.; Munien, I.; Vermeulen, A.; Chude-Okonkwo, U.K.; Philbin, S.P. A Framework for User-Focused Electronic Health Record System Leveraging Hyperledger Fabric. *Information* **2023**, *14*, 51. [CrossRef]
24. Mukherji, A.; Ganguli, N. Efficient and Scalable Electronic Health Record Management using Permissioned Blockchain Technology. In *Proceedings of the 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2–4 October 2020*; IEEE: New York, NY, USA, 2020; pp. 1–6. [CrossRef]
25. 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]
26. Randolph, J.; Faruk, J.H.; Saha, B.; Shahriar, H.; Valero, M.; Zhao, L.; Sakib, N. Blockchain-based Medical Image Sharing and Automated Critical-results Notification: A Novel Framework. In *Proceedings of the IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 27 June–1 July 2022*; IEEE: New York, NY, USA, 2022; pp. 1756–1761. [CrossRef]
27. Sammeta, N.; Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* **2022**, *8*, 625–640. [CrossRef]
28. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain. *arXiv* **2021**, arXiv:2103.10186.
29. Atreyapurapu, S.B.; Amarendra, K.; Alishah, M.M. Hyperledger Fabric based Medical Record Security. In *Proceedings of the 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January 2022*; IEEE: New York, NY, USA, 2022; pp. 223–228. [CrossRef]
30. Singh, A.P.; Pradhan, N.R.; Luhach, A.K.K.; Agnihotri, S.; Jhanjhi, N.Z.; Verma, S.; Kavita; Ghosh, U.; Roy, D.S. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5779–5789. [CrossRef]
31. Mahore, V.; Aggarwal, P.; Andola, N.; Raghav; Venkatesan, S. Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain. In *Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019*; IEEE: New York, NY, USA, 2019; pp. 1–6. [CrossRef]
32. Khatri, S.; Alzahrani, F.A.; Ansari, T.J.; Agrawal, A.; Kumar, R.; Khan, R.A. A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges. *IEEE Access* **2021**, *9*, 84666–84687. [CrossRef]
33. Nasir, Q.; Qasse, I.A.; Abu Talib, M.; Nassif, A.B. Performance Analysis of Hyperledger Fabric Platforms. *Secur. Commun. Networks* **2018**, *2018*, 3976093. [CrossRef]
34. Hyperledger Fabric, Peers—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html (accessed on 5 April 2023).

35. Hyperledger Fabric, The Ordering Service—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html (accessed on 5 April 2023).
36. Cakmak, A.; Ozcan, B.; Ozdem, M.; Bekin, F.; Kirtekin, K.; Aydin, S.; Ayaz, E. Blockchain Based Project Management. In *Proceedings of the 3rd International Informatics and Software Engineering Conference (IISEC), Ankara, Turkey, 15–16 December 2022*; IEEE: New York, NY, USA, 2022; pp. 1–6. [CrossRef]
37. Hyperledger Fabric, Channels—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/channels.html (accessed on 5 April 2023).
38. Hyperledger Fabric, Glossary—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/glossary.html (accessed on 5 April 2023).
39. How Fabric Networks Are Structured—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html (accessed on 5 April 2023).
40. Hyperledger Caliper, Architecture | Hyperledger Caliper. Available online: https://hyperledger.github.io/caliper/v0.3.2/architecture/ (accessed on 5 April 2023).
41. Choi, W.; Hong, J.W.-K. Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper. In *Proceedings of the 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Takamatsu, Japan, 28–30 September 2022*; IEEE: New York, NY, USA, 2022; pp. 325–329. [CrossRef]
42. Dabbagh, M.; Kakavand, M.; Tahir, M.; Amphawan, A. Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum. In *Proceedings of the 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), Kinabalu, Malaysia, 26–27 September 2020*; IEEE: New York, NY, USA, 2020; pp. 1–6. [CrossRef]
43. IBM Developer, Archived | Performance Testing Smart Contracts Developed within VS Code Using Hyperledger Caliper. Available online: https://developer.ibm.com/tutorials/blockchain-performance-testing-smart-contracts-vscode-caliper/ (accessed on 5 April 2023).
44. Panwar, A.; Bhatnagar, V.; Khari, M.; Salehi, A.W.; Gupta, G. A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. *Comput. Intell. Neurosci.* **2022**, *2022*, 3045107. [CrossRef]
45. Chen, C.-L.; Yang, J.; Tsaur, W.-J.; Weng, W.; Wu, C.-M.; Wei, X. Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT's Application. *Sensors* **2022**, *22*, 1146. [CrossRef]
46. Venkatraman, S.; Parvin, S. Developing an IoT Identity Management System Using Blockchain. *Systems* **2022**, *10*, 39. [CrossRef]