Fall 12-14-2022

A Comparative Study on Blockchain-based Electronic Health Record Systems: Performance, Privacy, and Security Between Hyperledger Fabric and Ethereum Frameworks

Md Jobair Hossain Faruk
Kennesaw State University

Hossain Shahriar
Kennesaw State University

Maria Valero
Kennesaw State University

Xia Li
Kennesaw State University

A Comparative Study on Blockchain-based Electronic Health Record Systems: Performance, Privacy, and Security Between Hyperledger Fabric and Ethereum Frameworks

A Thesis Presented to

The Faculty of the Software Engineering and Game Development Department

by

Md Jobair Hossain Faruk - MSSWE Candidate, December 2022

Student ID: 001007165

Advisor (s)

Professor Hossain Shahriar - Committee Chair
Professor Maria Valero - Committee Chair
Professor Xia Li - Committee Member

In Partial Fulfillment of Requirements for the Degree

Master of Science in Software Engineering

Kennesaw State University

December 2022

In presenting this thesis as a partial fulfillment of the requirements for an advanced degree from Kennesaw State University, I agree that the university library shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to copy from, or to publish, this thesis may be granted by the professor under whose direction it was written, or, in his absence, by the dean of the appropriate school when such copying or publication is solely for scholarly purposes and does not involve potential financial gain. It is understood that any copying from or publication of, this thesis which involves potential financial gain will not be allowed without written permission.

Md Jobair Hossain Faruk

I would like to take a moment to express my special thanks of gratitude to my supervisor Dr. Hossain Shahriar and other two committee members Dr. Maria Valero and Dr. Xia Li for their meaningful guidance to conclude this thesis. I also place on record, my sincere appreciation to my parents and my brother for their advice and encouragement in every step of my life.

ABSTRACT

Traditional data collection, storage, and processing of Electronic Health Records (EHR) utilize centralized techniques that pose several risks of single point of failure and lean the systems to a number of internal and external data breaches that compromise their reliability and availability. Addressing the challenges of conventional database techniques and improving the overall aspects of EHR application, blockchain technology is being evaluated to find a possible solution. Blockchain refers to an emerging distributed technology and incorruptible database of records or digital events which execute, validate, and maintain by a ledger technology to provide an immutable architecture and prevent records manipulation or alterations. However, there are multiple frameworks emerged in recent years where identifying the advantages and limitation is crucial. This thesis focuses on (i) introducing electronic health records systems using two widely used blockchain frameworks, Hyperledger Fabric and Ethereum. (ii) aims to provide a comparative study on both frameworks from the performance, privacy, and security perspectives. Based on two different introduced EHR systems, we identify the strength and weaknesses of both frameworks and present the challenges and limitations of these systems. According to a comparative study, the Hyperledger Fabric framework demonstrates advanced features including private and consortium networks that can facilitate EHR systems from both security and performance perspectives. Taking the experience into consideration, we aim to extend our study in software engineering domain to evaluate the limits to developing blockchain-based software applications and highlight the way to improve current SE practices in future studies.

Keywords: Electronic Health Records (HER), Blockchain Technology, Hyperledger Fabric, Ethereum

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION | MOTIVATION

1.1 Background

Health can be defined as “a state of physical, mental, and social prosperity and not merely the absence of disease or infirmity.” Having proper healthcare is a demand of human beings in the modern world [1]. Good quality of care and better access to healthcare facilities is of paramount importance for society and the elderly population. Statistics indicate that from 1980 to 2016, the average life expectancy at birth increased from 73.7 to 78.6 years [2]. As a result, the healthcare industry is an important sector that seems to emerge as one of the essential parts of human lives. The current scene of computerized well-being is not only technological, but also social, cognitive, and political; the ultimate goal is to cooperate with participatory health, a partnership with digital devices collecting data and generating insights, adopt new models of care, evolving through collaborations between clinicians, patients, and carers [3].

Health informatics encompasses not just the use of computers, but also the complete management of information in healthcare, including the creation and evaluation of methods and systems for acquiring, processing, and interpreting patient data [4]. According to a study by Hassan Aziz [5] health informatics is a wide-ranging science that encompasses the complex mixture of people, organizations, illnesses, patient care, and treatment all of which are intertwined with modern information technology, particularly in computing and communication. Health records used to be recorded on paper and kept in folders divided into categories based on the type of note, and there was only one copy available. This changed in the 1960s and 1970s when new computer technologies were developed to support Electronic Health Records (EHR) [6]. EHRs grew in popularity because of their ability to rapidly gather and manage sets of information, monitor changes in patient outcomes after installation of a new practice or treatment, and determine whether patients are due for physical exams, procedures, and immunizations [7]. Correspondingly, EHRs have revolutionized the format of health records, transforming the healthcare industry and making patients' medical records easier to read and access from virtually anywhere on the globe [6]. However, all the records in the conventional computing approach can be manipulated or altered easily, which creates concerns in terms of the security and privacy of patients [8]. This is where an approach called "blockchain" emerged to introduce a revolutionary computer protocol used for the digital recording and storing of information in a decentralized and distributed ledger [9], [10].

Data in healthcare systems are stored and processed centrally, which increases the danger of a single point of failure and exposes the systems to a number of external and internal threats [11]. However, data should never be stored as writing in pencil that could deface anytime and should be stored in an immutable format to protect data transaction transparency. In order to reform traditional healthcare practices, blockchain technology can be a model that helps to address such crucial problems [11], [12]. Blockchain is potentially a solution due to its immutability and architectural nature, where every block has a particular summary of the preceding block that is arranged using a secure hash value, string order, timing, content, and order of trades that cannot be manipulated or altered [13].

Considering various blockchain frameworks, there are different types of networks including private, public, and consortium blockchain networks [14], [15]. There is no concrete study were conducted so far to provide a comparative study between these frameworks, particularly in the healthcare domain. This research aims to provide a comparative study of two widely used blockchain frameworks including Hyperledger Fabric and Ethereum from the performance, privacy, and security perspectives. In order to conduct a comparative study, developing applications using both frameworks are important. Thus, we aim to develop two separate applications using blockchain frameworks to identify the strength and weaknesses of both frameworks and present the challenges and limitations of these systems.

1.2 Research

1.2.1 Research Goals

In this thesis, we explore blockchain technology for electronic health records (EHR) to develop EHR data storing and sharing system in a secure, immutable, and transparent network. The research goals are:

- To assess the feasibility of blockchain technology for electronic health records applications.
- To propose two frameworks by utilizing two widely used blockchain frameworks, Hyperledger Fabric and Ethereum.
- To provide a comparative study on both frameworks from the performance, privacy, and security perspectives.
- To explore means to structure and analyze the challenges and limitations of both EHR applications.

1.2.2 Research Questions

During the feasibility study, we embarked on various research questions to address in this thesis study are the following:

- Is blockchain technology a well-suited form of a database for electronic health records (EHR)?
- Which blockchain frameworks can be adopted for the development of an EHR-based systems?
- How a comparative study on blockchain frameworks can help future researchers to identify suitable techniques to develop EHR systems?

1.2.3 Organization on the Thesis

The organization of this thesis is as follows. Chapter I presents the background of the topic, research goal, and research questions. Chapter II discusses blockchain technology and two of its widely known frameworks, Hyperledger Fabric and Ethereum followed by reviewing the relevant literature on Blockchain and Electronic Health Records (EHR) applications in Chapter III. Chapter IV introduces blockchain-based novel EHR systems using two different frameworks. Chapter V discusses a comparative study between blockchain frameworks based on proposed EHR prototypes from a security and performance lens. Chapter VI presents the findings and discusses the challenges and limitations of both frameworks. Finally, Chapter VII provides some concluding comments and future research directions.

CHAPTER II

BLOCKCHAIN TECHNOLOGY

2.1 Overview of Blockchain Technology

It is defined as a distributed, incorruptible database of records or digital events which is executed, validated, and maintained by a network of computers instead of a single central network among participating parties around the world [16], [17]. Blockchain, according to the Organization for Economic Cooperation and Development (OECD) [18] is a combination of currently existing technologies that can be used to establish networks using distributed ledger technology (DLT). These networks can store data between a group of users that are authenticated by cryptographic tools and agreed upon through predefined network protocols, usually without the control of a central authority. The concept of blockchain is completely opposite to traditional methods; while the conventional approach stores data in a centralized database, blockchain stores data in a decentralized way. Blockchain records a timestamp to avoid tempering the stored data.

Blockchain technology allows the creation of a tamper-evident, shared, and trusted ledger that sequentially appends cryptographically secure data transactions. The ledger would only be accessible to trusted parties. The cryptographic techniques used to record information to a blockchain guarantee that once a transaction has been added to the ledger, it cannot be modified; thereby assuring participants that they are working with data transactions that are up-to-date, accurate, and nearly impossible to manipulate. The blockchain thus functions as the sole source of truth. And the immutable nature of blockchain technology could lead to reduced cost of regulatory compliance with greater transparency, improved traceability, increased speed, and efficiency.

Blockchain embraces the full spectrum of use cases that are crucial for enterprise-based systems. Multiple blockchain infrastructures have emerged, (i) permissionless blockchain that focuses on "trustless" networks used by any individuals. Bitcoin is an example of this kind since it is wide-open, permissionless, and anyone can buy bitcoins. (ii) permissioned blockchains where only pre-verified users shall have access which is vital for some enterprise-based systems in order to protect the business affairs [19], [20]. Ethereum and Hyperledger Fabric framework are two widely known blockchain-based approaches, where Hyperledger is a fully permissioned network designed for operations involving sensitive and confidential data, whereas Ethereum is a public network that enables permissioned networks [21].

2.1.1 Hyperledger Fabric

Hyperledger [22] is a consensus-based distributed peer-to-peer ledger that combines blockchain with a system for “smart contract” application and other assistive technologies that can be utilized to develop a new generation of transactional applications that focus on trust, accountability, and transparency at their core, while streamlining business processes and legitimate limitations. Hyperledger promotes a collaborative approach to developing blockchain applications through intellectual property rights and the acceptance of essential standards [23]. Unlike open permissionless systems that allow anybody to enroll through a trusted Membership Service Provider in order to participate in the network (MSP). MSP is the technique that allows the remainder of the network to trust and recognize an identity without releasing the member's private key [22]. On another venue, the Hyperledger framework allows the execution of up to 3,500 transactions per second while Ethereum can execute 35 transactions only.

Consensus is an essential component of Hyperledger Fabric which characterizes as a distributed procedure in which a network of nodes ensures that transactions are processed in a guaranteed unique order and verifies transaction blocks [24]. It enables foreordain the varieties of channels, peers and consensus procedures needed for implementing and testing the proposed approach. These features provide another layer of security, ensuring that resources can only be accessed by network members and network transactions. Therefore, the administrator controls who can join the network and what roles they can play, as well as the ability to delete nodes if necessary.

2.1.2 Ethereum

Ethereum was introduced as a platform in 2013 as a project which attempts to build a generalized blockchain technology in which all transaction-based state machine concepts can be built, with the goal of providing a tightly integrated end-to-end system to the enddeveloper. This allows building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework [25]. Ethereum represents a blockchain with built-in decentralized transactions and a turning-complete execution environment where the system can perform any computations. However, all nodes must have access to the whole records in the blockchain. A Merkle Patricia Tree (MPT) is being used to improve the state. MPT is a special type of data structure that may store cryptographically authenticated data as keys and values [26]. Figure 1 depicts the block structure of Ethereum and its Merkle Tree in which the hash of the root node (the tree's initial node) is dependent on the hashes of all sub-nodes.

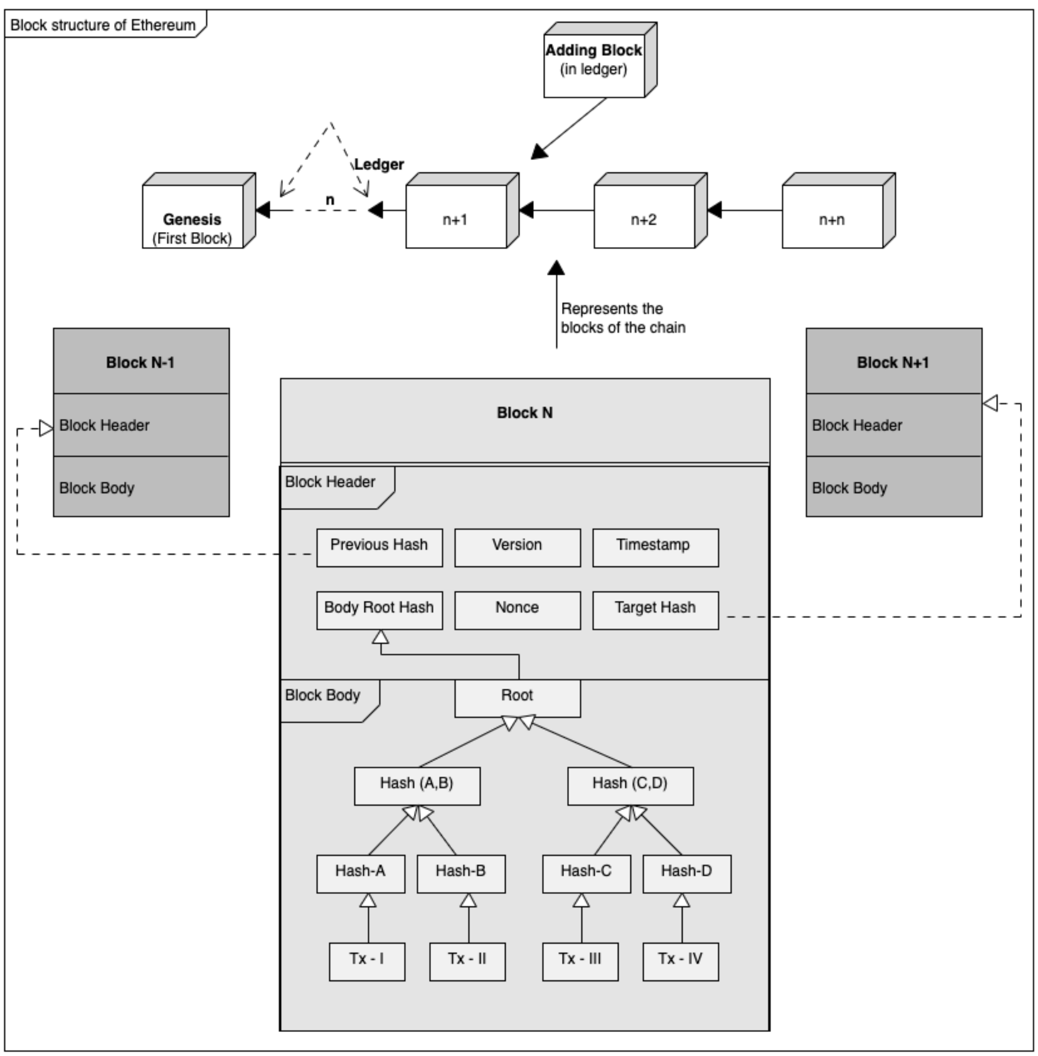


Figure 1: Ethereum's Block structure and Merkle Root

Figure 1 also illustrates the block header containing the block version that validates block rules; the hash of the “previous block” represents the value of the previous block and the "timestamp" represents the creation time of the current block. “Body Root Hash” is the root value of the Merkle tree created by transactions in the body of the block, and whereas the “Target Hash” is the hash value threshold of a new valid block. On the other hand, “Block Body” contains verified transactions, and all valid transactions are stored in a “Merkle Tree”. When the network is created, the “Genesis Block” is automatically assigned with hash default values, and further blocks are added to the ledger after the genesis block [27]. In addition, the “Ethereum State” is one of the most important aspects of the network consists of accounts, which have a 20-byte address and state transitions that are assigned to a single account [28]. The “World State” is liable for mapping addresses to account states, whereas the Ethereum network's “Consensus” is based on a modified version of the Greedy Heaviest Observed Subtree (GHOST) protocol.

2.2 Blockchain in Healthcare

Blockchain was initially used primarily in the financial industry to allow Bitcoin to function; however, efforts have been made to adapt the technology for a variety of industries, including healthcare, insurance, pharmacy, manufacturing, e-voting, energy, and many more [29]. The healthcare industry is particularly challenging as it has a complex mechanism with various influential stakeholders and a need to disrupt through innovative solutions. Blockchain has applications that can potentially address healthcare issues including public health management, remote monitoring, electronic health records (EHR), medical data management, data security, and drug development. Remarkably, blockchain can mitigate concerns about data ownership and sharing by allowing patients to keep their data and choose who they share it with [30]. Gaynor, Mark et al. [31] graphically displays several blockchain opportunities for transferring health care data in Figure 2, where these applications could assist the health care industry to better data exchange across all industry activities, including exchange, storage, and record keeping.

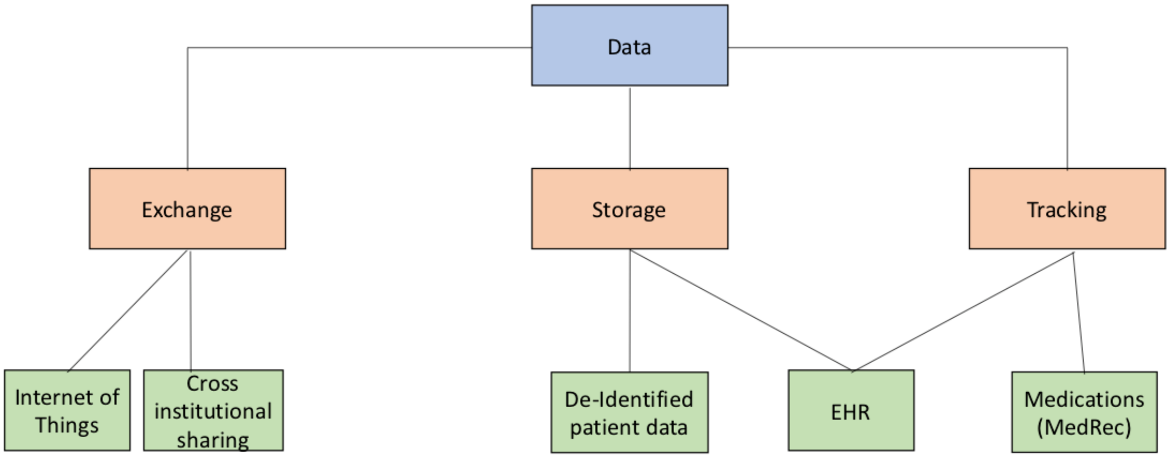


Figure 2: Data (electronic health record) exchange tree

The application of blockchain in healthcare is a recent addition to the trusted sharing of sensitive healthcare information. This novel approach was first devised to run Bitcoin cryptocurrency, but it is now being advocated by different industries including healthcare due to its enhanced authentication, confidentiality, transparency, and unique data-sharing characteristics verified by consensus. Healthcare industry adopts blockchain to address privacy and security of medical records and Hyperledger Fabric includes novel security features such as private data collections, which allow only certain authorized users to access certain data [19], [32]. In this research, we focus develop a system for secure, immutable, and transparent data storing, implementation of telehealth, and 21st-century patient data management. Figure 3 proposed by Seyednima Khezr et al. [33] depicts a workflow of blockchain-based healthcare applications.

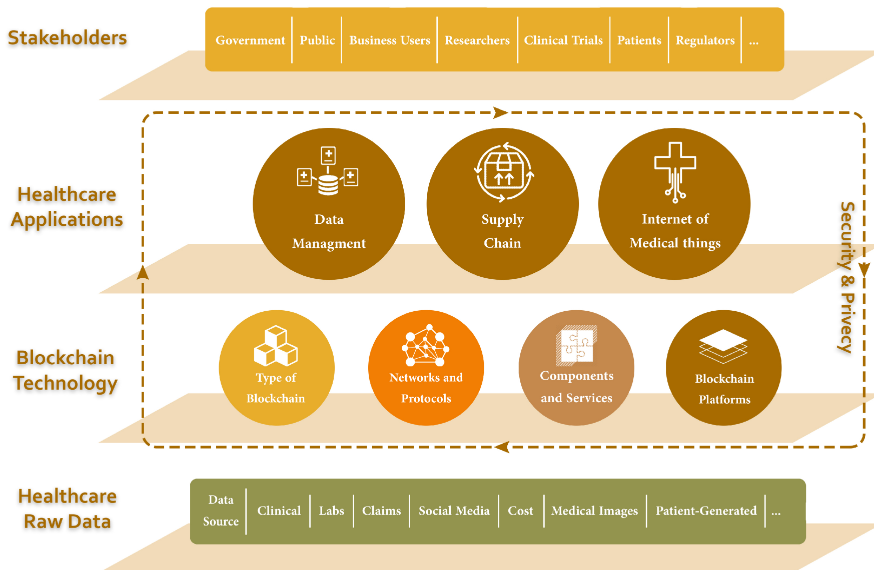


Figure 3: Blockchain workflow comprising primary layers including raw data, and stakeholders

Blockchain has the ability for addressing significant healthcare concerns while also providing unique chances to leverage the power of other emerging technologies. Despite interoperability challenges including the lack of an existing standard for developing blockchain-based healthcare applications, enabling blockchain to solve many complex problems found in today's healthcare industry that shall allow a transformation with the help of researchers and practitioners from different fields towards improving and innovating methods for viewing the health care industry [31], [34].

CHAPTER III

LITERATURE REVIEW

3.1 Related Study

According to a report of the Health System Tracker [2], the number of aging or older adults is set to augment by 69% (from 56M to 94.7M) in the next 35 years. Hence, improving the quality of care and better access to healthcare facilities is important for society and more so for the elderly population. Especially in pandemic times, when normal lifestyle is disrupted, and the population is expected to stay home, the need for remote patient monitoring has increased and the necessity is larger than ever before. Towards solving the existing problem in healthcare, researchers from different fields proposed different schemes by adopting blockchain technology. After reviewing several studies and systems of blockchain and smart contracts, we identify two frameworks, Ethereum and Hyperledger Fabric. However, we did not find any comparative study between Hyperledger Fabric and Ethereum on electronic health records (EHR) system. Thus, this study shall help the researchers in this field to better understand on both frameworks towards adopting most suitable framework based on various parameters including privacy, security, and performance.

3.1.1 Related Study: Research Work

A comparative study was conducted by Hongru Yu et al. [35] on smart contracts for blockchain-based healthcare applications. The researchers addressed various aspects of smart contracts including technical features, developing blockchain networks, testing, and summarizing implementation experience. The paper evaluated Hyperledger Fabric, Ethereum, and Multichain which emphasizes on the selection of smart contracts in accordance with the requirements of the application.

More studies have been conducted by various researchers. McSeth Antwi et al. [36] focused on Hyperledger Fabric-based applications for healthcare applications. The authors provided various testing scenarios to explore use cases and different criteria for healthcare systems. In a similar study, Qianyu Wang et al. [37] proposed enterprise-grade Hyperledger Fabric-based healthcare data management framework. The research utilizes Australian medical practice and contributed to three folds, enabling data access to patients, utilizing smart contracts for access control to automatically execute to provide permission accurately to the individuals, and confirming data ownership on health records.

3.1.2 Related Study: Application

Research has been conducted in the field of blockchain-based electronic health records (EHR) systems. In collaboration with Philips Blockchain Lab, a company named “Gem” develops enterprise health care applications networks using blockchain technology [34], [38]. The network includes wellness apps and global patient ID programs that create a healthcare ecosystem using the Ethereum approach. In order to address the trade-off between patient-centric treatment and operational efficiency, the applications would be connected to a universal data infrastructure [39]. As a result, different healthcare operators can access the same information using the Gem Health network which shall include identity schemes, data storage, and smart contracts.

In a similar context, MedRec developed a decentralized record management system for electronic medical records (EMRs) using blockchain technology [40], [41]. The system was developed using Go-Ethereum (Geth) and Solidity; however, it was not built on the live Ethereum network, instead, it creates a small-scale private blockchain with extensive, specific APIs [42]. MedRec makes it simple for patients to access their medical records across providers and treatment venues. Another startup company Carechain initiated a blockchain-based personal healthcare data management system that intends to focus on the protocol level and create a new infrastructure that no one owns, but everyone can control [43]. The Carechain adopted the Ethereum approach with the aim of creating a national blockchain for health data where the system allows individuals ownership and control over their own health information [44]. The system was designed to assign a universal digital ID owned and controlled by the individual in order to put the individual at the center.

CHAPTER IV

PROPOSED EHR SYSTEMS

4.1 System Overview

We propose research into the establishment of a decentralized, peer-to-peer network of participants wherein transactions are recorded on a shared distributed ledger for the purpose of patient data management and secure accessibility. Participants in the network would govern and agree by consensus on the updates to the records in the ledger. Also, every record would contain a timestamp and unique cryptographic signature. As a result, the ledger becomes an auditable, immutable record of all network transactions to ensure data security and integrity, while allowing the choice for patients and providers to access the data anytime and anywhere.

4.1.1 System Architecture

Our primary goal is to demonstrate the structure of both blockchain-based frameworks for telehealth and healthcare-based application. As part of our scratch, we develop two different prototypes to furnish a clear visualization of the proposed blockchain-oriented healthcare application. We adopt both Hyperledger Fabric and Ethereum frameworks towards a better understanding of how the system mechanism shall function within different blockchain environments. The developed prototype comprises (i) a secure Application Programming Interface (API) that meets the criteria of the Office of the National Coordinator for Health Information Technology's (ONC) requirements for facilitating easy access, sharing, and use of patient Electronic Health Records, (ii) Ethereum based EHR data repository, and Hyperledger Fabric based EHR data repository. For demonstration purposes, we focus on Electronic Health Records (EMR) that shall be created in a secure data repository to enable secure upload, storage, analysis, retrieval, and transmit patient data according to the patient's instructions, or distribution when and where it is needed.

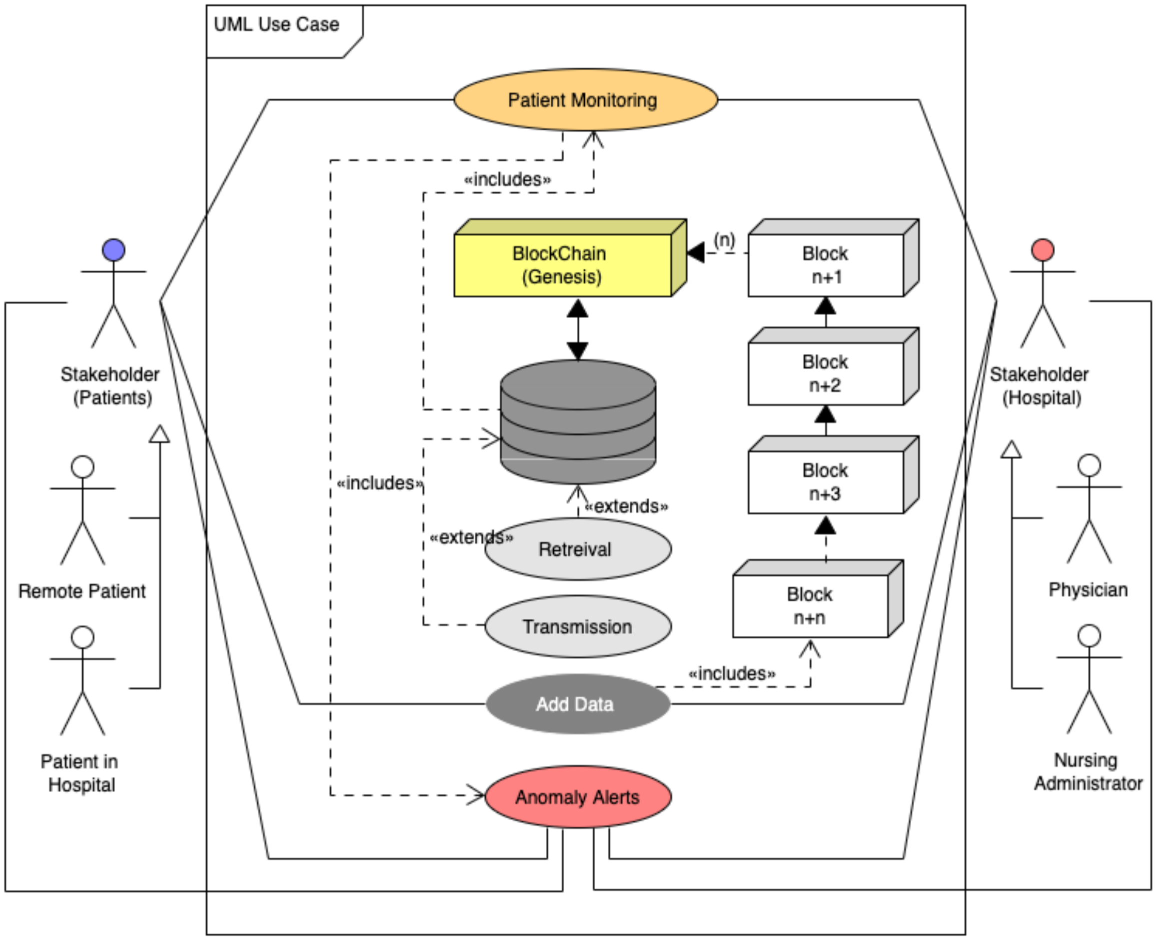


Figure 4: UML Use Case for Blockchain-Based Health Application

We followed a variety of guidelines from different organizations and approaches, and ONC and software engineering practices are included. In accordance with SE, we analyze the existing problem, elicit the requirements and identify the research questions by adopting the most suitable standards of Agile methodology in the blockchain. We develop a UML use case (80%) to scratch down the sequence of actions towards identifying objects and constituting a complete task or transaction in the proposed application during requirements analysis or creation process for current research. The use case initializes as a way to capture the main functional goals, and the motivation of laying the architectural foundation for a system, as a result, facilitating requirement coverage [45]. We display four types of stakeholders including (i) hospitals and (ii) Patients in the use case depicted in Figure 4. The use case also illustrates scores of functions; for instance, patient monitoring and anomaly alert which shall extend in continuous research.

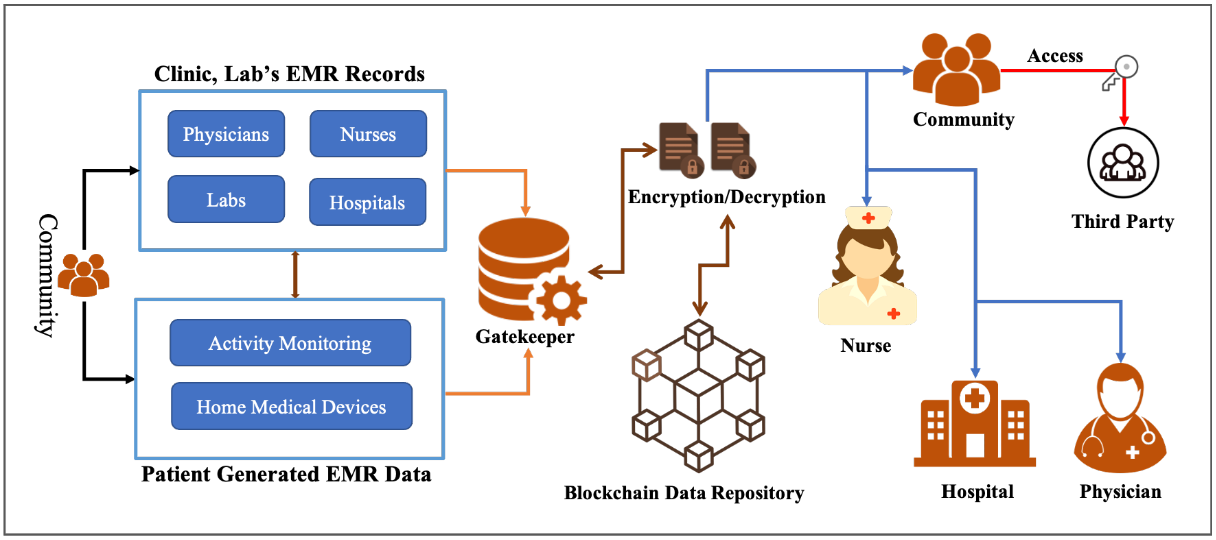


Figure 5: A low-level architecture of proposed application

We carried out a low-level architecture for a better understanding of the design of the proposed system where we present the overall flow of the application consisting of four entities. The data shall be collected from the residents either remotely or through home healthcare and shall be stored in a decentralized blockchain database. Each data shall be linked with a unique and unchangeable hash and timestamp and shall allow the assigned stakeholders the retrieval and transmission stored data using the designed API. An overview of the proposed system illustrates in Figure 5.

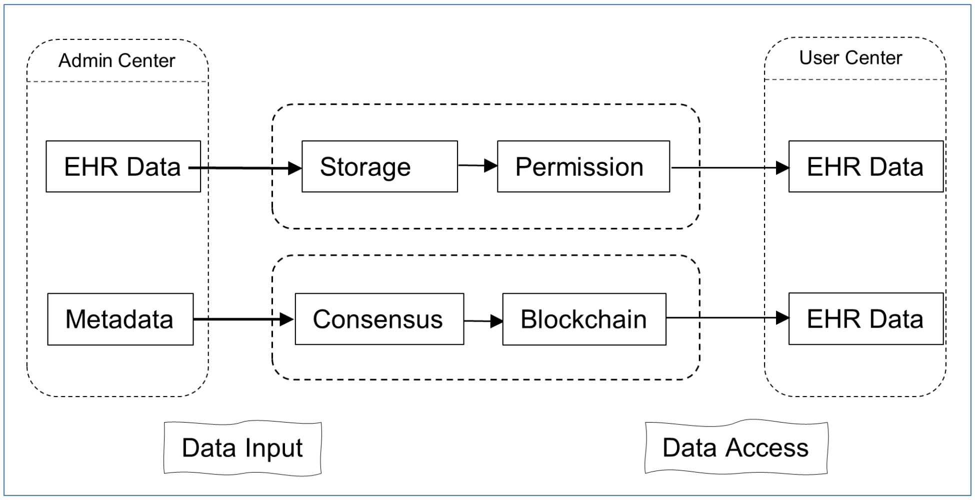


Figure 6: An overview of metadata of blockchain network

Users engage with the proposed platform using a simple online interface in which the metadata has been segregated yet tied together by a unique identifier, resulting in a metadata duple being considered an experiment with a name and an identity. The system will validate metadata by the consensus algorithm that operates among peers within the consortium, as illustrates in Figure 6. Once the metadata is verified by consensus, the metadata is merged into one block and attached to the screwless ledger, which consists of block-shaped metadata entries. The metadata shall be stored as an object with a timestamp. The peers within a consortium shall allow to search and retrieve the metadata and only be allowed to access that user has permissions. Each block of the proposed system is chained together in an append-only structure using a cryptographic hash function. As a result, altering and erasing recently affirmed data is impossible resulting in new data being appended in the form of additional blocks chained with earlier blocks. Meaning that updating data of one of the transacted blocks shall generate a different hash value and different link relation towards accomplishing immutability and security.

4.2 System Entities

The proposed system consists of two major modules, organizational and patient. The organizational section enables access to the permissioned stakeholders for adding, updating, retrieving, and monitoring EHR data information while the second modules allow patients and assigned representatives to access and update certain EHR records. The system was initially developed as a web application that may be extended to mobile applications in future research.

4.2.1 Blockchain Networks

Blockchain network is one of the primary components of the proposed framework intended to store Electronic Health Records (EHR) in a secure decentralized location. Stored EHR data with timestamp and hash shall be generated in the network. The network consists of two types of primary stakeholders responsible to add, update, retrieve data in a blockchain network.

4.2.2 Cloud Database

We utilize a cloud-based platform named Etherscan for Ethereum framework, which is a decentralized smart contracts platform suitable for Ethereum. Etherscan allows the users to look up, confirm and validate transaction histories including token transfer and contract execution on the Ethereum decentralized smart contracts platform. Stored data on the cloud can be remotely accessed by permissioned stakeholders from anywhere using the internet. Besides, we utilize localhost-based platform for Hyperledger Fabric framework.

4.2.3 Healthcare Stakeholders

Blockchain can facilitate healthcare stakeholders including physicians, nurses, and patients in different forms. The proposed system enables said authorized stakeholders to access the network which can help to reduce the complexity and security issues.

4.3 Ethereum-based EHR Framework

We adopt Etherscan which is a block explorer for the proposed platform for discovering, verifying, and approving transactions that occur on the Ethereum blockchain. We utilize the API service of Etherscan for developing a decentralized network. Etherscan store data as hash (TxHash) into the block along with the timestamp of real-time based confirmed transaction and its fees. To develop the smart contracts, we utilize Solidity programming language while Visual Studio Code as Integrated Development Environment (IDE) comprising extensions for Solidity development. We initiate our application by connecting with the Ethereum network and Etherscan wallet. We then deploy the smart contract on the Ethereum test network and test with a transaction. The smart contract needs to push live on the blockchain network after the test execution by utilizing the deploy method.

4.3.1 EHR-based Application Prototype

After contriving an initial prototype, we generally validate it through experimental simulation approaches. The test environment, observation points, transaction characteristics, workloads, and network size are all important factors to consider when creating a blockchain evaluation. These features should be included in the evaluation findings since revealing them makes it easier to evaluate performance across platforms.

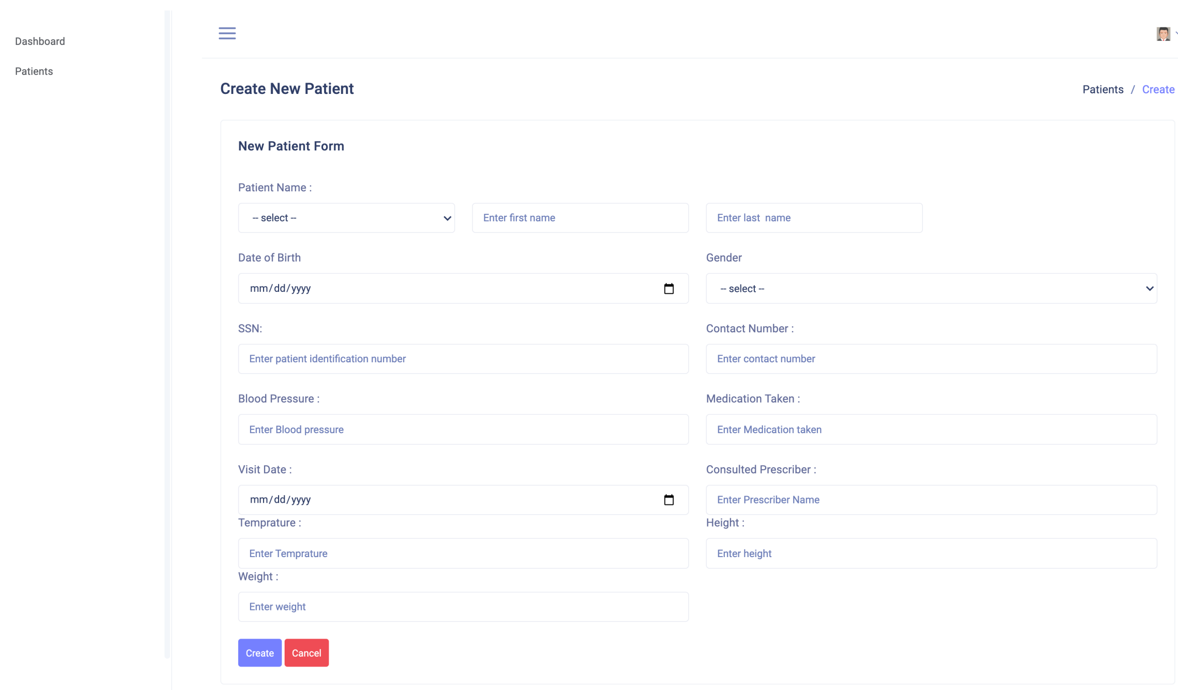
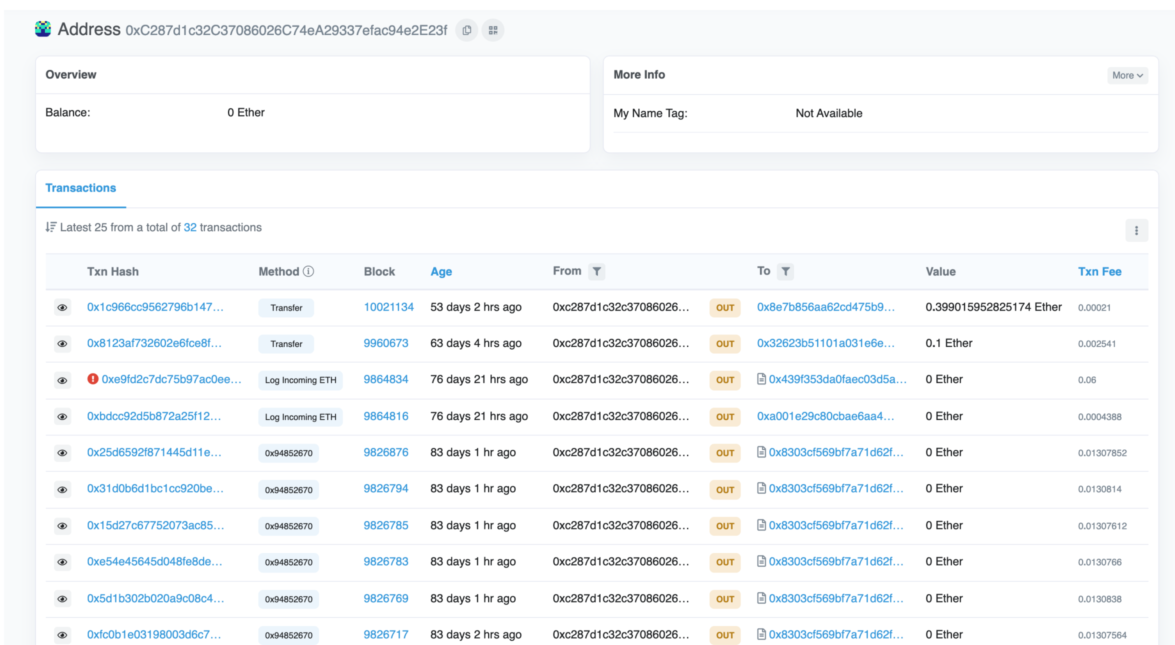


Figure 7: Depicts a form to create patient data

ID	Name	Date of Birth	Gender	SSN	Blood Pressure	Medication Taken	Visit Date	Consulted Prescriber	Temprature	Height	Weight	Contact No
1	Abdur Rahim	1977-01-03	Male	456	A+	N/A	2021-01-07	Dr. Ali	99	5	69	6014373678
2	Sharon Glassgow	1969-06-22	Female	8901	B+	N/A	2021-02-28	Dr. Robert	101	5	83	8092942495
3	Harry Dorvili	1999-11-11	Male	111111	B	N/A	2020-11-11	AAA	98	6	76	1232332411
4	Erjola Salmorin	1988-09-22	Female	8860	B+	Paracetamol	2020-10-20	Dr. Mai	100	5	66	9294567890
5	riya arya	1996-12-06	Female	463634	110	paracetamol	2021-11-04	dr. singh	99	160	56	9604792966
6	raghu veer	1998-02-02	Male	56465	110	covidsil-19	2021-03-16	dr. henary	97	185	86	9604792946
7	Mohammad Hasan	1989-03-13	Male	3456	B	N/A	2021-03-11	Dr. Ahmad	98	6	66	9234567890
8	Abdur Shah	1977-01-03	Male	4567	A+	N/A	2021-01-09	Dr. Ali	99	6	69	6014714678
9	rocky jangir	1976-08-12	Male	5343	125	covidsil	2021-02-04	dr. paul	99	185	86	9604792946
10	kamlesh arya	1998-09-02	Male	123	120	dolo 650	2021-02-10	Dr. Rajveer	97	185	86	9604792946

Figure 8: An interface for accessing stored data using API



	Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
	0x1c966cc9562796b147…	Transfer	10021134	53 days 2 hrs ago	0xc287d1c32c37086026…	OUT	0x8e7b856aa62cd475b9…	0.399015952825174 Ether	0.00021
	0x8123af732602e6fce8f…	Transfer	9960673	63 days 4 hrs ago	0xc287d1c32c37086026…	OUT	0x32623b51101a031e6e…	0.1 Ether	0.002541
	0xe9fd2c7dc75b97ac0ee…	Log Incoming ETH	9864834	76 days 21 hrs ago	0xc287d1c32c37086026…	OUT	0x439f353da0faec03d5a…	0 Ether	0.06
	0xbdcc92d5b872a25f12…	Log Incoming ETH	9864816	76 days 21 hrs ago	0xc287d1c32c37086026…	OUT	0xa001e29c80cbae6aa4…	0 Ether	0.0004388
	0x25d6592f871445d11e…	0x94852670	9826876	83 days 1 hr ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.01307852
	0x31d0b6d1bc1cc920be…	0x94852670	9826794	83 days 1 hr ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.0130814
	0x15d27c67752073ac85…	0x94852670	9826785	83 days 1 hr ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.01307612
	0xe54e45645d048fe8de…	0x94852670	9826783	83 days 1 hr ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.0130766
	0x5d1b302b020a9c08c4…	0x94852670	9826769	83 days 1 hr ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.0130838
	0xfc0b1e03198003d6c7…	0x94852670	9826717	83 days 2 hrs ago	0xc287d1c32c37086026…	OUT	0x8303cf569bf7a71d62f…	0 Ether	0.01307564

Figure 9: Stored data saved in Ethereum-Based Blockchain Network

In Figure 7, an API is depicted where stakeholders can create new patients' profiles by filling out the preset form. Once submitted, the EMR data shall transact to the blockchain storage, details shown in Figure 8. Each EMR data consists of a unique hash and timestamp and the stored data is accessible using the authorized API, in Figure 9.

4.4 Hyperledger Fabric-based EHR Framework

We also develop another prototype for an EHR-based application using the Hyperledger Fabric framework. In the first step, we develop a Hyperledger Fabric network infrastructure where we define relevant stakeholders or network participants within distributed nodes or peers. We create keys, secure identities, and roles. We then develop Chaincode which is equivalent to smart contracts. We use Golang (Go) programming language to develop the system and user chaincode within fabric API. We then define permissions and access rules for the participants. Hyperledger data is pulled from the communication with the developed web application and Hyperledger blockchain server. We develop an ExpresJS server API for communication between web applications and the Hyperledger server. After developing all the components and modules, we test our Hyperledger Fabric network.

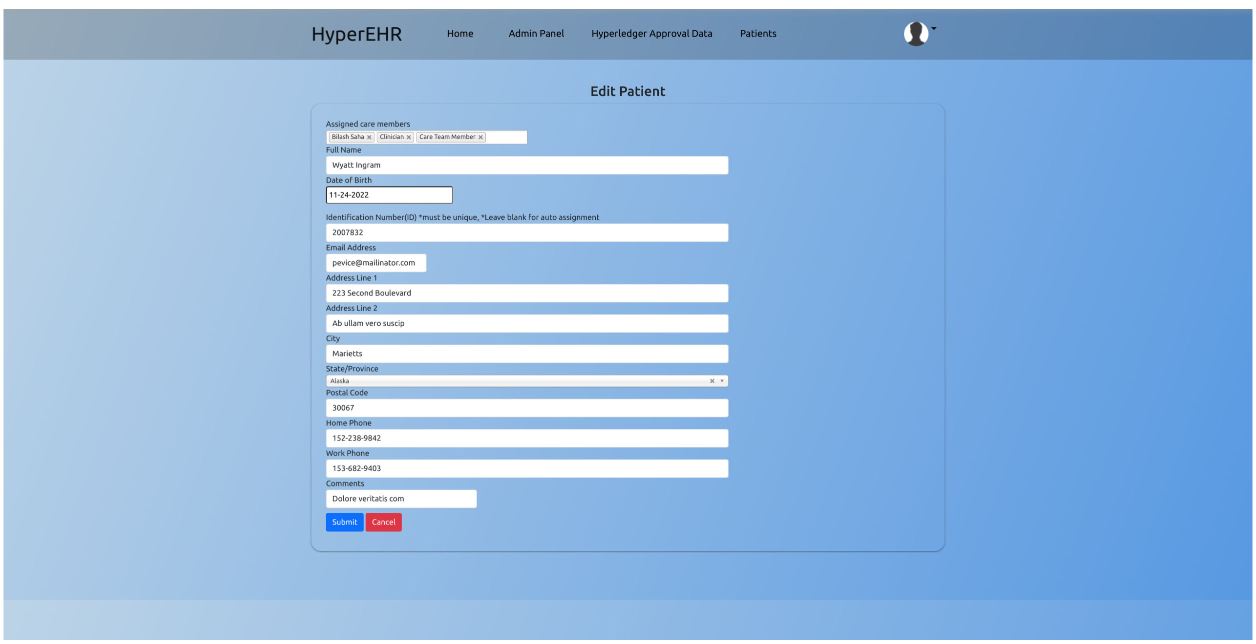


Figure 10: API for patient data (create and update)

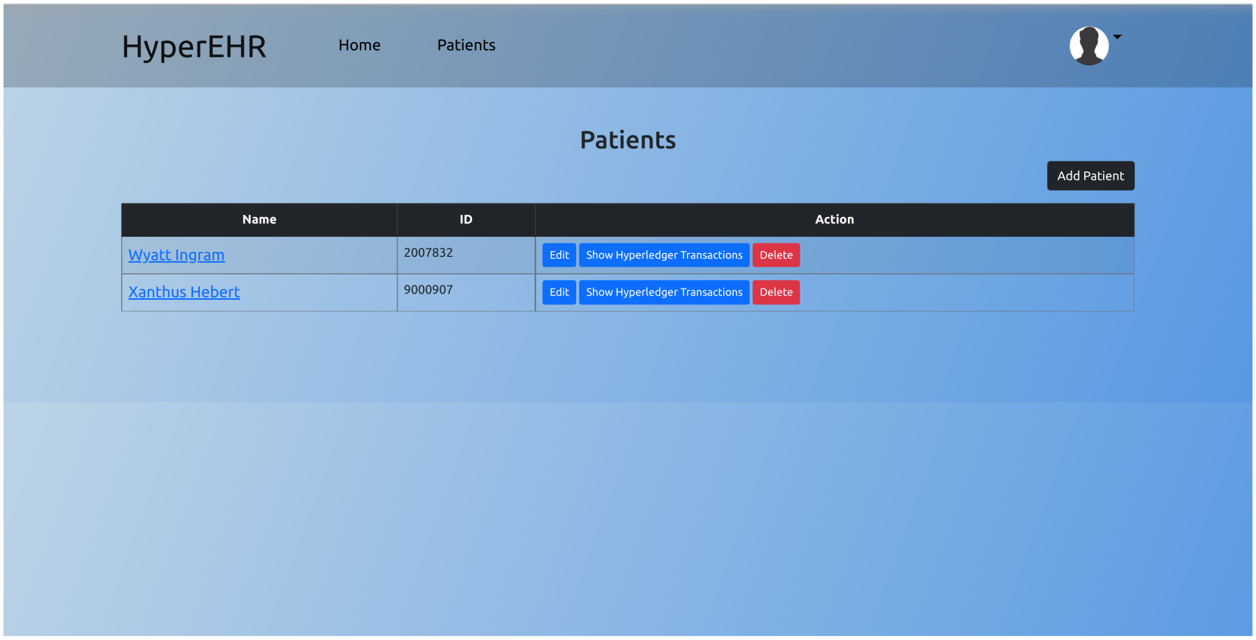


Figure 11: API for displaying the list of patients with unique id

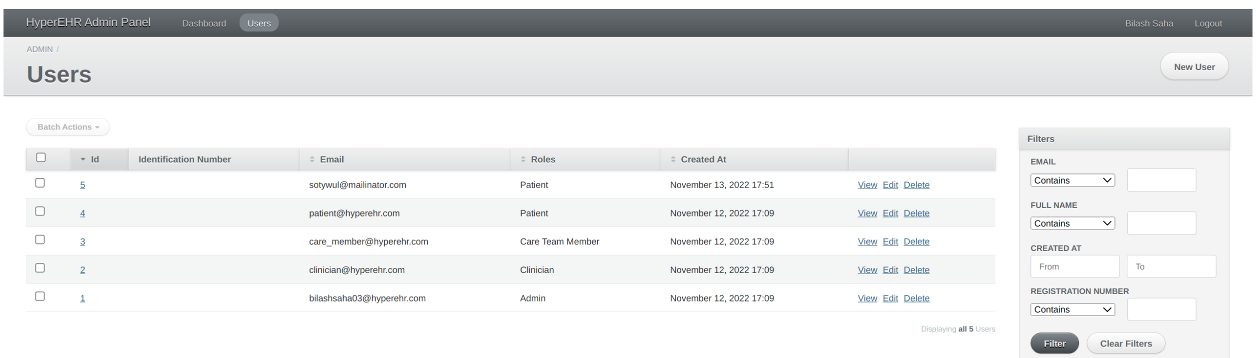


Figure 12: Illustrates the admin panel to manage the Hyperledger system

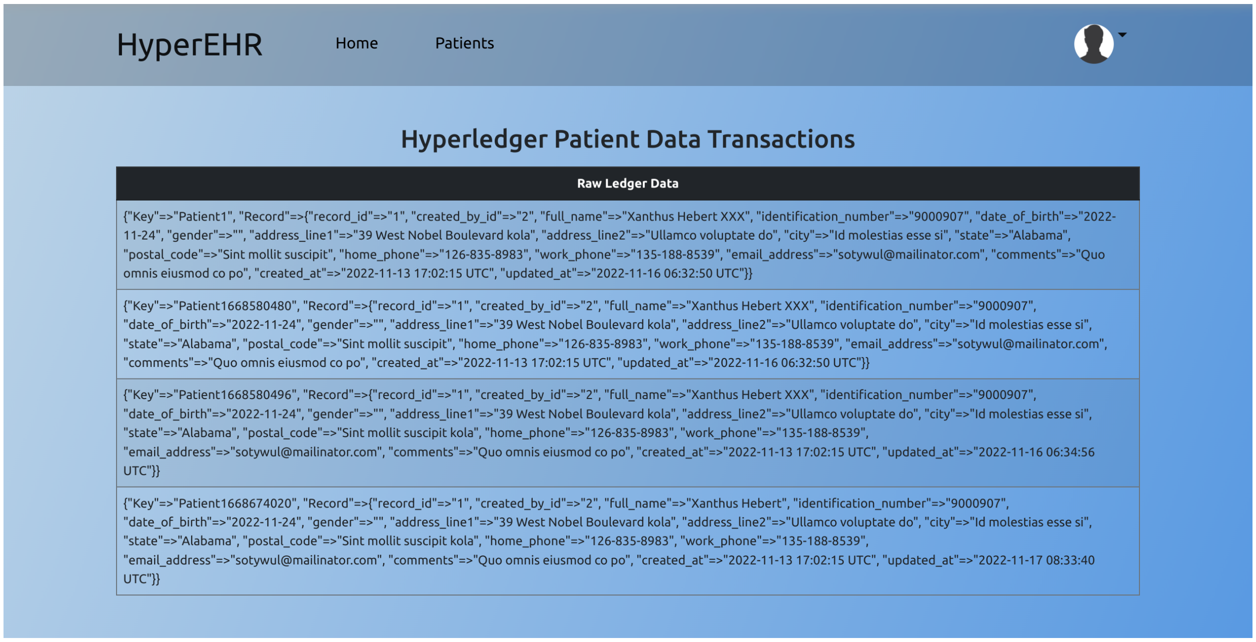


Figure 13: Display the records of data transactions of Hyperledger Network

Figure 10 illustrates a restful API for patient data that allow permissioned users to create and update health records. Figure 11 display the API that allows authorized users to access the list of patients with unique ids. Figure 12 depicts the admin panel where the system enables the admin to manage the Hyperledger system. Lastly, Figure 13 illustrates the patient data transactions record within Hyperledger Fabric networks.

CHAPTER V

COMPARATIVE STUDY AND DISCUSSION

5.1 Analogy Between Hyperledger Fabric and Ethereum

The Linux Foundation hosts Hyperledger Fabric, one of the most prominent blockchain frameworks. It provides plug-and-play components, such as consensus and membership services, as the basis for a solution with a modular architecture. Ethereum, on the other hand, is a decentralized platform that allows smart contracts and apps to execute without the risk of downtime, censorship, fraud, or third-party interference [46]. Hyperledger Fabric intends to provide a Business-to-Business (B2B) platform with a modular and extendable architecture that can be used in a variety of industries, ranging from banking and healthcare to supply chains. However, Ethereum is mostly Business-to-Commerce (B2C) that advertises itself as agnostic to any given field of application [47]. An analogical summary is given in Table I.

Table 1: Analogical illustration between Hyperledger Fabric and Ethereum

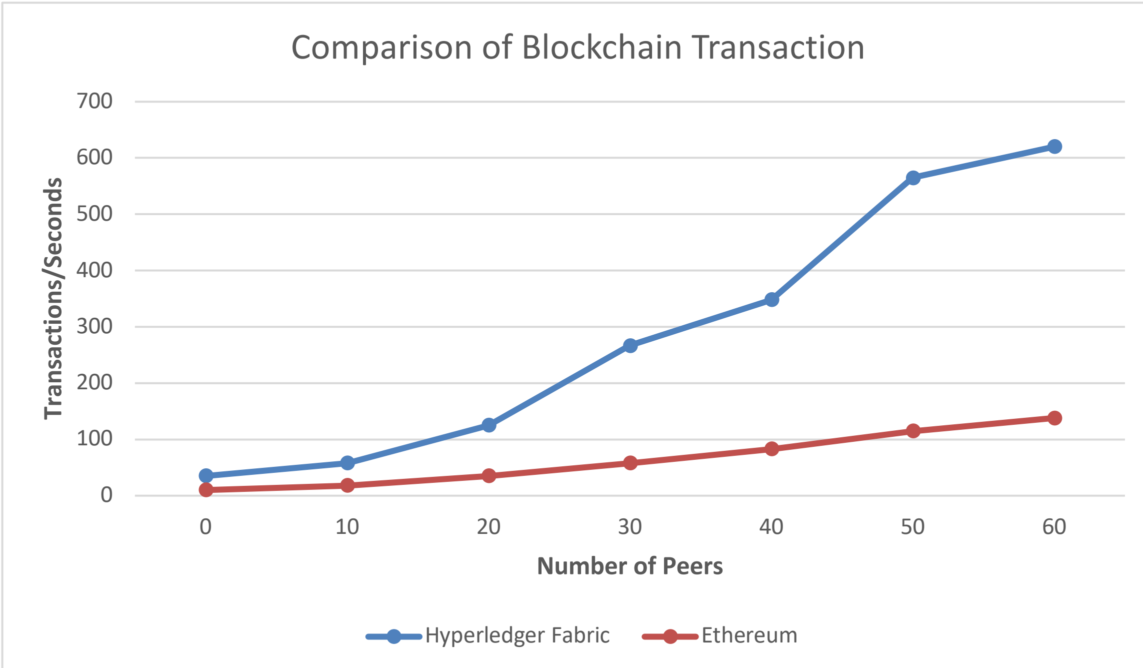
Category	Hyperledger Fabric	Ethereum
Purpose and Confidentiality	Hyperledger Fabric is designed for B2B businesses with Confidential transactions	Ethereum is designed for B2C businesses and generalized applications with transparent transaction
Modularity and Extendibility	Hyperledger Fabric is a flexible and extendable architecture that may be used in a variety of enterprise settings	For Modularity and Extendibility, different approaches need to be adopted for Ethereum
Cost-Effective	Hyperledger Fabric is a native platform that enables the creation of a self-contained private ledger and contract management without the use of fees.	Ethereum based blockchains network require a fee for each transaction
Scalability	Hyperledger Fabric allows more scalability when organizations are added or removed from a channel	Ethereum's scalability bottleneck is notable since each node in the network has to process each transaction
Plug and Play API	Hyperledger Fabric provides SDKs in Node.js and Go that can be used to interact with the blockchain efficiently	Ethereum's plug-and-play modularity allows you to customize privacy and permissions on a single platform
Consensus	Hyperledger Fabric consists of different phases of checking consensus and all	Proof-of-work (PoW) is a consensus protocol that allows the Ethereum

	peers on the network do not have to come to some agreement before a transaction is successful	network's nodes to agree on the state of all information recorded on the Ethereum blockchain
Security and Privacy	Fabric is a permission network, all nodes participating in the Modular Membership Provider provides an identity to everyone in the network (MSP)	Although Ethereum employs transparency as part of its security, there are concerns about data vulnerability
Transaction Speed	Hyperledger Fabric's transaction speed capacity vary from 3000 transactions per second to 20000 which is impressive	Ethereum network can only support approximately 30 transactions per second which are quite narrow as of today

Both Ethereum and Hyperledger come with their unique advantages for different business scenarios and challenges. However, based on our extensive investigation, we conclude that Ethereum serves well for public applications; Hyperledger's capabilities seem more appealing in enterprise-based blockchain development. Therefore, Hyperledger Fabric shall be adopted for healthcare-based applications due to its suitability for managing health records compared to Ethereum. Hyperledger provides highly flexible, scalable and confidential infrastructure solutions with explicit anonymity and transaction privacy [20].

5.1.1 Performance in Blockchain Frameworks

Performance evaluation of blockchain platforms is crucial due to the novelty of this technology and provides a better understanding of the blockchain community. For instance, consensus or smart contracts algorithms and proof work (PoW) concepts are novel approaches and understanding the performance of these algorithms is a demand. We utilize various parameters including analytical modeling for measuring the performance of blockchain framework. Considering the number of transactions, Hyperledger Fabric outperformed Ethereum. Besides, scalability in multiple peer networks proved Hyperledger Fabric's superiority over Ehtereum where Hyperledger's latency, average throughput, and execution time is more efficient than Ethereum.



Some research reported that Ethereum's blockchain supports 15-30 transactions per second while Hyperledger Fabric supports thousands of transactions per second with a latency of less than one second. Figure 10 indicates the average transaction in Hyperledger Fabric and Ethereum in different transactions.

5.1.2 Privacy in Blockchain Frameworks

In this research, one of the goals is to analyze the privacy and scalability of blockchain frameworks. Ensuring the privacy aspects in software applications is necessary, particularly in systems containing sensitive data including electronic health records (EHR). In the proposed system, we consider evaluating the application to measure privacy level. Both Ethereum and Hyperledger Fabric comprise strong privacy in terms of data sharing. However, we identified Hyperledger Fabric as more privacy-protected due to the private nature of architecture that protects users' privacy in both data storage and sharing. Privacy-preserving schemes and privacy protection mechanisms in the blockchain are strong compared to conventional database systems. Introduced systems authenticate the identity of stakeholders to allow participation in the network. Thus, both blockchain frameworks offer certain privacy protection; however, Hyperledger Fabric meets the necessary privacy-preserving mechanisms to ensure data integrity and protection.

5.1.3 Security in Blockchain Frameworks

Analyzing aspects of security in the blockchain framework is our motivation in this research. We analyze four types of blockchain components including chaincode or smart contracts, consensus, privacy mechanism, and network to define possible risks and flaws. Consensus protocols in Hyperledger Fabric enhance the trust within the network. We tested out the system using a solo protocol to find single-point-of-failure that indicates strong privacy settings in blockchain networks. Although there are records of consensus-oriented attacks, certain protocols can mitigate such flaws in the network. Similarly, smart contracts are prone to program errors while the code can be manipulated by malicious programmers. We evaluated ledgers including random key generation, concurrency, and query risks where we identify strong protection in blockchain networks. However, certain vulnerabilities can be employed including chaincode, and execution tools.

5.2 Discussion

In this study, we developed Hyperledger Fabric and Ethereum-based system that has competency in storing electronic health records (EHR) within secure and immutable blockchain networks. System demonstration indicates that the prototype allows the permissioned stakeholders to add, update, and retrieve EHR data on a RESTful API environment. Our comparative study on Hyperledger Fabric and Ethereum from performance, privacy, and security perspective indicates the key differences between both blockchain frameworks. The demonstration indicates a positive result in both Hyperledger and Ethereum-based healthcare and telehealth data management. This research shall not only help the blockchain community but also broader stakeholders in general.

CHAPTER VI

CONCLUSION

Blockchain is emerged to solve issues people are going through for conventional databases and related existing problems. In this research, we developed two separate electronic health records (EHR) systems by adopting two widely used blockchain frameworks, Ethereum and Hyperledger Fabric. Based on our development experience, we carried out a comparative study to evaluate both frameworks from the performance, privacy, and security lens. After analysis of the introduced systems, we advocate adopting Hyperledger Fabric because of its unique and novel architectural model including private and consortium networks. According to our findings, Hyperledger Fabric offers unique privacy-preserving schemes and security protection features that can protect electronic health data to store and share EHR data seamlessly. In future studies, we aim to extend our study to evaluate the development perspective of blockchain-based applications from software engineering perspective and to highlight the way to improve current SE practices in future studies.

BIBLIOGRAPHY

[1] H. Thimbleby, “Technology and the future of healthcare,” *J. Public health Res.*, vol. 2, no. 3, pp. e28–e28, Dec. 2013, doi: 10.4081/jphr.2013.e28.

[2] S. Gonzales, M. Ramirez, and B. Sawyer, “How does U.S. life expectancy compare to other countries?,” *Heal. Syst. Tracker*, 2019, [Online]. Available: https://www.healthsystemtracker.org/chart-collection/u-s-life-expectancy-compare-countries/#item-start.

[3] U. Aickelin, W. W. Chapman, and G. K. Hart, “Health Informatics—Ambitions and Purpose,” *Front. Digit. Heal.*, vol. 1, 2019, doi: 10.3389/fdgth.2019.00002.

[4] M. Imhoff, A. Webb, and A. Goldschmidt on behalf of the ESICM, “Health informatics,” *Intensive Care Med.*, vol. 27, no. 1, pp. 179–186, Jan. 2001, doi: 10.1007/PL00020869.

[5] H. A. Aziz, “Health Informatics – Introduction,” *Am. Soc. Clin. Lab. Sci.*, vol. 28, no. 4, pp. 238–239, 2015, doi: 10.29074/ascls.28.4.238.

[6] R. S. Evans, “Electronic Health Records: Then, Now, and in the Future,” *Yearb. Med. Inform.*, pp. S48–S61, 2016, doi: 10.15265/IYS-2016-s006.

[7] P. C. McMullen *et al.*, “Electronic Medical Records and Electronic Health Records: Overview for Nurse Practitioners,” *J. Nurse Pract.*, vol. 10, no. 9, pp. 660–665, Oct. 2014, doi: 10.1016/j.nurpra.2014.07.013.

[8] C. Camara, P. Peris-Lopez, and J. E. Tapiador, “Security and privacy issues in implantable medical devices: A comprehensive survey,” *J. Biomed. Inform.*, vol. 55, pp. 272–289, 2015, doi: 10.1016/j.jbi.2015.04.007.

[9] T. Kitsantas, A. Vazakidis, and E. Chytis, “A Review of Blockchain Technology and Its Applications in the Business Environment,” *Conf. Pap.*, no. October, 2019, [Online]. Available: https://www.researchgate.net/publication/334615432.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[11] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, “The role of blockchain technology in telehealth and telemedicine,” *Int. J. Med. Inform.*, vol. 148, 2021, doi: 10.1016/j.ijmedinf.2021.104399.

[12] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,” *Cryptography*, vol. 3, no. 1, pp. 1–16, 2019, doi: 10.3390/cryptography3010003.

[13] Shivani & Neelam, “How to avoid data tampering using blockchain technology,” [Online]. Available: https://www.cisin.com/coffee-break/technology/how-to-avoid-data-tampering-using-blockchain-technology.html.

[14] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, “Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring,” *Proc. - 2021 IEEE Int. Conf. Digit. Heal. ICDH 2021*, pp. 299–308, 2021, doi: 10.1109/ICDH52753.2021.00054.

[15] M. J. Hossain Faruk, S. Hossain, and M. Valero, “EHR Data Management: Hyperledger Fabric-based Health Data Storing and Sharing,” *Fall 2021 Symp. Student Sch.*, 2021, doi: 10.13140/RG.2.2.20299.05928.

[16] J. Peral, E. Gallego, D. Gil, M. Tanniru, and P. Khambekar, “Using visualization to build transparency in a healthcare blockchain application,” *Sustain.*, vol. 12, no. 17, 2020, doi: 10.3390/SU12176768.

[17] M. Crosby, P. P. Nachiappan, S. Verma, and V. Kalyanaraman, “BlockChain TechnologyBeyond

Bitcoin," *Sutardja Cent. Entrep. Technol. Tech. Rep.*, 2015, [Online]. Available: scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

[18] OECD, "OECD Blockchain Primer," *Oecd*, p. 12, 2018, [Online]. Available: http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf.

[19] G. Leeming, J. Cunningham, and J. Ainsworth, "A Ledger of Me: Personalizing Healthcare Using Blockchain Technology," *Front. Med.*, vol. 6, 2019, doi: 10.3389/fmed.2019.00171.

[20] E. Elrom and E. Elrom, "An Introduction to Hyperledger," *Blockchain Dev.*, pp. 299–348, 2019.

[21] A. S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 288–297, 2018, doi: 10.1016/j.csbj.2018.08.002.

[22] Hyperledger Foundation, "Hyperledger Fabric Docs: Peers," [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/peers/peers.html.

[23] Hyperledger Foundation, "A Blockchain Platform for the Enterprise," *Hyperledger Docs*, 2018, [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/.

[24] H. Performance, The Hyperledger White Paper Working Group, and H. Performance, "Hyperledger Blockchain Performance Metrics," *Hyperledger.org*, pp. 1–17, 2018, [Online]. Available: https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg.

[25] G. W. et Al., "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Proj. yellow Pap.*, vol. 151, pp. 1–32, 2014.

[26] S. Peyrott, "An Introduction to Ethereum and Smart Contracts," p. 68, 2017, [Online]. Available: https://auth0.com/e-books/intro-to-ethereum.

[27] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101966.

[28] D. Vujičić, D. Jagodic, and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," 2018, pp. 1–6, doi: 10.1109/INFOTEH.2018.8345547.

[29] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, "Block chain Technology in Healthcare," *Int. J. Adv. Sci. Res. Eng.*, vol. 4, no. 5, pp. 154–159, 2018, doi: 10.31695/IJASRE.2018.32723.

[30] A. Tandon, A. Dhir, N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, 2020, doi: 10.1016/j.compind.2020.103290.

[31] M. Gaynor, J. Tuttle-Newhall, J. Parker, A. Patel, and C. Tang, "Adoption of Blockchain in Health Care," *J. Med. Internet Res.*, vol. 22, no. 9, p. e17423, Sep. 2020, doi: 10.2196/17423.

[32] Hyperledger, "Hyperledger-Powered Healthcare Solutions in Action," *Hyperledger*. https://www.hyperledger.org/tag/healthcare.

[33] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, 2019, doi: 10.3390/app9091736.

[34] S. Yaqoob *et al.*, "Use of blockchain in healthcare: A systematic literature review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 644–653, 2019, doi: 10.14569/ijacsa.2019.0100581.

[35] H. Yu, H. Sun, D. Wu, and T. T. Kuo, "Comparison of Smart Contract Blockchains for Healthcare Applications," *AMIA ... Annu. Symp. proceedings. AMIA Symp.*, vol. 2019, pp. 1266–1275, 2019.

[36] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain Res. Appl.*, vol. 2, no. 1, 2021, doi: 10.1016/j.bcra.2021.100012.

[37] A. Dubovitskaya *et al.*, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, 2020, doi: 10.2196/13598.

[38] T. Smith *et al.*, “Blockchain to blockchains in life sciences and health care,” *TechTrends*, p. 9, 2018, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-tech-trends2-blockchain.pdf%0Ahttp://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf.

[39] J. Prisco, “The Blockchain for healthcare: Gem launches Gem Health Network with Philips Blockchain Lab,” *Bitcoin Mag.*, 2016.

[40] L. A. Ekblaw A, Azaria A, Halamka JD, “MedRec: A Case Study for Blockchain in Healthcare — MIT Digital Currency Initiative,” [Online]. Available: https://dci.mit.edu/research/blockchain-medical-records.

[41] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[42] MedRec MIT, “MedRec Technical Website,” [Online]. Available: https://medrec.media.mit.edu/technical/.

[43] Bitcoin Exchange Guide News Team, “CareChain: Blockchain Personal Healthcare Data Management System?,” *Btcoin Exch. Guid.*, 2018, [Online]. Available: https://bitcoinexchangeguide.com/carechain/.

[44] J. Sellström, “Care Chain The Infrastructure Consortium,” *Infrastruct. Consort.*, 2018, [Online]. Available: https://www.academia.edu/36347853/Care_Chain_The_Infrastructure_Consortium?

[45] B. Dobing and J. Parsons, “Understanding the role of use cases in UML: A review and research agenda,” *J. Database Manag.*, vol. 11, no. 4, pp. 28–36, 2000, [Online]. Available: http://proquest.umi.com/pqdweb?did=126518971&Fmt=7&clientId=12010&RQT=309&VName=PQD.

[46] A. V. Aswin and B. Kuriakose, “An Analogical Study of Hyperledger Fabric and Ethereum,” *Lect. Notes Data Eng. Commun. Technol.*, vol. 33, pp. 412–420, 2020, doi: 10.1007/978-3-030-28364-3_41.

[47] M. Valenta and P. Sandner, “Comparison of Ethereum, Hyperledger Fabric and Corda,” *Frankfurt Sch. Blockchain Cent.*, no. June, p. 8, 2017, [Online]. Available: www.fs-blockchain.decontact@fs-blockchain.dewww.twitter.com/fsblockchainwww.facebook.de/fsblockchain%0Ahttps://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6.

APENDIX

Example of Scripts of developed blockchain network.

```
package main
import (
    "encoding/json"
    "fmt"
    "strconv"
    "github.com/hyperledger/fabric-contract-api-go/contractapi"
)

// SmartContract provides functions for managing a patient
type SmartContract struct {
    contractapi.Contract
}

// Patient describes basic details of what makes up a patient
type Patient struct {
    RecordId  string `json:"record_id"`
    CreatedById   string `json:"created_by_id"`
    FullName  string `json:"full_name"`
    IdentificationNumber string `json:"identification_number"`
    DateOfBirth  string `json:"date_of_birth"`
    Gender  string `json:"gender"`
    AddressLine1  string `json:"address_line1"`
    AddressLine2  string `json:"address_line2"`
    City  string `json:"city"`
    State  string `json:"state"`
    PostalCode  string `json:"postal_code"`
    HomePhone  string `json:"home_phone"`
    WorkPhone  string `json:"work_phone"`
    EmailAddress  string `json:"email_address"`
    Comments  string `json:"comments"`
    CreatedAt  string `json:"created_at"`
    UpdatedAt  string `json:"updated_at"`
}

// QueryResult structure used for handling result of query
type QueryResult struct {
    Key    string `json:"Key"`
    Record *Patient
}

// InitLedger adds a base set of patients to the ledger
```

```
func (s *SmartContract) InitLedger(ctx contractapi.TransactionContextInterface) error
{
    patients := []Patient{
        Patient{RecordId:  "Init", CreatedById:  "Init", FullName:  "Init",
IdentificationNumber:  "Init", DateOfBirth:  "Init", Gender:  "Init", AddressLine1:
"Init", AddressLine2:  "Init", City:  "Init", State:  "Init", PostalCode:  "Init",
HomePhone:  "Init", WorkPhone:  "Init", EmailAddress:  "Init", Comments:  "Init",
CreatedAt:  "Init", UpdatedAt:  "Init"},
    }

    for i, patient := range patients {
        patientAsBytes, _ := json.Marshal(patient)
        err := ctx.GetStub().PutState("Patient"+strconv.Itoa(i), patientAsBytes)
        if err != nil {
            return fmt.Errorf("Failed to put to world state. %s", err.Error())
        }
    }

    return nil
}

// CreatePatient adds a new patient to the world state with given details
func (s *SmartContract) CreatePatient(ctx contractapi.TransactionContextInterface,
patientNumber string, record_id string, created_by_id string, full_name string,
identification_number string, date_of_birth string, gender string, address_line1
string, address_line2 string, city string, state string, postal_code string,
home_phone string, work_phone string, email_address string, comments string,
created_at string, updated_at string) error {
    patient := Patient{
        RecordId:  record_id,
        CreatedById:  created_by_id,
        FullName:  full_name,
        IdentificationNumber:  identification_number,
        DateOfBirth:  date_of_birth,
        Gender:  gender,
        AddressLine1:  address_line1,
        AddressLine2:  address_line2,
        City:  city,
        State:  state,
        PostalCode:  postal_code,
        HomePhone:  home_phone,
        WorkPhone:  work_phone,
        EmailAddress:  email_address,
        Comments:  comments,
        CreatedAt:  created_at,
        UpdatedAt:  updated_at,
    }
```

```go
    patientAsBytes, _ := json.Marshal(patient)
    return ctx.GetStub().PutState(patientNumber, patientAsBytes)
}

// QueryAllPatients returns all patients found in world state
func (s *SmartContract) QueryAllPatients(ctx contractapi.TransactionContextInterface)
([]QueryResult, error) {
    startKey := "Patient0"
    endKey := "Patient99"

    resultsIterator, err := ctx.GetStub().GetStateByRange(startKey, endKey)
    if err != nil {
        return nil, err
    }
    defer resultsIterator.Close()
    results := []QueryResult{}

    for resultsIterator.HasNext() {
        queryResponse, err := resultsIterator.Next()
        if err != nil {
            return nil, err
        }
        patient := new(Patient)
        _ = json.Unmarshal(queryResponse.Value, patient)
        queryResult := QueryResult{Key: queryResponse.Key, Record: patient}
        results = append(results, queryResult)
    }
    return results, nil
}

func main() {

    chaincode, err := contractapi.NewChaincode(new(SmartContract))
    if err != nil {
        fmt.Printf("Error create fabpatient chaincode: %s", err.Error())
        return
    }
    if err := chaincode.Start(); err != nil {
        fmt.Printf("Error starting fabpatient chaincode: %s", err.Error())
    }
}
```