People's Democratic Republic of Algeria

Ministry of High Education and Scientific Research

University of Akli Mohand Oulhadj Bouira

Faculty of Sciences and Applied Science

Computer Science department

LIMPAF Research laboratory

Master Thesis

In Computer Science

***Specialty**: Computer Systems Engineering*

Electronic Health Record (EHR) Management

Blockchain-Based in Healthcare Systems

Supervised by :

– Dr Djellabi Brahim

Realized by :

– Smail Abd El Madjid

– Harmali Fares

2021/2022

Acknowledgments

*First and foremost, we thank **ALLAH**, the Almighty, for providing us with the patience, health, and courage to complete this project.*

Many thanks to our dear parents and families who, with their prayers and encouragement, helped us overcome all the obstacles.

*Our sincere gratitude goes out to our promoter, **Mr. DJELLABI Brahim**, who supervised the project and provided invaluable support,guidance, and courage during its development.*

Our heartfelt gratitude also goes to our Master of Computer Systems colleagues and teachers who assisted us throughout our journey.

Smail Abd El Madjid & Harmali fares

Dedication

I dedicate this modest work:

To my loving parents, thank you for all of your sacrifices, love, kindness, support, and prayers during our studies.

To ***Ouanis****, my annoying brother*

To my lovely aunties

To my entire family

To my friend and partner ***Fares***

Without exception, to all of my friends, Billal, Aghiles, Mohamed $_3$*, Hassan, Smail, Islam*$_3$*, Nazih, Maroua, Rihab, Lina, Chakib, Wahib, Amayas, Said, Amin, Lyes , Ayoub, Brahim, Hakim, Acheref, Hanin, Manar, Hafid, Houssam, Dadi . . .*

To all of my colleagues with whom I have shared my happy times throughout my studies.

Thank you, Merci, Gracias

Smail Abd El Madjid

Dedication

First of all, thank God for all the blessings and opportunities

I dedicate this work to :

My Beautiful family who supported me every waking hour.

My friends and colleagues whom I spent five beautiful years with .

My best friend and annoying partner ***MADJID***

Our teacher and supervisor ***Brahim Djellabi****.*

My Boss ***Brahim*** *who was very patient with me.*

Last but not least .. to ***wafia*** *just for existing.*

Thanks for Everything.

Harmali Fares.

Table of contents

List of Figures

List of Tables

List of Acronyms

CCP	Common Connection Profile.
EHR	Electronic Health Record.
DLT	Distributed Ledger Technology.
P2P	Peer to Peer.
TTP	Trusted Third Party.
CA	Certificate Authority.
SDK	Software Development Kit.
EMR	Electronic Medical Record.
IT	Information Technology.
MSP	Membership Service Provider.
HLF	Hyprledger Fabric.
DApp	Decentralized Application.
RH	Human Resources.
JSON	JavaScript Object Notation.
CPR	Computer-based Patient Record.
PoW	Proof of work.
PoS	Proof of Stake .
DPS	Delegated Proof of Stake.
PBFT	Practical Byzantine fault Tolerance.
IBM	International Business Machines .
GDP	Gross domestic product .

General introduction

In Healthcare, Hospitals, Doctors, Medical facilities, laboratories, and research centers require their patients' data to operate. However. The issue of healthcare data security and more particularly protecting patients' sensitive data has taken more and more interest. Where the impact is mostly in connection with breaches and leaks. For example, in August 2021, the DuPage Medical Group has reported that 600,000 patient records had been exposed[14]. The need of gathering patient's personal data (which known as PHI as Protected Healthcare Information, EHR as Electronic Health Record) is increasing in high paced way. (history, Blood analysis from lab results, antecedents, insurance, etc.). the emergence of the Blockchain technology with its powerful feature in terms of Decentralization, security and privacy makes the healthcare industry is one of the most promising applications of blockchain technology, as it is extremely practical when it comes to sharing patient information and health-related data.

Generally , health records are typically stored in traditional databases that is managed by different providers. Therefore, several security issues might be raised in such situation. Which need to be faced seriously. The blockchain is one of the most recent methods discovered for securing patient information and ensuring the confidentiality and interoperability of health data. Because of its decentralized nature and invulnerability, it has the potential to ensure the integrity of health data across all information systems. It can create a high secure distributed database where queries may be done without the interference of unauthorized identities. It is extremely efficient and can minimize a lot of resources and costs when multiple participants need to access the same database safely.

Since Healthcare systems rely mainly on the storage and sharing of medical data.

So transmitting personal data among multiple individuals via unprotected methods can result in vital information being leaked. Furthermore, the absence of client control over their personal information has negative effects, such as unauthorized identities having access to and editing personal medical information and exposing patient information can expose you to even greater dangers.

Our main goal in this thesis is to design a healthcare system based on blockchain technology In order to cope with limitation, to achieve this objective, Our thesis is organized as the following: In the first part we introduce the state of art on Healthcare systems, blockchain technology. In the second part, we discuss our design, its implementation, and finally its performance evaluation and validation. At end we recap our finding with a general conclusion and future perspectives.

Part I

State of art on Healthcare Systems and Distributed Systems

Chapter 1

Healthcare Systems

1 Introduction

Technology has a significant part in today's world, both in business and in our personal life. Healthcare is unquestionably one of the most essential areas in which technology plays a critical role.

In this chapter we introduce Healthcare systems, in which we will cover health records, starting with traditional paper records and progressing to e-health records, as well as the problems that this sector of the health industry faces.

2 Algerian electronic health status

Algeria's massive population, which surpassed 45,382 million people in 2022, made it one of the most important countries in North Africa, with an estimated 26.35 million Internet users, including 25 million social media users, allowing for a successful implementation of e-health in Algeria, which has evolved globally due to health-related sites with over 175 million applications. Electronic health services, on the other hand, are not widely used in Algeria. Furthermore, this notable absence is attributable to the Algerian content's reputation for being inadequate in most domains, rather than the developers' lack of interest in apps.

Particularly in the sphere of medicine. Aside from a lack of awareness on both sides, doctors, specialists, and patients about the benefits of this advanced technology that

shortens distances and makes people's lives easier, there is also a lack of understanding among doctors, specialists, and patients about the benefits of this advanced technology. The fact that information storage services are limited, and development costs remain high, does not mean Algerians are uninterested in technological advancement. On the other hand, there are approximately 21000 applications that serve the field of electronic health, with the majority of them being foreign applications that deal with traditional medicine and religion.

According to the most recent medical insurance figures, one doctor per 100,000 people is under insured. 1000 people, which is a small number in comparison to the 42 million people in the city. Furthermore, health-care administrators encounter a number of challenges. Some of these concerns can be addressed by introducing electronic health, such as the usage of an app that keeps track of a patient's medical records or an app that can be used to arrange doctor visits [15][16][17].

3 Healthcare record

The health record is a repository for the clinician's observations and analysis of the patient. The first recorded interactions between a doctor and a patient are often the history and physical examination. The history typically includes the patient's main complaint, current illness history, past medical history, family history [1]. Many Healthcare record structures have been introduced in the literature:

3.1 Paper-based health record

A paper record includes various sections, such as patient identity, reasons for visit, patient background and history (history, physical exam results, current symptoms (status). status), assessment and treatment, time document points, treatment results, letter of release and who wrote the record [1].

Paper-based medical records have a number of drawbacks. The first is that you can only use the record in one location at a time. This is a difficulty for individuals with complex medical issues who work with a variety of doctors, nurses, physical therapists, and other professionals [18].

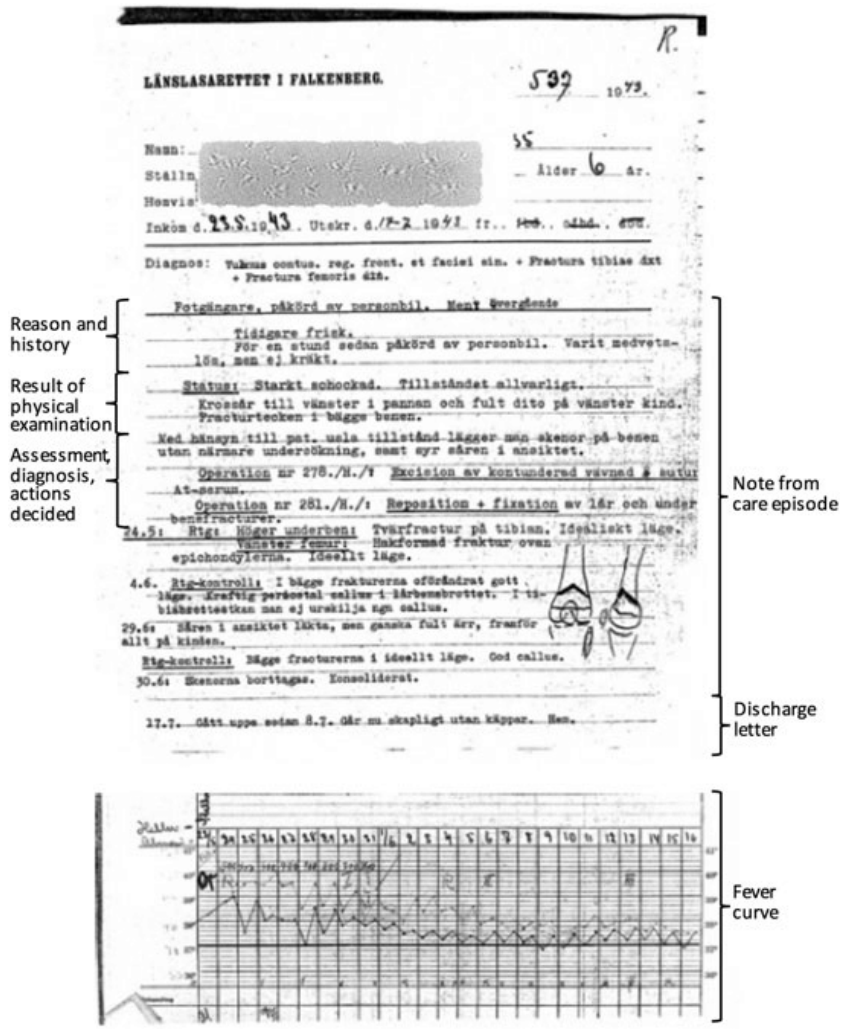

Figure 1.1: Description of the parts of a Swedish medical record from 1943 [1].

Another issue with paper records is that they can be quite unorganized. Not only might they be dispersed throughout numerous doctor offices and hospitals, as previously mentioned, but the records at each place can also be jumbled, with little overall overview. Most paper records have pages added to them as they are created chronologically, making it impossible to view summarized data across time. Another issue with the paper record is that it is incomplete [18].

The security and secrecy of the paper-based record is a final issue. Although commonly attributed to the EHR, there are characteristics of the paper record that make it more vulnerable to non-privileged outsider access. Because of the difficulties in duplicating it, suppliers and institutions rely heavily on photocopying and faxing. Furthermore, abstracts of paper records are saved in massive databases, such as the Medi-

cal Information Bureau's, which are managed by health insurance companies to avoid fraud but contain the medical information of over 12 million Americans [18].

3.2 Electronic healthcare system

Refers to health services and information supplied or enhanced via the Internet and similar technologies, and is a growing field at the crossroads of medical informatics, public health, and business. In a larger sense, the phrase describes not just a technological advancement, but also a state of mind, a style of thinking, an attitude, and a commitment to utilize information and communication technology to enhance health care locally, regionally, and globally [19].

3.3 Electronic Health Record

EHR is an electronic health record that contains longitudinal health information about a patient derived from one or more encounters with a doctor. The information includes demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. An EHR automates and streamlines the clinician's workflow. Quality management, evidence-based decision support, and outcome reporting can all be included in a complete record of a clinical patient contact.

4 Electronic Healthcare Record

4.1 EHR history

Medical records have existed since the beginning of the healthcare industry. The medical record was first used to record the disease and the most likely cause of that sickness. Medical records were stored on three by five cards in the early twentieth century. The federal government passed laws establishing Medicare in the 1960s and 1970s, ushering in a fast changing age in healthcare. At the same time, more third-party payers began to enter the healthcare sector, healthcare lawsuits became more common, healthcare quality became more essential, and the government enacted more strict regulations. This is when medical records became a true necessity in healthcare,

and the first electronic health record was introduced[20].

4.2 EHR terminology

Before going deeper into the specifics of EHRs for use in patient care, a few key terms must first be defined and separated.

The term “electronic health record” or “EHR,” refers to a patient’s electronic health record for use by nurses, doctors, and other health-care professionals. However, there is other terms used similarly when referring to the EHR. While the definitions of these terms are similar in some ways, they differ in others[21].

4.2.1 Electronic Medical Records(EMR)

EMR is frequently used in conjunction with EHR. Within a healthcare organization, it is a fully interoperable electronic health record of a patient. However, other people think of an EMR as a collection of patient records tied to a particular contact or care event. According to this viewpoint, an EMR is a snapshot of a bigger EHR. This method considers an EHR to be the sum of a patient’s EMR’s.

4.2.2 Personal Health Records(PHR)

It contains the same types of information as EHRs diagnoses, medications, immunizations, family medical histories, and provider contact information but are designed to be set up, accessed, and managed by patients. Patients can use PHRs to maintain and manage their health information in a private, secure, and confidential environment. PHRs can include information from a variety of sources including clinicians, home monitoring devices, and patients themselves [22].

4.2.3 Computer-Based Patient Record (CPR)

A lifetime patient record that contains all information from all disciplines (including dentists and psychiatrists) and demands full interoperability (possibly internationally), which is unlikely to be realized in the near future [23].

4.3 EHR benefits

The EHR system is expected to improve doctor efficiency, lower costs, and standardize care. [24]. The following are the primary benefits of the EHR:

1. Data can be continuously updated from the EHR system can be used in statistical analyses for improving quality outcomes, monitoring resource management, infection prevention and surveillance, all this in an anonymous manner.

2. Information can be shared between multiple EHR systems, allowing for better coordination of health care delivery at non-affiliated facilities.

Possible clinical trial volunteers may be located more easily with the use of the EHR, administrative costs expenses may be lowered, data errors may be significantly reduced, and negative outcomes may be detected more quickly [24].

Using the EHR to collect and analyze data in clinical trials may assist clinicians and researchers [24].

4.4 EHR drawback

EHRs provide a number of advantages, but they also have several drawbacks, the most notable of which are listed below.

1. Privacy and Cybersecurity Issues: The Consequences of Medical Information That Isn't Public Getting into the wrong hands might have disastrous consequences [25].

2. Inaccurate Data: anyone accessing an EHR may be getting incorrect or incomplete information if it is not updated as soon as new information becomes available this could lead to errors in diagnosis treatment and health outcomes not only by the issuing practitioner but also by any specialists pharmacists physical therapists or personal trainers involved in the patients care [25].

3. Accidentally scaring patients: When a patient has full discretion over his or her health information, they will be exposed to information that they do not completely appreciate [25].

4. Medical Liability Concerns: There are several liability concerns to consider while establishing an EHR system, such as how to ensure that sensitive medical data is not lost or erased during the transition from paper to electronic records.

   As a result, treatment mistakes may occur.

   Doctors may be found responsible if they are unable to collect all of the medical data available to them, especially when that data is expected to be more accessible [25].

5. Energy and resources : Selecting and setting up an EHR system, as well as properly converting all of your paper data to digital information, can take years. During that period, you'll need to figure out your budget and what features you'll need [25].

4.5 EHR architecures

EHR systems can be set up in a variety of ways. Depending on the specific demands and requirements of a medical practice, each offers advantages and disadvantages.

4.5.1 Physician-Hosted System

All data is stored on the doctor's personal servers in physician-hosted systems this means that a doctor is in charge of purchasing hardware and software as well as maintaining and protecting the data stored on their servers an EHR system hosted by a health care professional at their medical office may be beneficial for larger practices that can afford the overhead costs of the complex software [26].

4.5.2 Remotely-Hosted System

The storage of data is moved from the physician to a third party with remote-hosted systems.This organization is responsible for maintenance, data backup, and security. This type of system delegates data maintenance to someone other than a single physician or medical practice. Smaller practices or any healthcare provider who wishes to focus more on gathering information rather than preserving it may find this shift in responsibilities appealing. This type of solution avoids some of the IT issues that can divert a doctor's attention away from their patient's treatment and well-being [26].

5 Requirements for Electronic Health Records

EHR requirements are as follows:

1. Interoperability: The ability of devices and systems to exchange and convert shared data [27].

2. Security: In the healthcare, security is meant to offer patients the right to control their medical records [28][29].

3. Confidentiality differs from privacy in that it refers to the dimension of reliable communication or contract between providers and patients. The patient's records must be kept private [29].

4. Access control: Only authorized healthcare specialists and patients should have access to medical information [30].

   Patients should be able to obtain their data and have control over who has access to it.

5. Data sharing: Because the patient's treatment is spread across multiple health care providers, the exchange of medical records is a must; thus, the data is shared with other medical institutions and the government [30]. Integrity: Maintaining the data's efficiency and consistency, it ensures that data in EHR has not been tainted by unauthorized use [31].

6 Electronic Health Record (EHR) Market

Between 2021 and 2027, the electronic health record industry is expected to grow at a CAGR of more than 6.4 percent, with a market value of over USD 29.5 billion in 2020. The electronic health record, or EHR system, is primarily used to collect and store organized electronic medical data in a digital format for patients. EHR systems help to increase the amount of patient data that can be accessed, which improves the overall productivity and efficiency of patient care. Because of its multiple features, applications, and interoperability across a number of healthcare settings, electronic health records are projected to become more popular in the future [32].

The market's growth can be attributed to a growing adoption of technologies to fulfill expanding client needs. Speech-recognition software with natural language processing improves medical practitioners' interactions with EHR. It improves patient engagement while cutting down on the time specialists spend on paperwork. Using artificial intelligence (AI) to anticipate EHR-based clinical outcomes has also benefited in enhancing patient experience by facilitating improved care delivery. Market expansion will be assisted by favorable government initiatives and finance in the field, in addition to these advances [32].

7 Existing Systems and limitations

The main disagreement over EHR is about whether to save and share data on cloud infrastructures or on local centralized systems as a result of these centralized systems, healthcare facilities are required to store data locally in locally maintained structures and databases [33].

8 Motivations and objective

8.1 EHR based on Blockchain

Blockchain technology has already secured billions of dollars around the world. As a result, it could also be used to secure medical health records. The current EHR system can be undermined by utilizing the strong security of blockchain technology, which provides a more technologically superior, yet cost-effective solution. The proposed solution is to use blockchain to build a distributed access and validation system that will completely replace the current centralized intermediaries. This allows anyone to enter medical information about the patient into a database. However, no one will be able to make sense of anything until the patient explicitly grants permission.

By establishing a safer approach for medical data sharing in the field of healthcare productivity blockchain has the ability to revolutionize electronic health record exchanges by securing it through a distributed peer-to-peer connection the blockchain approach is presented as a means of sustaining and simplifying the process of grasping

distributed ledger technology [34].

Blockchain has the potential to modernize electronic health record exchanges by providing a secure approach for medical data exchange in the field of healthcare productivity, by safeguarding it through a dispersed peer-to-peer linkage. The Blockchain approach is proposed to provide sustenance and convenience to the procedure for comprehending the dispersed ledger technology [35][36].

Blockchain will handle the features of security, dependability, immutability, and interoperability [37]. Access to patient's health histories is critical for recommending medications, and blockchain can help with that. It will be simple to significantly improve the framework of medical care services [38].

8.2 Main objective

The goal of this thesis is to create a prototype for a blockchain-based EHR application that meets some requirements such as information privacy, traceability, safe data access, and sharing in a decentralized manner. The prototype will be built on Hyperledger Fabric1 (HL Fabric) and will act as an access control system for users and patients, allowing them to manage their identities, give traceability, and maintain their privacy.

The following are some of the advantages that a permissioned blockchain solution can give to the healthcare sector, and in particular to EHRs:

1. Safety: a blockchain is designed to be safe. In fact, the information saved on the ledger is tamper-proof under specific circumstances.

2. Resilience: a blockchain network may reach consensus and continue to function even if Byzantine faults occur.

3. Secure information sharing: data is saved or referred on the blockchain, which becomes a source of truth.

4. Avoid scattered information: data is stored or referenced on the blockchain, which becomes a source of truth [39].

9 Conclusion

After determining/understanding what an EHR is, its history, how it functions, and so on. We also looked into certain security issues, inconveniences, and potential risks, and came to the conclusion that users' data and privacy are at risk when utilizing this system. As a result, a solution, or an alternative must be created to ensure patients privacy and safety. The next chapter will discuss blockchain, blockchain applications, and blockchain's application in the healthcare industry.

Chapter 2

Distributed Systems and Blockchain

1 Introduction

In this chapter, we present at decentralized and distributed systems, as well as peer-to-peer networks, as a preparation for the second section, in which we'll go over the blockchain technology's structure and types, and provide some examples (applications) of how it's used.

2 Distributed Systems

A distributed system is a collection of self-contained computing pieces that seem as a single coherent system to users. The term "*distributed system*" refers to two distinct properties of distributed systems. The first is that a distributed system is made up of a number of computing parts that may all act independently of one another. A node, or computer element, can be either a hardware device or a software process. Another feature is that users (whether people or software) assume they are interacting with a single system. This means that the autonomous nodes must collaborate in some way. In the creation of distributed systems, the question of how to establish this collaboration is crucial. It's worth mentioning that we don't make any assumptions regarding the node types. Within a single system, they may theoretically range from high-performance mainframe computers to small devices in sensor networks. We also don't make any assumptions about how nodes are connected [40].

A distributed system consists of numerous independent computers connected via a computer network. In order to achieve a common goal, the computers communicate with one another. A distributed program is a computer program that runs on multiple computers in a network, and distributed programming is the process of creating such programs. In distributed systems, which are made up of a collection of independent computers connected by a network, a peer-to-peer architecture is employed. In a distributed system, each node has adequate computing power to work together on a task. Users have equal access to data in a distributed system, and user privileges can be enabled as needed. Individual component failures have little impact on the overall system, increasing availability and dependability. Traditional centralized systems have problems and limitations, such as security, data storage, and privacy concerns. Distributed systems have evolved to address these concerns. The Internet, blockchain, and SOA-based systems are all examples of large-scale distributed systems in action.

2.1 Pros and cons of Distributed Systems

1. Scalability: In distributed computing systems, new machines can be added as needed.

2. flexibility: It is simple to deploy, implement, and debug new services because of its flexibility.

3. Faster computation speed: A distributed computer system can combine the computing capacity of several computers, allowing it to perform calculations faster than traditional systems.

4. Open source: Because it is an open system, it can be accessed locally as well as remotely.

5. High performance: When compared to centralized computer network clusters, it can deliver better performance and cost savings.

A distributed system is not without flaws, the following are some of the system's drawbacks:

1. Difficult troubleshooting: Because of the distribution across multiple servers, troubleshooting and diagnostics are more difficult.

2. Less software support: One of the major disadvantages of distributed computer systems is the lack of software support.

3. Expensive network infrastructure: Basic network configuration issues, such as transmission, high load, and data loss.

4. Data security and sharing are at risk in distributed computer systems due to the characteristics of open systems.

2.2 Centralized vs Decentralized

Centralized System Characteristics	**Decentralized System Characteristics**
One component with non-autonomous parts	Multiple autonomous components
Component shared by users all the time	Component are not shared by users
All resources accessible	Resources may not be accessible
Software runs in a single process	Software runs in concurrent processes on different process
Single point of control	Multiple point of control
Single point of failure	Multiple point of failure

Table 2.1: Centralized and Decentralized Characteristics [11]

2.3 Decentralization and distributed systems

decentralized systems are classified into distributed systems in a distributed system there is no one point of decision-making each node makes its own decisions and the systems overall reaction is a consequence of these actions [41][42].

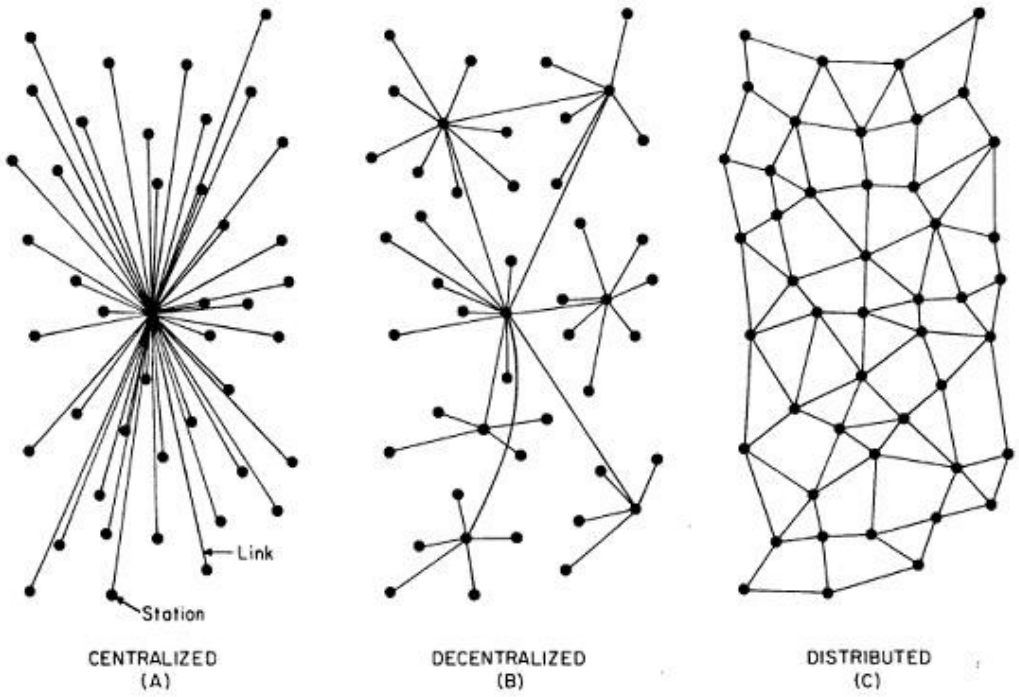

Figure 2.1: Distributed communications networks. [2]

3 Peer-to-Peer Networking

The term “peer to peer” refers to a decentralized computing network in which users exchange files with one another directly.

Members of peer-to-peer networks share responsibility for delivering and maintaining the network’s resources. You are required to make files available to other members of the network in exchange for being able to download files from the network.

In a peer-to-peer (P2P) network, your computer can operate as a server, serving content to other members’ computers [43].

3.1 P2P architecture

Multiple clients will communicate with a central server in a typical client-server design. A peer-to-peer (P2P) architecture is made up of a decentralized network of peers, which are nodes that can function as both clients and servers. Without the need for a centralized server, P2P networks share burden across peers, and all peers contribute and consume resources inside the network.

Peers, on the other hand, are not all created equal. Super peers may have greater resources and be able to give back more than they take in. Edge peers do not contribute

any resources to the network, they simply consume it.

P2P architecture is entirely decentralized in its purest form. However, in some applications, a central tracking server is overlaid on top of the P2P network to assist peers in finding one another and managing the network [44].

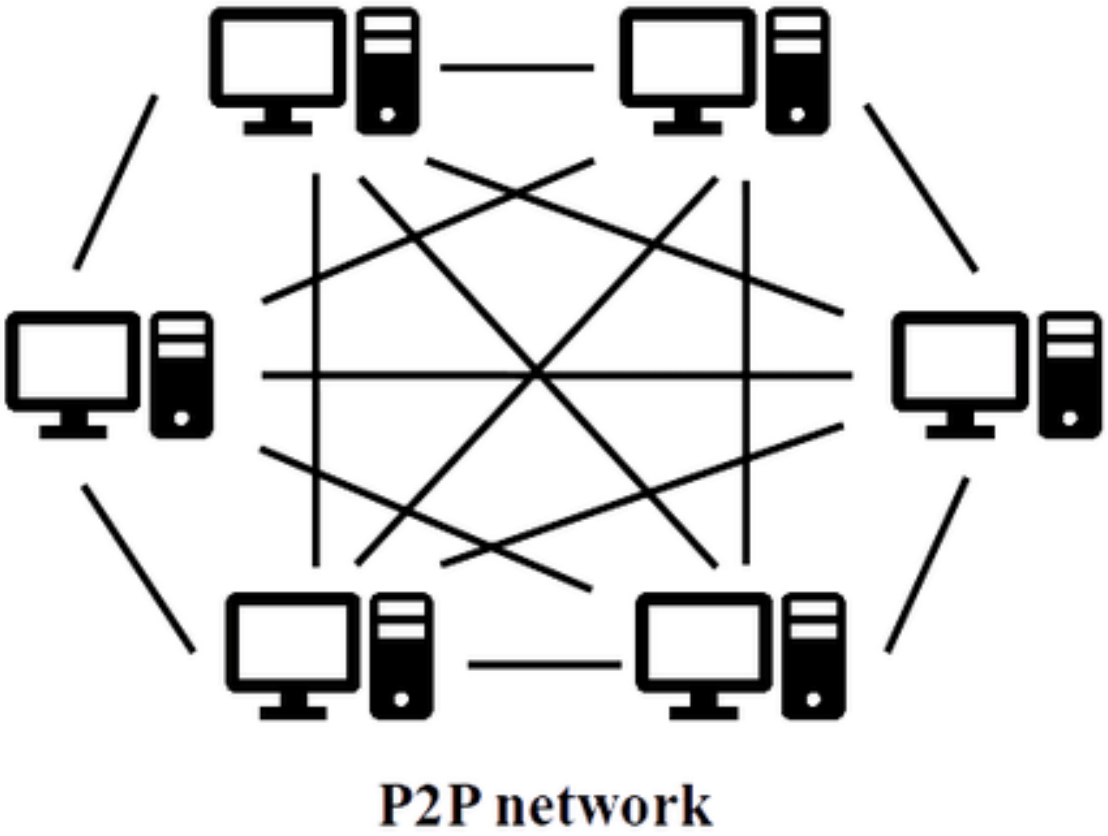

Figure 2.2: Peer-To-Peer architecture [3]

3.2 Role of P2P in blockchains

P2P is a technology based on the decentralization principle, which is a relatively basic concept. All cryptocurrencies can be transacted internationally without the use of an intermediary, intermediaries, or a central server thanks to blockchain's peer-to-peer architecture. On the decentralized peer-to-peer network, anyone who wishes to participate in the system of checking and validating blocks can set up a Bitcoin node. Blockchain is a decentralized ledger that maintains one or many digital contents over

a peer-to-peer network. A decentralized peer-to-peer network is one in which all computers are connected in some way and each maintains a complete copy of the ledger, which is compared to other devices to ensure the data is legitimate [45].

4 Blockchain

4.1 History

The concept of blockchain technology was first proposed in 1991 by researchers **Stuart Haber** and **W. Scott Stornetta**, who proposed a theoretically feasible mechanism for time-stamping digital documents so that they could not be backdated or tampered with [46].

The time-stamped papers were stored in a cryptographically secure chain of blocks, and Merkle trees were added to the architecture in 1992, making it more efficient by allowing several documents to be collected into one block. However, the technique was never implemented, and the patent expired in 2004, four years before Bitcoin was created[46].

In late 2008, a person or group using the pseudonym **Satoshi Nakamoto** sent a white paper to a cryptography mailing list introducing a decentralized peer-to-peer electronic payment system known as Bitcoin [46].

Bitcoin was created on January 3rd, 2009, when Satoshi Nakamoto mined the first bitcoin block, which had a reward of 50 bitcoins. **Hal Finney** was the first Bitcoin recipient, receiving ten bitcoins from Satoshi Nakamoto in the world's first bitcoin transaction on January 12, 2009 [46].

4.2 Definition

Blockchain is a decentralized peer-to-peer network of nodes that records authenticated, encrypted transactions as a distributed public ledger, thereby providing a trust and verification system by governing the replication of the ledger throughout the network's processing nodes using programmed rules [47].

Blockchain is a decentralized transaction ledger, commonly known as a peer-to-peer system. It is made up of a network of nodes that keep track of a common set of

historical transactions. Each transaction is agreed upon within the system, and each transaction is validated by participant consensus. The data is encrypted, traceable, and auditable [48].

Blockchains are made up of data blocks, each of which is linked to the one before it by a cryptographic pointer. The chain continues to the first block, which is the originator. When a new block is added to the system, it is linked to the one before it. Organizations all across the world are attempting to capitalize on these features. Distributed consensus, safe, traceable, validated, and visible data are all important features [48].

4.3 Blockchain features

1. Decentralized: the system works without the use of a middleman, and all Blockchain members make decisions. Every system has its own database [49] [50][51].

2. Transparent: Every action is recorded on the Blockchain, and the records' data is visible to all Blockchain participants and cannot be changed or removed. The results of this recording highlight the Blockchain's transparency [49] [50][51].

3. Immutable: The Blockchain achieves this by agreeing on and sharing transactions. After a transaction is connected to the Blockchain, it will be impossible to change or delete it [49] [50][51].

4. security is ensured: Because each person who joins the Blockchain is assigned a distinct identity that is linked to their account [49] [50][51].

4.4 Key Concepts of Blockchain

4.4.1 A Distributed Ledger

A Distributed Ledger is a new and rapidly expanding method of collecting and distributing data across many data repositories (or ledgers). Transactions and data can be recorded, exchanged, and synchronized over a distributed network of different network participants using this technology [52].

4.4.2 Smart Contract

A smart contract is a piece of blockchain-based code that facilitates, executes, and enforces the terms of a contract. A smart contract's principal goal is to automatically carry out the terms of an agreement once certain criteria are met. As a result, smart contracts promise lower transaction fees than traditional systems, which rely on a trusted third party to enforce and execute an agreement's provisions [53].

4.4.3 Consensus

As a fault-tolerant technique for transaction verification, consensus mechanisms have been included into blockchains. The consensus algorithm is used to keep the network's nodes in accord. As the network grows, the number of nodes grows as well, making consensus more difficult [54].

4.5 Blockchain Consensus

Blockchain is a peer-to-peer security system that uses distributed consensus algorithms or protocols to replace traditional centralized signature-based security. Surprisingly, there is no reliable third party. Furthermore, the parties do not have any mutual trust. As a result, a consensus algorithm is required for this type of distributed ledger system [55].

1. Proof of work (*PoW*): is a process in which each network node calculates the hash value of a continually changing block header.

   The main idea is to distribute Bitcoins across nodes based on their hashing power. Someone must be chosen at random to record the transaction in a decentralized network. A random selection is used to accomplish this. The estimated hash value must be equal to or less than a particular provided value in order for the consensus to be reached. When a node gets its target value, it broadcasts the block to other nodes, requiring all other nodes to authenticate the integrity of the hash value. If other miners agree that the block is genuine, they can add it to their own Blockchains.

   In Bitcoin, the PoW technique is known as mining, and the nodes that find the hash values are known as miners [55].

2. Proof of Stake (*PoS*): Iis a low-energy alternative to Proof of Work (PoW).

   People must prove their ownership of the money amount in order to use PoS. People with more currencies are less inclined to attack in a network [55].

3. Delegated Proof of Stake(*DPoS*): DPoS is a point-of-sale system that is similar to POS. Miners are given priority in generating blocks based on their stake. New transactions are validated by miners and recorded on the global ledger. Delegates are elected by stakeholders to generate and certify a block in DPOS is representative [55].

4. Practical Byzantine fault Tolerance (*PBFT*): Byzantine Fault Tolerance is a well-known approach in distributed systems (BFT). It is said to be an excellent way for resolving transmission faults. The early Byzantine system, on the other hand, necessitates exponential operations. PBFT (Miguel and Barbara, 1999) is a replication algorithm that can handle Byzantine failures. The algorithmic complexity of BFT is decreased to a polynomial level with the help of PBFT, which considerably improves the efficiency. Because PBFT can handle up to 1/3 malicious Byzantine replicas, Hyperledger Fabric (hyperledger, 2015) uses it as its consensus mechanism [55].

4.6 Blockchain Architecture

A blockchain's architecture is made up of a decentralized and distributed network of nodes. The immutable ledger is replicated in each node. A cryptographically linked set of append-only blocks makes up the immutable ledger. To add blocks to the ledger, the nodes conduct transactions and reach consensus. Clients sign and submit transactions to the nodes. The verified transactions are forwarded to the smart contracts for execution. Ordered transactions are grouped together into blocks. The blockchain is updated with the new blocks. A blockchain's core design consists of blocks, chains, and a network [56].

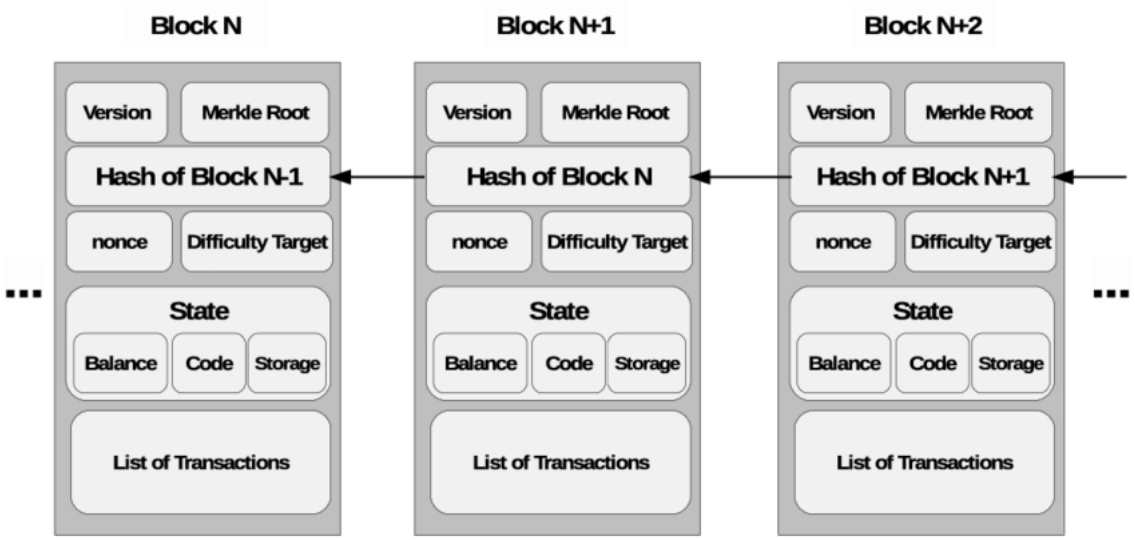

Figure 2.3: Blockchain design Architecture, showing chained blocks with header and body fields [4].

4.6.1 Nodes

Because of their function in constructing the distributed network, computers are referred to as *nodes*. They could be cloud-based virtual computers hosted on real servers. They could be laptops connected to a distributed network. They could be IoT devices that operate in decentralized industrial networks.

They may even be intelligent light bulbs. A node is a generic phrase that refers to a network's endpoint. It is possible to have a wired or wireless network. Peer is another term for a node, as in peer-to-peer networks, which are intended for decentralized applications. [56].

4.6.2 Blocks

Blocks are used to keep the logs of completed transactions. Each block has a header, a timestamp, and the hash of the previous block. The genesis block, which is the first block, contains more information about the blockchain, such as policies. The genesis block will contain a list of member organizations and their certificates, as well as policy information detailing the amount of organizations that must endorse transactions, if it's in a permissioned blockchain like Hyperledger Fabric. It will also include the identity of the orderer node, which is in charge of ordering transactions and creating blocks

for peers to add to the blockchain [56]. Additional data is stored in the block, which is used to bind the blocks together and impose integrity restrictions, prohibiting tampering with the data. The blocks are connected, and this connecting is what gives the term blockchain its meaning [56].

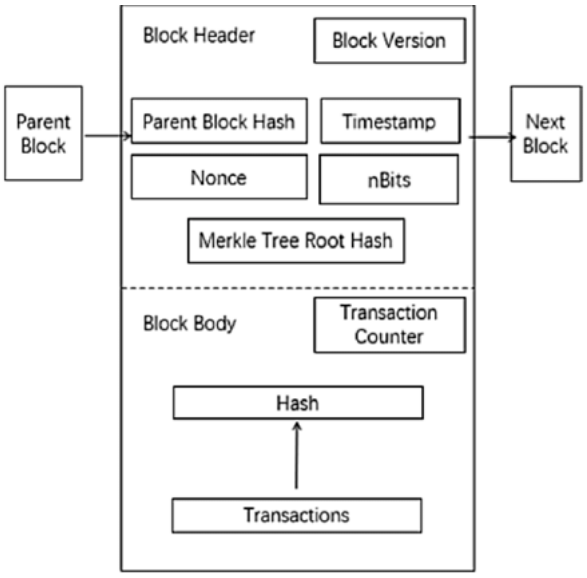

Figure 2.4: The structure of a block in a Blockchain [5].

4.6.3 Chains

A chain is a collection of linked blocks. They are append-only and immutable. One or more chains can be found in a blockchain architecture. Chains can be as long as you want them to be, or as many blocks as you want them to be. Pruning can help prevent or manage this, but it also has negative consequences, such as lowering trust in the blockchain network and removing the ability to browse and audit the full chain. This may compromise the chain's integrity [56].

5 Blockchain Types

The two most common types of blockchains are private and public, although there are a few others, such as consortium and hybrid blockchains.

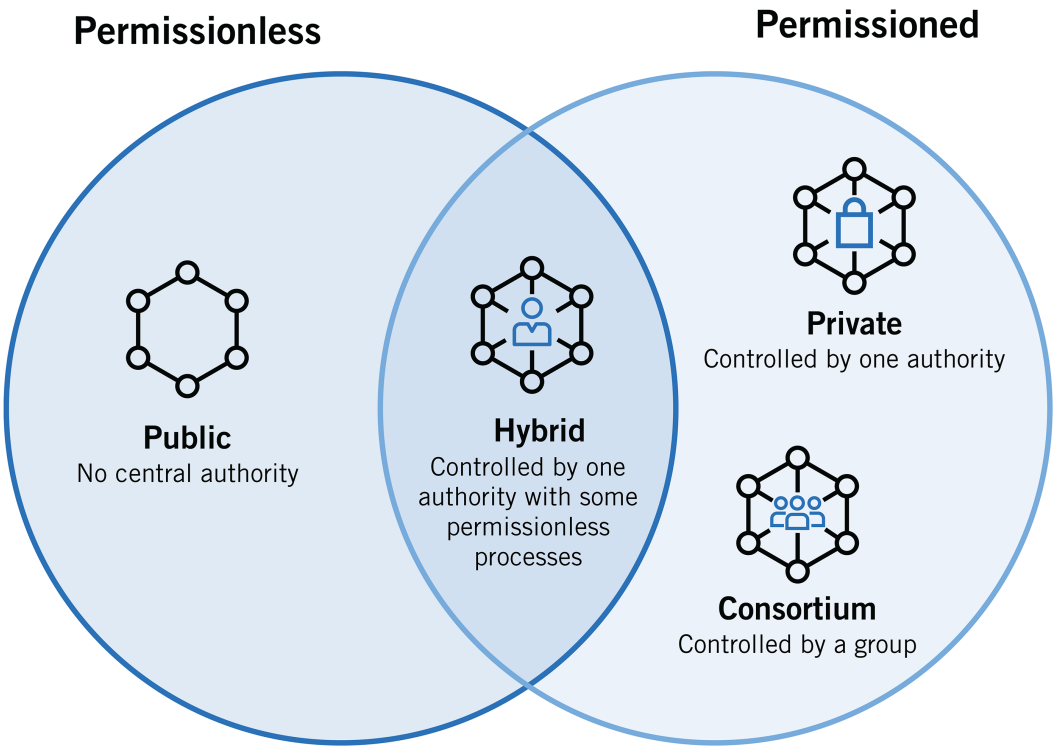

Figure 2.5: Blockchain Types [6]

5.1 Public blockchains

Public blockchains are permissionless and entirely decentralized, allowing anybody to participate. All nodes of the blockchain have equal rights to access the network, create new blocks of data, and validate blocks of data in public blockchains [6]. Currently, public blockchains are mostly utilized for bitcoin exchange and mining. Popular public blockchains like Bitcoin, Ethereum, and Litecoin may be familiar to you. On these public blockchains, nodes “mine” for cryptocurrency by solving cryptographic equations to create blocks for the transactions requested on the network. The miner nodes are compensated for their efforts with a tiny amount of bitcoin. The miners are essentially new-age bank tellers who create transactions and are compensated (or “mind”) for their services [6].

5.2 Private blockchains

Private blockchains limit access to the data stored in the blockchain by requiring users to be authorized before reading or writing data to it. Depending on who has

access to the data in the blockchain [57] [6].

5.3 Consortium blockchains

Consortium blockchains, unlike private blockchains, are permissioned blockchains that are governed by a group of organizations rather than a single entity. As a result, consortium blockchains have a greater degree of decentralization than private blockchains, making them more safe. Forming consortiums, on the other hand, can be a complex process because it requires collaboration among a number of companies, which presents logistical challenges as well as the danger of antitrust violations Furthermore, some supply chain participants may lack the appropriate technology or infrastructure to adopt blockchain technologies, while others may decide that the upfront expenditures of digitizing their data and communicating with other supply chain members are too high a price to pay [57][6].

5.4 Hybrid blockchains

Hybrid blockchains are those that are managed by a single entity but have some oversight from the public blockchain, which is necessary to conduct certain transaction validations. IBM Food Trust is an example of a hybrid blockchain, which was created to improve efficiency across the whole food supply chain. In a subsequent piece in this series, we'll go through IBM Food Trust in further depth [6].

6 Blockchain Applications

6.1 Internet of things (IoT)

In both the commercial and consumer worlds, the Internet of Things (IoT) is rapidly becoming the most popular technology. The IoT market may require a silver bullet in the form of blockchain innovation. It could be used to link and track billions of devices all over the world, making it simple for IoT manufacturers to protect their equipment and potentially saving a lot of money. The bulk of IoT systems use a centralized paradigm in which a broker or hub manages connectivity between various devices. This strategy has proven to be impractical, especially when devices must communicate

with one another independently. This particular requirement has drawn the attention of academics to the direction of decentralized IoT systems [58].

6.2 Scientific Research

The reliability of scientific findings is significant, especially in subjects as important as medical sciences. Scientific research, on the other hand, has been polluted by result manipulations, selective result publication, and a plethora of studies funded by corporations with the objective of promoting their own products, that blockchain-time stamped techniques can be used to audit and certify the integrity of scientific research study outputs in a cost-effective, independently verified manner [58].

6.3 Finance

Blockchain technology can help traditional financial services in a number of ways, including:

1. Increasing the efficiency of financial transactions by lowering their costs and making them faster, safer, and more traceable across the financial system [59].
2. Ensures transparency and integrity, which are two key factors in financial transactions [59].
3. Improving back-office infrastructure and facilitating cross-border settlements [59].
4. Smoothing real peer-to-peer financial transfers and payments [59].
5. Increasing financial inclusion by providing billions of unbanked people throughout the world with simple, digitalized financial transactions at a cheap cost, particularly in developing nations [59].

The usage of blockchain in a number of banking activities could benefit banks. Blockchain could improve trust, efficiency, transparency, information availability, banking service availability, and reduce the time and cost associated with providing such services in the banking sector. One of them is the *Know Your Customer* (KYC) procedures. Despite the fact that this technique takes a long time and costs a lot of money, banks continue to have difficulty discovering unlawful financial activity such as money laundering, tax evasion, and terrorism financing [59].

6.4 Healthcare

With the advent of some potential in such an important business, the realization of the idea of using Blockchain in the healthcare sphere has begun to expand. New ideas for storing and sharing medical information have undoubtedly emerged, utilizing Blockchain's potential to provide trust and security while decreasing the costs and resources required by traditional healthcare administration infrastructure [58].

7 Blockchain in healthcare

Algeria's health system has improved as a result of an increased share of the state budget committed to the health sector, which now accounts for 5.2 percent of GDP. Over the last decade, the government has allocated US $ 28 billion, including US $ 3 billion in the state budget for 2020, and the people continue to benefit from free public healthcare and social security. Algeria, like other middle-income nations, is confronted with a number of issues, including growing inequalities in healthcare access and rising economic and social vulnerabilities [60].

Despite significant investments, the public health system suffers from a lack of leadership, low service quality, disorganization, and excessive bureaucracy. The sanitary crisis exposed systemic flaws, prompting the government to embark on a series of reforms to modernize the sector [60].

Healthcare is becoming more interconnected and data-driven as our world becomes more connected and data.

These changes, on the other hand, come at the cost of more regulation, overhead expenditures, and increasing educational requirements for those who engage. As a consequence, healthcare changes are taking longer and the result of greater data availability, additive manufacturing AI, and wearable and implanted gadgets to monitor our health, the way healthcare is given is projected to alter drastically by 2030 [61].

The number of body functions that can be tracked using a wearable device is expanding. Blood pressure, hydration, oxygen level, brain activity (EEG), glucose, respiration, temperature, heart rate variability, and movement can all be tracked using today's wearable technology [62]. "From assistance for Alzheimer's patients to understanding complex knee injuries, wear- able computing will transform how we under-

stand pharmaceuticals, rehabilitation and preventative care" [62].The range of bodily functions that can be monitored using a wearable device is growing.

Wearable equipment can monitor blood pressure, hydration, oxygen levels, brain activity (EEG), glucose, respiration, temperature, heart rate variability, and movement [63].

7.1 Blockchain data management in healthcare

Data management is one of the most significant impacts blockchain can have in the healthcare industry. Health care organizations and health care personnel use a variety of approaches and tools to exchange patient health information [64]. People travel for a variety of reasons, and as a result, they frequently seek health care services from a variety of providers in various places. Health-related data might be fragmented and outdated, resulting in a poor data exchange relationship between the provider and the patient's medical information.

The blockchain is a promising technology that has the potential to help rationalize health-data management operations while ensuring a high level of efficiency and bolstering trust. She has a long list of crucial and integrated features, such as decentralized storage, transparency, immutability, authentication, data access flexibility, interconnection, and security, allowing for widespread adoption of blockchain technology for health data management. Blockchain is based on the concept of intelligent contracts, which contain requirements that are agreed upon by all the network's health-care partners. It allows you to cut down on unnecessary administrative costs [65].

7.2 Blockchain applications in healthcare

Blockchain is a powerful technology that allows many parties to securely share and access data. This is a serious concern in digital health, where medical data privacy and security are critical. Blockchain can help digital health by making it easier to securely communicate data across disparate healthcare systems with patient approval.

Figure 2.6 showcases the many aspects and key enablers of the Blockchain idea across a number of healthcare fields and related topics.

Figure 2.6: Capacities of blockchain technology for healthcare domain. [7]

7.2.1 Health Insurance Claims

One of the healthcare industries that can benefit from blockchain's immutability, openness, and auditability of data stored on it is health insurance claims. While the processing of healthcare insurance claims is an important area where blockchain might help [66][67].

Prototype implementations of such systems, on the other hand, are quite limited. MIStore is a blockchain-based medical insurance solution that provides encrypted and immutably stored medical insurance data to the medical insurance sector [68].

7.2.2 Remote Patient Monitoring

Remote patient monitoring is the collecting of medical data using mobile devices, body area sensors, and IoT (Internet of Things) devices in order to remotely monitor a patient's condition. Blockchain is useful for storing, distributing, and retrieving biomedical data that has been collected remotely [67].

Ichikawa et al. demonstrate an application that uses mobile devices to send data to a Hyperledger Fabric-based blockchain application [69].

7.2.3 Pharmaceutical Supply Chain

Patients may suffer serious effects if they receive counterfeit or inadequate drugs. Drug tracking has identified blockchain technology as having the potential to solve this problem. Blockchain can build tracing and chain of custody from manufacturer to

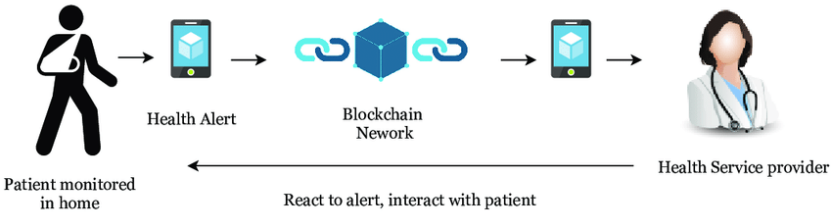

Figure 2.7: Remote Patient Monitoring. [8].

patient [67] [70] [71].

Chronicled is a technology startup building a chain of custody model that shows where a drug was made, where it has been since, and when it was distributed to patients, using the immutability of the blockchain to avoid pharmaceutical fraud and theft [71] [72].

7.2.4 Electronic health records

When used to secure medical data, blockchain can store data in a fashion that is open to all users on the network, entirely unchangeable, and tamper-proof.

Doctors and nurses would be able to regulate the flow of information from a single, trusted platform using blockchain-based electronic health records. Everyone would have access to the same information, and any changes would be accessible to the entire network very instantly. This means that medical personnel can be confident that the information they obtain about a patient is both accurate and current [73].

8 Conclusion

The blockchain's application has expanded beyond the realm of cryptocurrencies. It is getting more popular as a result of its application in a wide range of fields with helpful features included out of the box, and people are considering its development. We focused on the electronic health record in this thesis, and after researching for and understanding all of the needs and goals, a solution was proposed. We will present our solution and its different approach in the next chapter.

Part II

Electronic Health Record Systems Based on Blockchain Technology

Chapter 3

An efficient design for EHR based on blockchain

1 Introduction

We will suggest an application that should fulfill our need in order to achieve our goal of creating an electronic health record. A Blockchain-based decentralized application. We developed a solution to safeguard the users data. We will present a concept in which the user has control over access to his data and can regulate his privacy. Then we will specify The data flow (data structure) and user interactions with the app and blockchain.

2 Related work

Several researchers have recently investigated the use of intelligent agents in healthcare to offer interoperability. Recently, some researchers have looked into blockchain technology, most of them, like us, have taken a theoretical approach, proposing techniques to improve EHR mobility and security utilizing distributed ledgers. Because blockchain is a relatively new technological breakthrough, we only discovered a few references detailing actual EHR implementations over blockchain.

In [74], [33], The problem of EHR accessibility and sharing was addressed with certain cloud-based solutions. Manas Ranjan Patra, and all [74] studied how cloud com-

puting may be used to improve and facilitate healthcare services. The system must meet a number of needs, including accessibility, scalability, security, data transport, storage, and gathering methods. They suggest that storing patient data in the cloud can be done at a reasonable cost.

Doctors and medical professionals can then exchange and access this information. However, they do not elaborate on the concept and confine the scope to a strong design model with no implementation or tests.

X. Yue, and all [75] based on the concepts of [74]. they suggested the design of a so-called data gateway application for healthcare data on the blockchain They claim to be the first to present a distributed ledger system that meets needs such as EHR sharing and data management by patients. Although the architecture anticipates a private blockchain running in the cloud, it does not specify how it should be implemented or offer performance tests.

Azaria, Ekblaw, [76] were the first to present a fully functional prototype of blockchain technology used to EHRs. They propose MedRec, a system that not only manages EHRs in a distributed way but also regulates access and authenticates users to address concerns including health data fragmentation, slow access, system interoperability, patient agency, and enhanced data quality and quantity for medical research.

They attempt to accomplish this by describing a system with a modular design that is simple to incorporate. In actuality, for scalability and adoption reasons, the actual medical record is kept off-chain on the hospital or provider's relational database. Metadata and references to the EHR location are stored on the blockchain. A smart contract, more specifically, regulates the interaction between actors and data, as well as defining access restrictions and references to that data. The pointer is a tuple that includes a query string to run on the provider's database as well as the location (host port and credentials) where the EHR can be accessed [76].

3 Problem statement and application scenarion

The most difficult challenge for health-care systems is figuring out how to share medical data with interested parties (doctors, hospitals, patients) while maintaining

data integrity and protecting individuals' privacy.

3.1 Design goals

Whether it's features, traits, or qualities, the literature provides crucial insights into the requirements that an EHR system must meet in order to improve the operations of doctors and workers as well as the security of the healthcare system. According to the blockchain and EHR literature, the following list outlines the most important needs [76][77][78][79][80][78].

- **Scalability**: An EHR system should be scalable in terms of the number of users who use it. In the context of the blockchain, a system should be able to work with any number of nodes and users in the network without causing any issues [80].

- **Identification**: Every user that interacts with the EHR system must be identified, and access to information must be provided or restricted based on that identity [78].

  Because anonymity and pseudonymity are intrinsic characteristics, this condition excludes public blockchain implementation. It is conceivable to connect an identity to the corresponding pseudonymous, but this threatens the patient-physician relationship's privacy and confidentiality.

- **Privacy and access control**: The information is only accessible to those who have permission: a doctor can only access and alter a patient's record with the patient's consent. Every interaction between the user, whether a patient or a doctor, and the health record must also be tracked.

- **Patient control**: Patients should have access to their medical records. It not only allows patients to combine their records with notes and additional information, but it also helps them become more aware of and involved in their own healthcare, which is especially important for patients with chronic diseases [79].

- **Data sharing**: Because a patient may seek treatment at multiple hospitals and clinics, healthcare facilities must establish a safe data sharing mechanism [77].

- **Data analysis for the research**: A significant portion of the literature highlights the importance of medical data research. It is critical to provide anonymized clinical data in order to develop research into novel treatments and cures. As a result, an EHR system must have means for aggregating and transmitting anonymised data to research laboratories [78].

- **Integration**: Finally, a new system must be built for integration in order to give all of the above features. In reality, blockchain-based EHR management systems are designed to integrate with existing systems and deliver functionality that were previously unavailable [76].

3.2 Application Scenario

To manage patient medical records in a our system, hospitals and Lab function as nodes. Patient information has been handled as an asset in the ledger. It is also conceivable to keep the EHR data reference in the ledger, but since the application is not maintained by real data, it will be necessary to have a separate database with patient personal data.

When a doctor is medicating a patient, patient history data will be available, which will help doctors in assigning treatment plan. It is aimed to provide extra stages in application for patients to improve the privacy of records. A patient might choose to allow a specific doctor access to his or her data. Doctors have restricted access to patient information, Patient, on the other hand, can read all fields but only update personal ones.

4 System design and proposed architecture

4.1 Functional Requirements

The functional requirements specify how the system will function. The functional requirements used in the system's development are listed in the table 3.1.

Nº	**Functional requirements**
1	All users will have access to their accounts.
2	Patients should be able to access their previous medical records at any time and from any location, as long as they are connected to the Blockchain.
3	The patient should be able to give the doctor access to their medical records.
4	All recodes must be accessible outside of the organization. Medical data must be accessible throughout any health facility.
5	All users should be able to logout .

Table 3.1: Functional requirements

4.2 Non-Functional Requirements

Non-functional requirements are any aspects of the system that are unrelated to the system's behavior. The primary goal of the functional requirement is to demonstrate how the system should be. The main goal of the system is to create an immutable platform that can handle the basic workflow of medical facilities, as well as a suitable and convenient platform that emphasizes the components that are required to make it usable and valuable to the user. The primary source of these requirements is the analysis of responses from interviews with the selected sample population. The non-functional requirements are shown in table 3.2.

No	Non-Functional requirements
1	The application must be compatible with any browser.
2	The application should be simple and straightforward to use.
3	The application should ensure the patient's data's integrity and verification.
4	The error management and notification interface in the application should be simple.
5	The system should allow patients to keep their records private while sharing them.
6	The user's data should always be accessible through the system.
7	All the data entered should be validated by the system.

Table 3.2: Non-Functional requirements

4.3 Proposed architecture

Our EHR consists of three primary actors in this blockchain-based EHR implementation: HR, Patients,Labs and Doctors.

As a participant in the EHR system, patients play a significant role. They have control over the health records that are created and stored on the blockchain. They have the ability to update their personal information. As a result, they have the authority to control who has access to their records.

Doctors collect medical data from patients via diagnoses. Only those patients who have validated them as authorized Doctors and given them permission to write into their records are accountable for updating health-related information in their records. They have the ability to modify their personal information or profile.

Patients who have approved them as authorized labs and given them permission to write into their records are in charge of running tests, generating test results, and

updating this information in their records. They can make changes to their profile information.

RH is in charge of setting up the blockchain network and creating user accounts.

Medical records are the network's most valuable asset in this system. Each medical record belongs to a patient who has signed up for the network. The asset's value changes whenever a transaction is completed. Changes include things like updated records if the patient is diagnosed with a new ailment, medication changes, test findings, and so on.

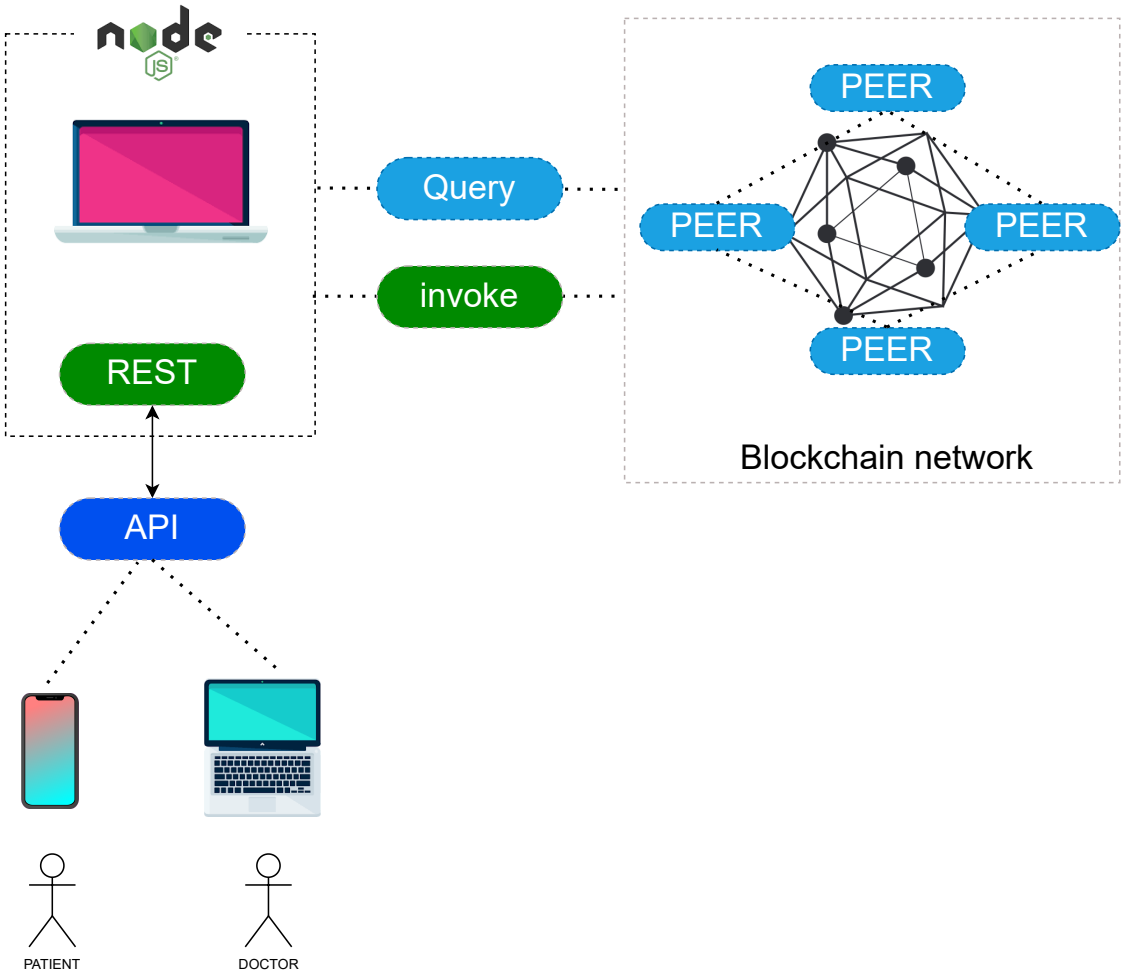

Figure 3.1: System Architecture.

The transactions are generally actions conducted on the network asset, such as generating a medical record, receiving specific information from the network, updating the medical record, giving and revoking access to doctors and labs. A relationship between the two participating nodes is required for the execution of some of

these transactions. For example, the lab or doctor must have their *userID* in the assets(*medical record*) to update the medical record. The permission rules are also defined by this system, these rules determine who has access to what resources and under what conditions.This helps in restricting access to all system resources, only authorized users can make changes to or read specific records.

the main transactions of this system are the following :

- **CreateMedicalRecord**: This transaction would generate network records. It includes fields such as ID, owner, and a list of authorized doctors and labs. It includes fields for storing patient medical information such as medical history, last consultation with which doctor, date of consultation, allergies, and so on. The generated ID is unique, and it's used to identify that specific record in the collection.

- **GrantAccess**: To make changes to the records, the doctor, and the lab would need access to the record only the authorized doctor and lab can read or write on the medical record. This transaction is used to grant this authorization.

- **RevokeAccess**: Once the need to access a specific record has been met, the owner of the medical record can revoke access to the doctor or lab, and the record will no longer be accessible. The doctor and the lab are no longer permitted to read or modify that record.

- **EditePrivacy**: We previously stated that the user owns his information; consequently, this transaction allows him to change the privacy of his data, allowing users without authorization to view it or not.

5 System Modeling

5.1 Main use Cases

The system has four users with the roles of HR, patient, lab, and doctor. Each user has their own set of use cases.

5.1.1 HR use case

We'll start with the HR actor, whose job in the system is to manage users and have the only option to remove medical records (see figure 3.2).

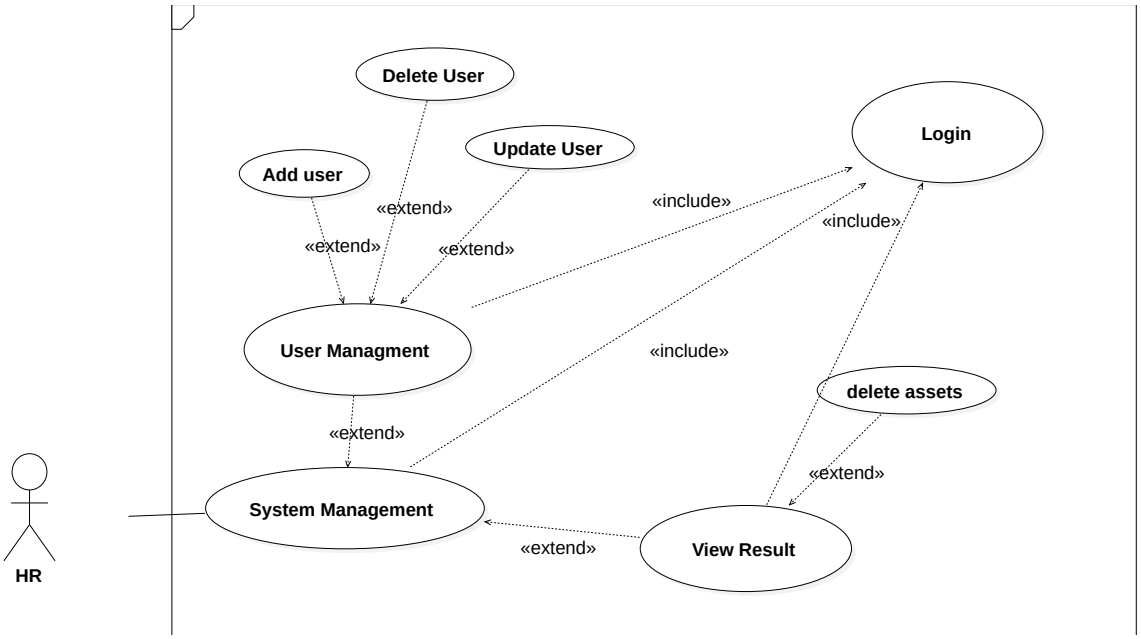

Figure 3.2: HR use Case Diagram

5.1.2 Doctor use case

The doctor has a critical task to do, update the medical record. This activity requires the patient's permission more information in the table 3.3.

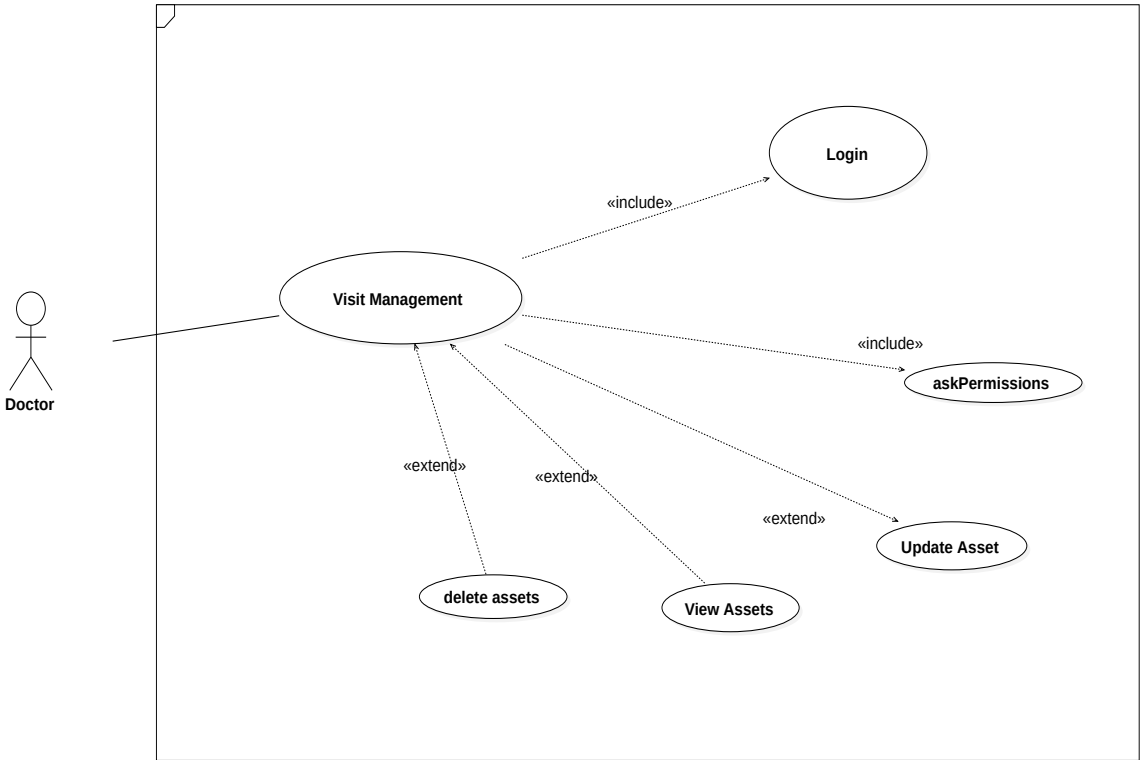

Figure 3.3: Doctor Use Case Diagram

Use case	Update medical record Use Case
Primary actor	Doctor/LAB
Stakeholders	1. Doctor wants to diagnose the patient. 2. LAB to examine the patient
Preconditions	1. Login 2. Authorization
Post condition	doctor and lab should have access to the patient medical record, update it and store new data in the blockchain

Table 3.3: Update medical record Use Case.

5.1.3 Lab use case

The laboratory actor has nearly the same usecase as the doctor, they can update the medical record after receiving authorization from the user, and they can also host x-ray images to reduce the size of the medical record on the network.

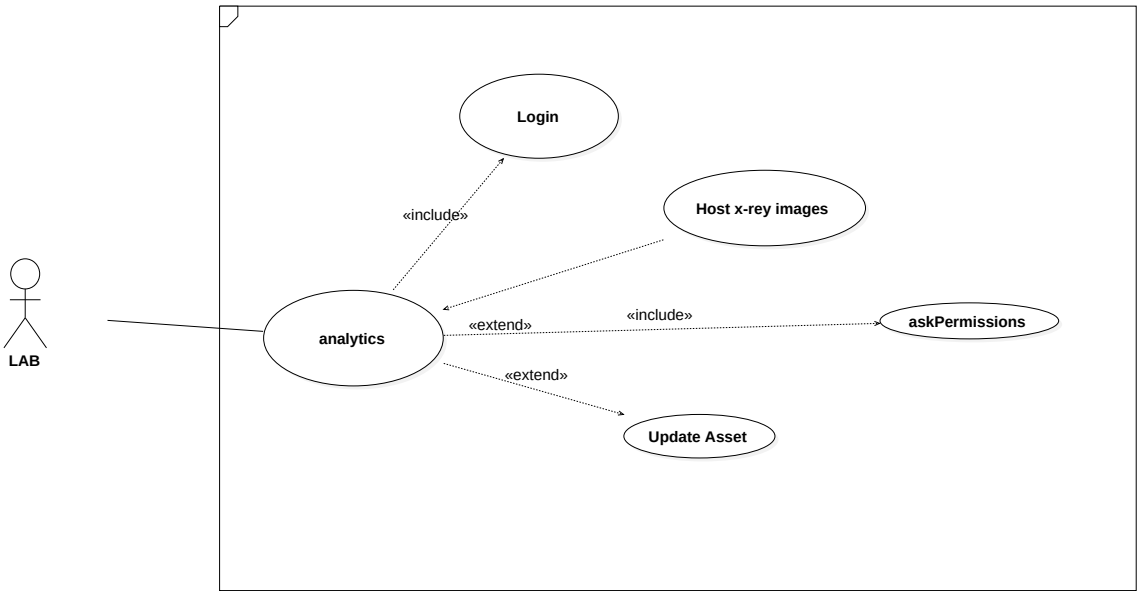

Figure 3.4: Lab Use Case Diagram

5.1.4 Patient use case

The patient has access to his medical record, but he is unable to edit or modify it. The patient has the authority to grant or revoke access to any other system actor (doctor and lab) more details in the table 3.4.

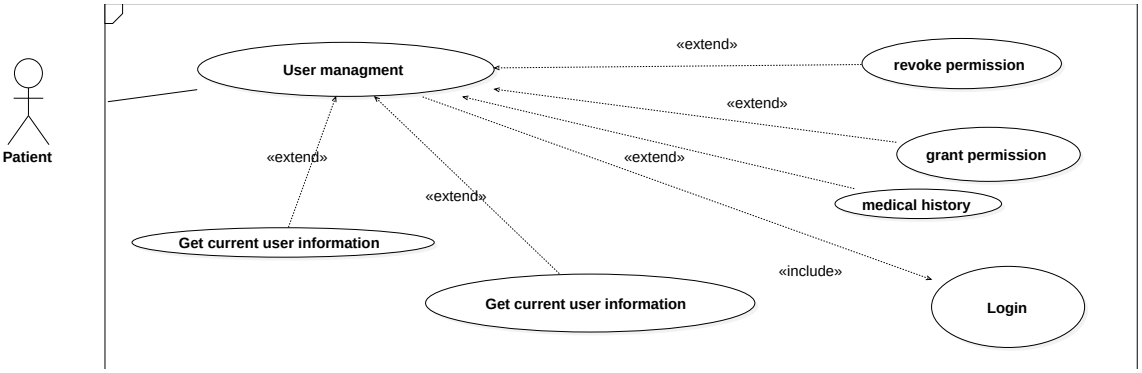

Figure 3.5: Patient Use Case Diagram

Use case	Grant permission Use Case
Primary actor	Patient
Stakeholders	1. The patient wants to give authorization for previous records. 2. The doctor is willing to look over the patient's records. 3. LAB to Update medical record user
Preconditions	1. Login 2. LAB/Doctor obtains proper EHR authorisation .
Post condition	doctor and lab should have access to the patient medical record

Table 3.4: Grant permission Use Case Case.

5.2 Flowchart

The read and update medical record operation, as well as the various logic and procedures utilized to secure the operation, will be described in this flowchart. First, a user will make a request for a medical record. When the request is processed, the system will check the role of the user who made the request. If the user is a patient, the system will check the user ID to see if it matches the medical record key. If it does, the user will receive a response with the medical information otherwise, the user will be redirected to another page. If the user is a lab or a doctor, the system will check for permeation, and if it is, he will be able to continue and get medical record information. If not, he can ask the patient for approval. The user will be redirected if the patient does not authorize him. The doctor or laboratory can then update the medical record, and only them who can submit the modification to blockchain they will be notified if an error occurs.

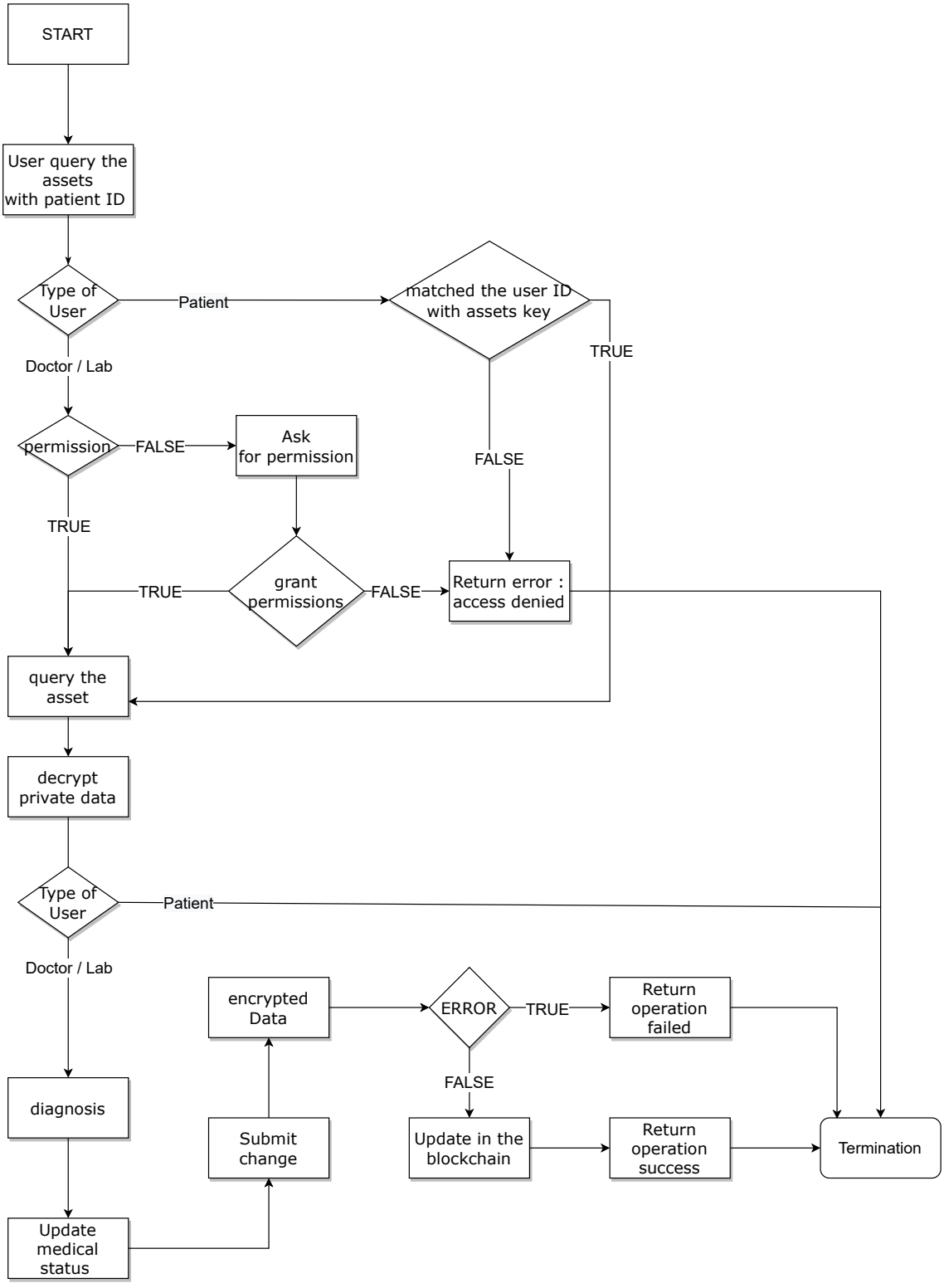

Figure 3.6: Flowchart of the process

5.3 Sequence diagrams

It sequentially represents the course of processing and interactions between the elements of the system and / or its actors.

5.3.1 Get user information

Only the user with the same id as the medical record and the doctor/Lab with permission have the rights to access the medical record, described in the section 5.2 too.

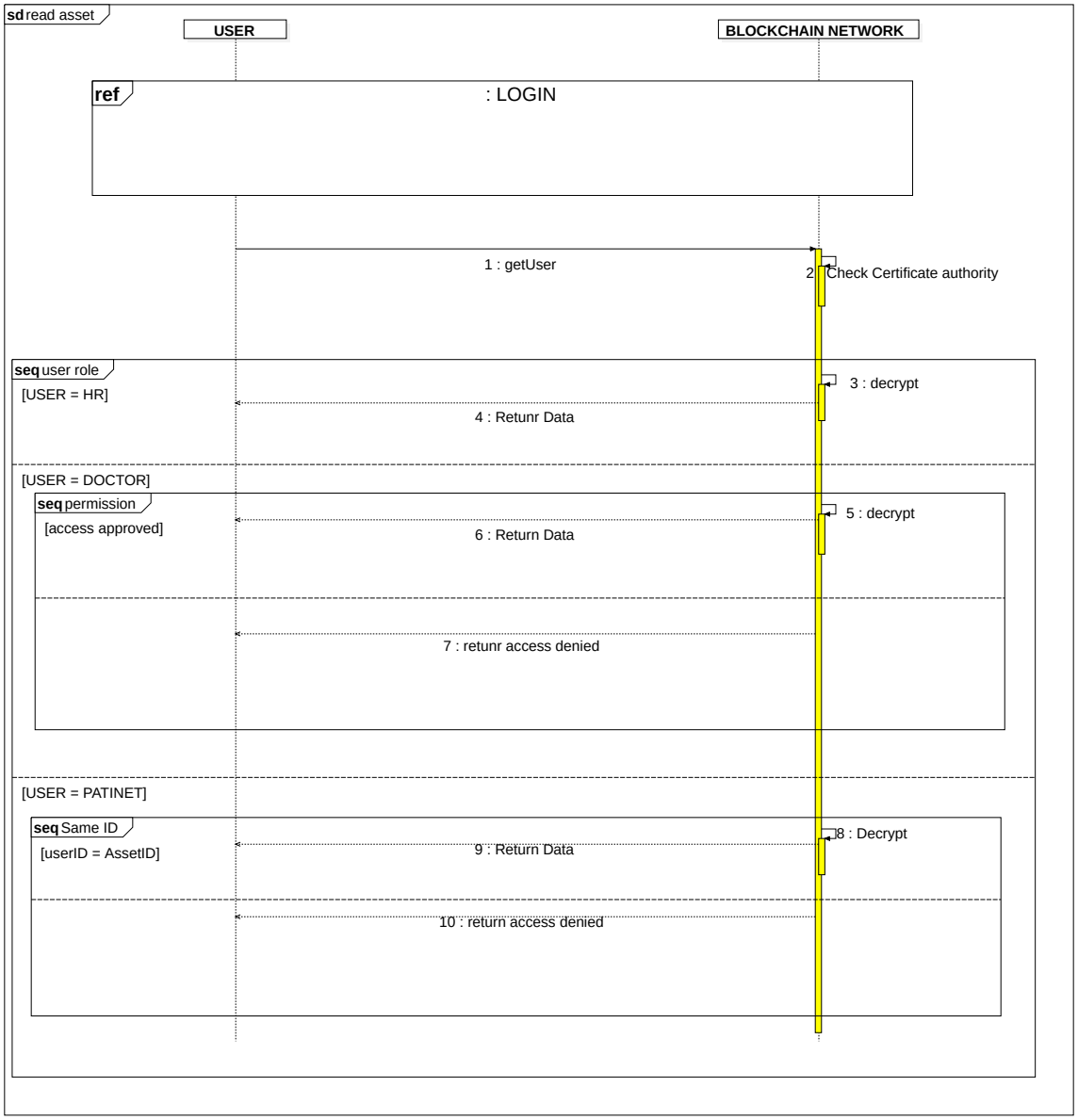

Figure 3.7: Read user information

5.3.2 Update medical record

The doctor and lab can submit their evaluation in the medical record after logging in and reading it, and then transmit it to the blockchain. The doctor can then request radio and X-ray pictures straight from the laboratory.

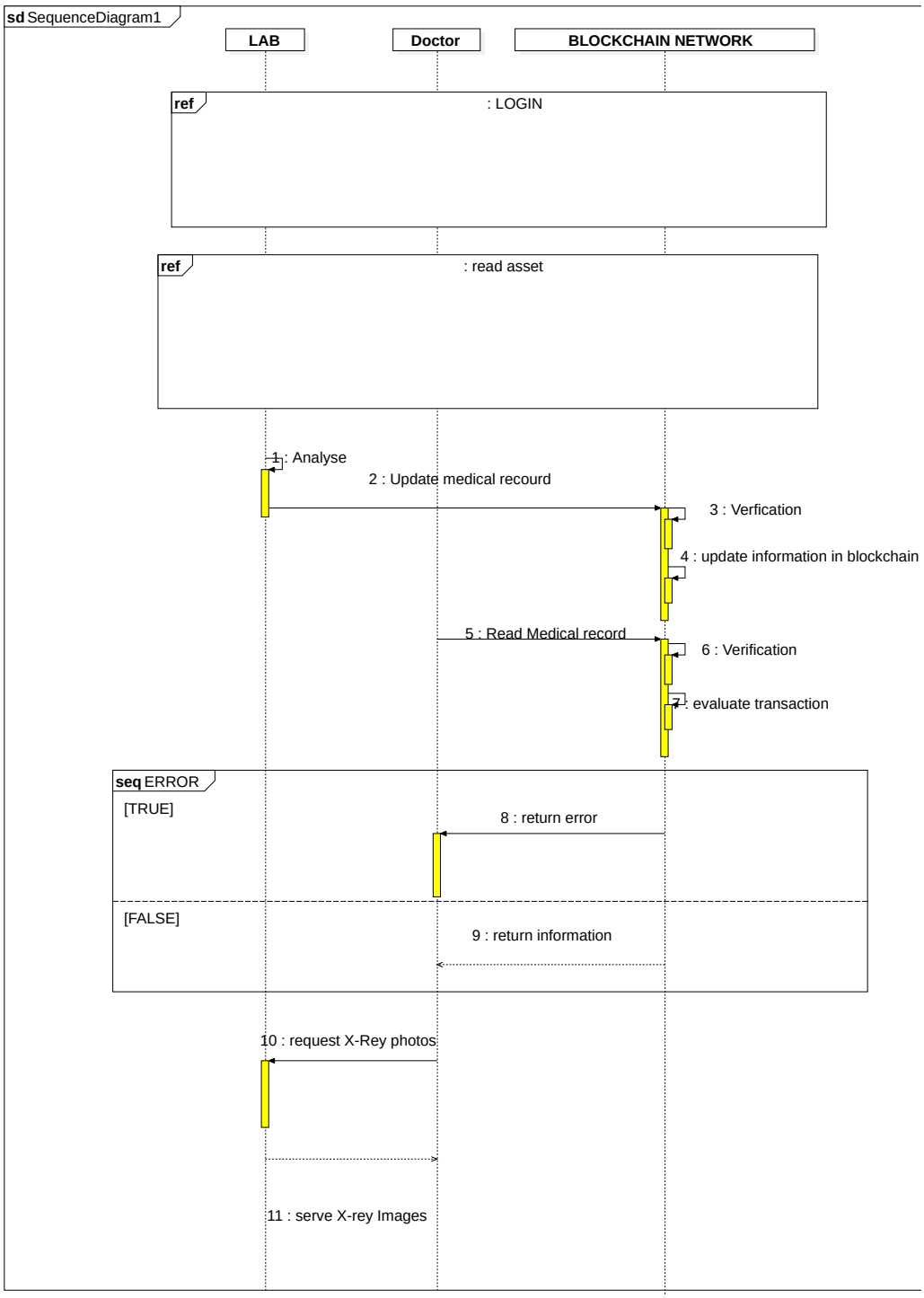

Figure 3.8: Update medical record

5.4 Class diagram

5.4.1 System class diagram

With the help of the class diagram, we implemented the system, it shows that all actors inherit from the user and have different methods to call, the patient is associated to a medical record, a patient can have one or multiple medical record, and a medical record belongs to only one patient.

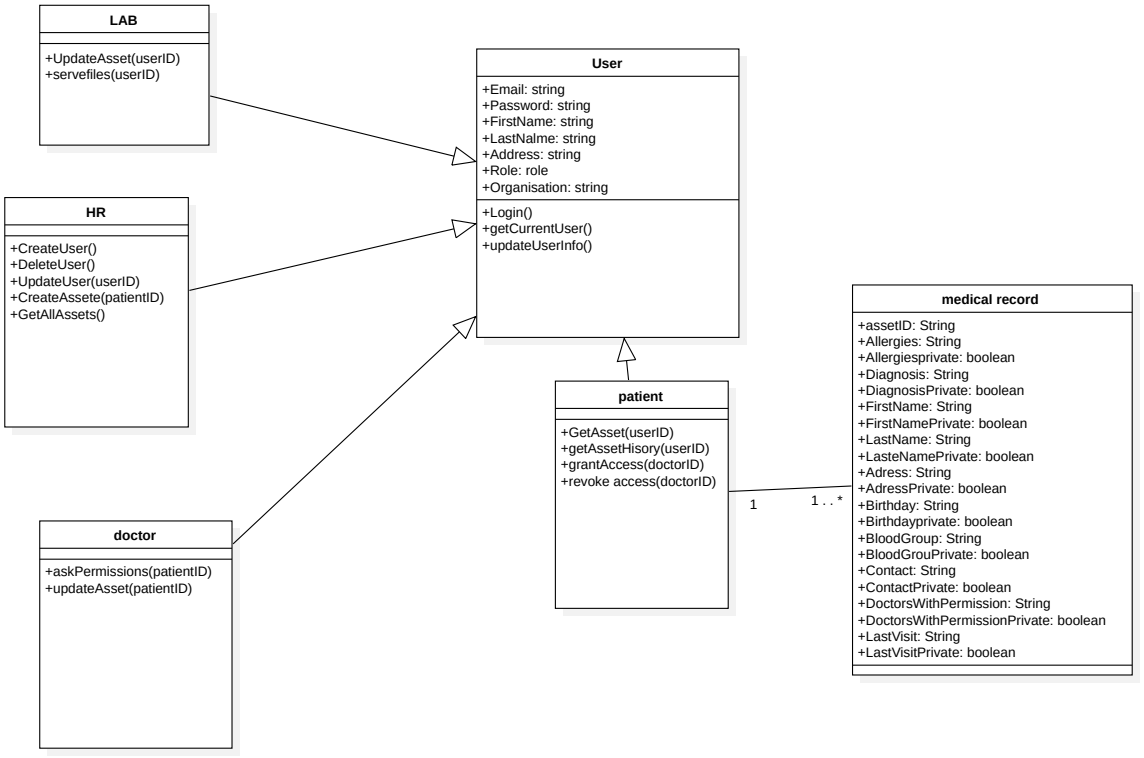

Figure 3.9: System class diagram

5.4.2 Chaincode Hierarchy

This section will show how each actor's blockchain methods are used. We limited some functionality to make the system more safe, such as the HR can not see the medical record and the patient is unable to change his medical record.

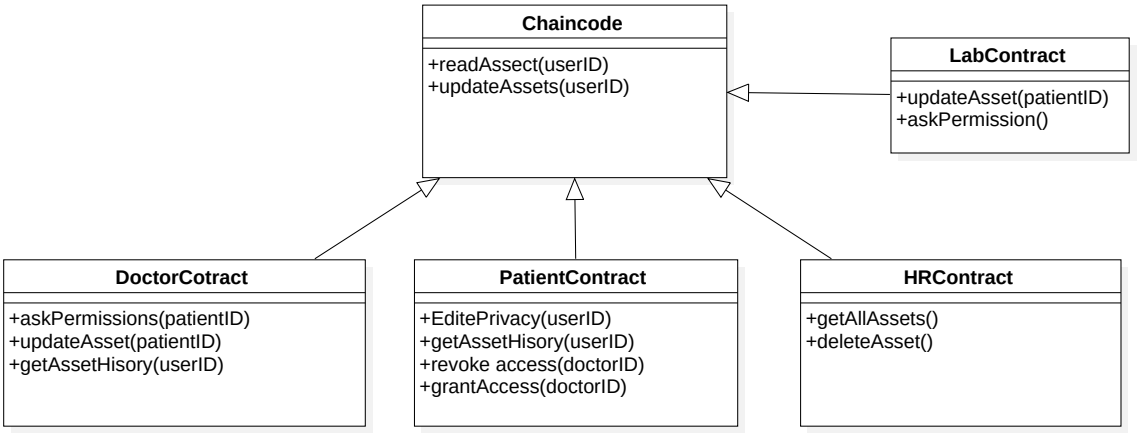

Figure 3.10: Chaincode Hierarchy

6 Stored data format and structure

All health files are saved on the blockchain, and user personal information is stored throughout couchDB all in the blockchain network.They are transformed to basic JavaScript objects and sent to the client as simple JSON objects.

Figure 3.11 illustrates how the EHR data delivered to the client is saved in JSON format.


```
{
  "message": {
    "Allergies": "Pollen Allergy.",
    "Allergiesprivate": true,
    "Diagnosis": "Food poisoning",
    "Diagnosisprivate": true,
    "bloodGroup": "AB+",
    "bloodGroupprivate": true,
    "doctorsWithpermissionprivate": true,
    "lastVisitsprivate": true,
    "radio": "[\"http://host:8081/uploads/9244bd6a-945c-4adb-a0c5-c3dc7ef3f424/2022-6-16-39/image-1655375964645.png\",\"http://host:8081/uploads/9244bd6a-945c-4adb-a0c5-c3dc7ef3f424/2022-6-16-39/image-1655375964646.png\"]",
    "radioprivate": true,
    "report": "madji",
    "reportprivate": true,
    "symptoms": "vomiting diarrhoea, which may contain blood or mucus stomach cramps and abdominal pain a lack of energy and weakness loss of appetite",
    "symptomsprivate": true,
    "treatment": "NHS hearing aids",
    "treatmentprivate": true
  }
}
```


Figure 3.11: JSON data for single EHR information

Figure 3.12 shows how user personal information are stored in JSON format and provided to the client.

Figure 3.12: JSON data for user personal information

7 Conclusion

In this chapter, We described our proposed architecture as well as the relationships that exist between the various actors and their interactions with the system and clarified the data structure. we've been able to create a EHR application by adapting UML diagrams such as the use case diagram, sequence diagram, and class diagram. in the following chapter, we discuss the implementation and our contribution of how to make the system more efficient.

Chapter 4

Implementation and Evaluation

1 Introduction

This chapter will discuss the application development process, including system implementation, development tools, and screen captures of the finished program. Finally, we will discuss future work that can be done and added to this system.

2 Blockchain development frameworks

2.1 Hyperledger

Hybrid blockchains are those that are managed by a single entity but have some oversight from the public blockchain, which is necessary to conduct certain transaction validations. IBM Food Trust is an example of a hybrid blockchain, which was created to improve efficiency across the whole food supply chain. In a subsequent piece in this series, we'll go through IBM Food Trust in further depth [81].

2.2 Ethereum

Ethereum is an open source Blockchain platform that enables anybody to create and deploy Blockchain applications. In an Ethereum Distributed Environment, any type of application, including cryptocurrency, tokens, wallets, social apps, and so on, can be designed and deployed. In other words, rather than focusing solely on Bitcoin, Ethereum extended the capabilities of 'blockchain' and 'distributed ledger' technology

to a broader range of applications [82].

2.3 Multichain

Multichain is a free and open source blockchain technology that allows you to establish private and permissioned blockchain networks. The bitcoin core software has been updated to create Multichain. To Multichain, the bitcoin engine gives security and control over peer-to-peer connections [82].

2.4 Corda

Corda is a distributed ledger platform that was created with the financial industry in mind. It's an open source platform that can be used to create financial institution-specific apps. It's a password-protected private network for recording, managing, and synchronizing contracts and other shared data amongst partners. The R3 consortium, which is made up of more than 70 financial institutions, oversees Corda. Corda is a distributed ledger system, not a blockchain, according to R3. R3 is, in fact, a framework for designing and deploying distributed apps for a variety of financial scenarios. CorDapps are the distributed apps produced with Corda. DemoBench is a Corda-provided stand-alone desktop application for configuring and launching local Corda nodes. It's a handy tool for training sessions for CorDapp development [82].

Characteristic	**Ethereum**	**Hyperledger Fabric**	**Corda**	**EOSIO**
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Block.one
Mode of operation	Permissionless	Permissioned	Permission	Permissioned
Consensus	Mining based on proof-of-work (PoW). - Ledger level.	Broad understanding of consensus that allows multiple approaches - Transaction leve	pluggable	Delegated Proof of Stake
Smart contracts	Smart contract code (Solidity)	Smart contract code(Go, Java)	Smart contract code (Java or Kotlin.)	Smart contract code(C++)
Currency	Ether	None	None	None

Table 4.1: Comparison of Ethereum, Hyperledger [12][13]

3 Hyperledger

Hyperledger is a collection of open source tools and subprojects that make up one of the largest blockchain projects, it is made up of business executives who seek to create a solid, business-driven blockchain architecture. It's an umbrella project with the goal of providing enterprise solutions as well as universal blockchain deployment instructions.

Hyperledger Fabric, Hyperledger Iroha, Hyperledger Indy, Hyperledger Sawtooth, Hyperledger Cello, Hyperledger Explorer, and Hyperledger Composer are the core projects of the Hyperledger framework [83][9].

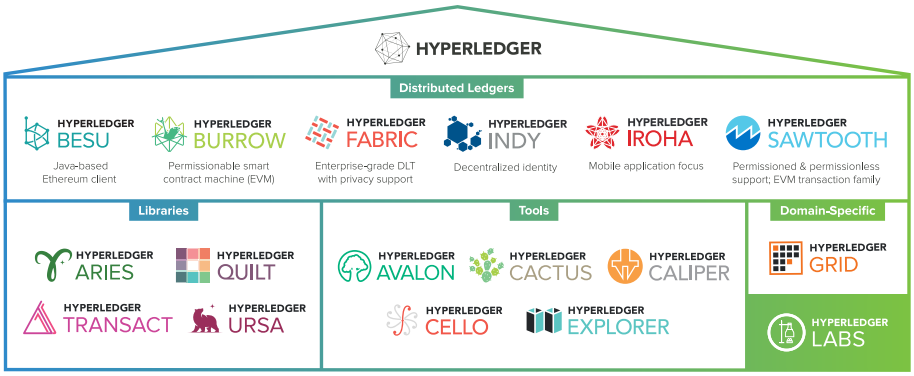

Figure 4.1: HL Greenhouse [9].

4 Hyperledger Frameworks

Enterprise blockchains are built using Hyperledger business blockchain frameworks with the goal of creating a consortium of organizations. They differ significantly from public ledgers such as the Bitcoin blockchain and Ethereum. The Hyperledger frameworks contain smart contracts for processing transaction requests, a consensus mechanism for agreeing on changes to the ledger, an append-only distributed ledger, and permissioned access for transaction privacy.

The different Hyperledger Frameworks are as follows:

4.1 Hyperledger Fabric

Hyperledger Fabric is an enterprise-grade distributed ledger platform that provides modularity and flexibility for a wide range of industry use cases. The Hyperledger Fabric modular architecture supports a wide range of enterprise use cases with plug-and-play components such as consensus, privacy, and membership services [84].

4.2 Hyperledger Burrow

The Linux Foundation hosts the Burrow Hyperledger Project. It enables a Blockchain client to create a permitted smart contract machine with EVM specifications (Ethereum Virtual Machine).

Burrow offers high transaction throughput and transaction finality thanks to its proof-of-stake consensus engine. A consensus engine, smart contract application, application Blockchain interface, application binary interface, and API gateway are among the features of Burrow [85].

4.3 Hyperledger Indy

Hyperledger Indy is a distributed ledger that focuses on decentralized identity. Its goal is to accomplish this by developing and deploying autonomous digital identities on blockchains for interoperability with any DLT that supports them by offering tools, artifacts, libraries, and reusable components that are independent of any ledger. People, not corporations, are in command of their own privacy and disclosure using Hyperledger Indy, which is a unique characteristic [85][86].

5 Hyperledger Tools

Hyperledger tools or modules are additional software that aids in the maintenance and deployment of blockchains. They're also used to check and double-check ledger data, and used to build, test, and develop blockchain networks. Let's look into the various Hyperledger tools:

5.1 Hyperledger Caliper

Hyperledger Caliper is a blockchain benchmarking tool that allows users to assess a blockchain implementation's performance against a set of predefined use cases. Hyperledger Caliper will generate reports with a number of performance indicators for use with Hyperledger Besu, Hyperledger Burrow, Ethereum, Hyperledger Fabric, FISCO BCOS, Hyperledger Iroha, and Hyperledger Sawtooth blockchain solutions [87].

5.2 Hyperledger Cello

Hyperledger Cello aims to act as a Blockchain operational dashboard, reducing the time and effort necessary to create, manage, and use blockchains. It can also be utilized to make Blockchain as a Service easier to create. Cello provides a management console for efficiently maintaining blockchains on a variety of infrastructures, including baremetal, virtual machines, and multiple container platforms [88].

6 Hyperledger Fabric

Hyperledger Fabric is a Hyperledger project and a blockchain framework implementation from the Linux Foundation. This framework is popular because it provides for plug-and-play components such as consensus and membership services. It allows container technology to host smart contracts, often known as "*chaincode*", which form the logic of the system [89].

Hyperledger Fabric use chaincode container technology to host smart contracts. Chaincode contains the system's application logic. It is currently one of the most secure and enterprise-ready blockchain development platforms available. RESTful APIs are used to run all queries in Hyperledger Fabric. Hyperledger Fabric supports enterprises with trust, accountability, and transparency, as the architecture delivers IBM Blockchain Platform [90].

It is open-source and executes defined smart contracts, as well as providing robust security and identification features. The peers execute protocols in the ledger. There are two types of peers validating and non-validating.

6.1 Membership Service Provider (MSP)

MSP stands for Membership Service Provider, and it is a Hyperledger Fabric component that abstracts membership activities. An MSP, in particular, abstracts away the cryptographic processes and protocols involved in issuing, validating, and authenticating users. An MSP can design its own concept of identity, as well as the rules that regulate (validate) and verify those identities (signature generation and verification). One or more MSPs can control a Hyperledger Fabric blockchain network. This allows membership operations to be modularized and interoperable across different membership standards and architectures [91].

6.2 Peer

A blockchain network is made up of a collection of peer nodes (or, simply, peers). Because they host ledgers and smart contracts, peers are critical components of the network. Remember that a ledger is a permanent record of all smart contract transactions.

In a network, smart contracts and ledgers are utilized to contain shared operations and information.

6.3 Consensus in Hyperledger Fabric

Endorsement, Ordering, and Validation are the three phases of Hyperledger Fabric consensus.

1. Members support a transaction based on a policy (for example, m out of n signatures) [10].

2. The ordering phase accepts the endorsed transactions and agrees to commit the order to the ledger [10].

3. Validation verifies the accuracy of a block of ordered transactions, including checking endorsement policy and double-spending [10].

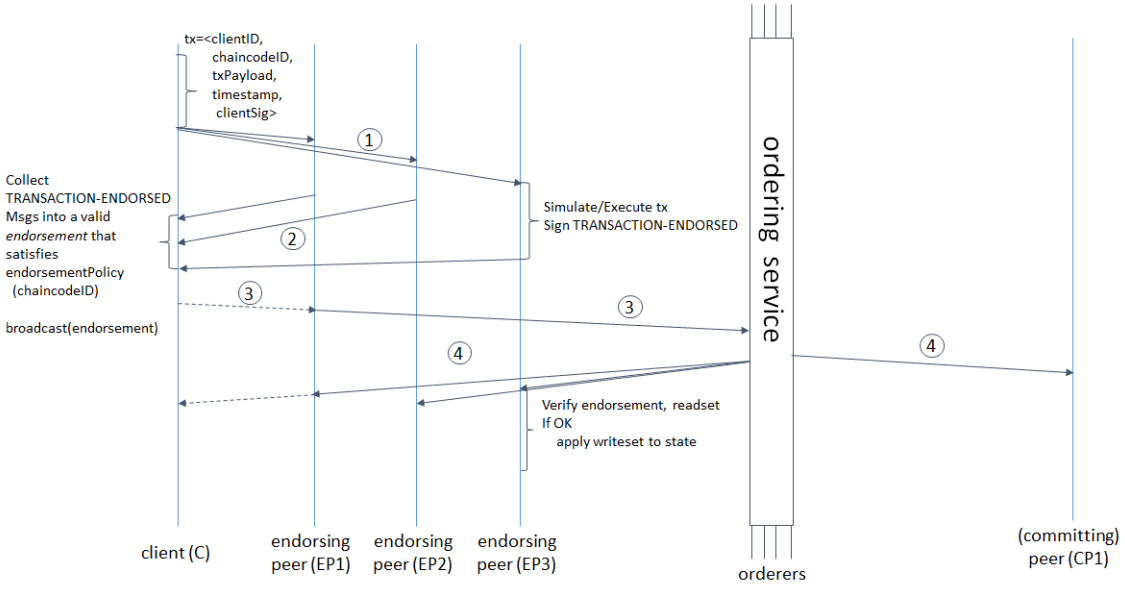

Figure 4.2: Transaction flow in Hyperledger Fabric [10].

7 Tools and developing environments

We used a number of tools and frameworks, as well as JavaScript, while developing the system.

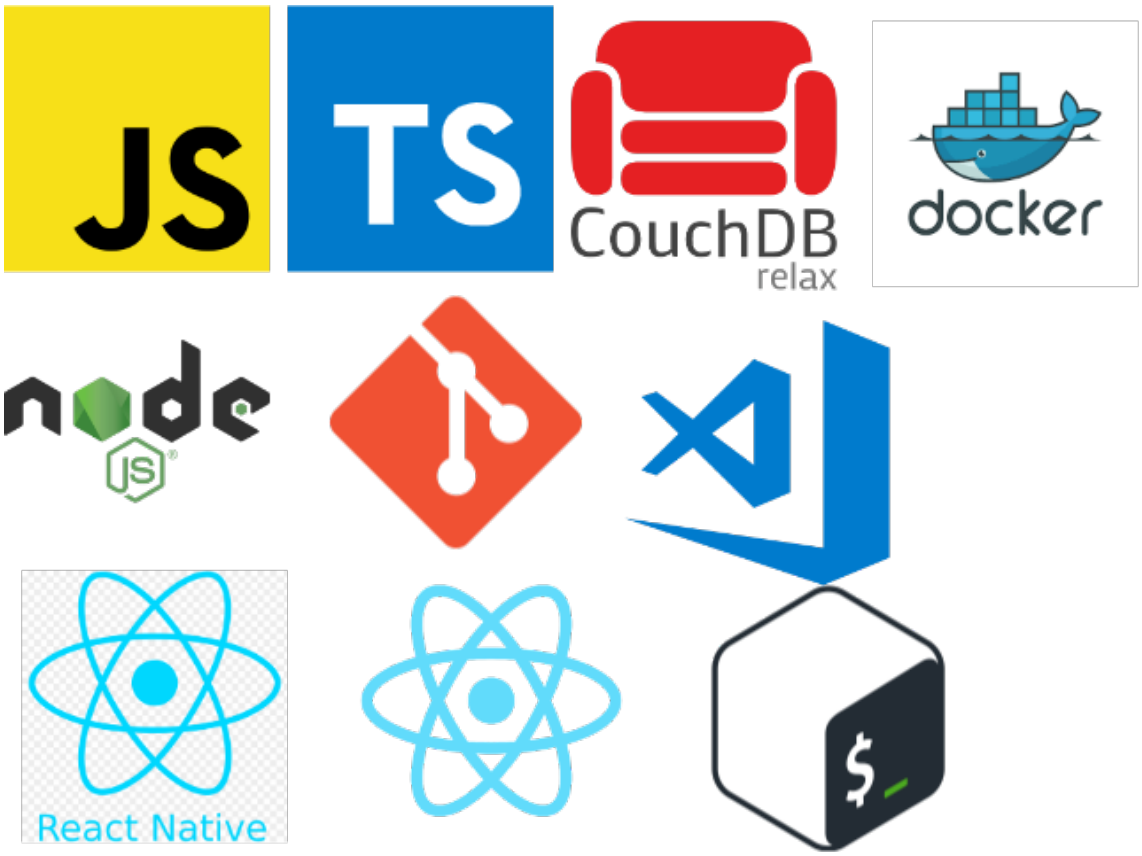

Figure 4.3: Tools and developing environments

7.1 Software development environment

7.1.1 Visual Studio Code

vscode is a open source editor developed by microsoft that is available for free. It contains built-in support for the programming languages JavaScript and TypeScript, as well as a rich ecosystem of extensions that enable support for other languages [92].

7.1.2 Doker

Docker is a full platform that includes the ability to create digital containers, which is the function with which it is most closely identified in casual conversation. Docker is designed to provide a fast and lightweight environment in which code may be run

efficiently, as well as an additional facility of the proficient work process to take code from the computer for testing before production [93].

CouchDB is a database that is entirely web-based. JSON documents can be used to store data. Using HTTP, you can access your documents through your online browser. With JavaScript, you may query, combine, and alter your documents. CouchDB is well-suited to current online and mobile applications. Using CouchDB's incremental replication, you may efficiently disseminate your data. CouchDB supports master-master configurations and detects conflicts automatically [94].

7.2 Developing languages

JSON

JSON is a data exchange language that is both human readable and easy to parse and utilize by machines. JSON is directly supported by JavaScript and is ideally suited for JavaScript applications, resulting in considerable performance improvements over XML [95].

YAML

YAML is mostly used for data serialization. Because XML was created to be backwards compatible with the Standard Generalized Markup Language (SGML), it was subjected to a number of architectural constraints that YAML does not. XML, which is based on SGML, is intended to support organized documentation, whereas YAML is more focused on data structures and messaging [96].

Bash

A Bash shell is nothing more than a command processor that executes scripts. it's a command interpreter that gives a user interface to the extensive range of UNIX utilities as well as a programming language that allows them to be integrated. The shell accepts commands from either a terminal or a file. It is possible to construct files that include commands and turn them into commands, allowing users or groups to create their own bespoke environments [97].

NodeJs

Node.js is JavaScript runtime environment built on top of Google's V8 engine. S0, it gives us a context in which we can create JavaScript code on any platform that supports Node.js. Anywhere [98].

JavaScript

JavaScript (JS) is a first-class programming language that is lightweight, interpreted, or just-in-time compiled. While it is best known as a scripting language for Web pages, it is also used in a variety of non-browser settings, including Node.js, Apache CouchDB, and Adobe Acrobat. JavaScript is a single-threaded, prototype-based, dynamic language that supports object-oriented, imperative, and declarative (e.g. functional programming) programming styles. Get more information about JavaScript.

TypeScripte

TypeScript is a JavaScript-based strongly typed programming language that provides improved tooling at any size.

Reactejs

React allows for the creation of huge, complicated online applications that can update their data without requiring further page refreshes. It serves as the View (V) in the Model-View-Controller (MVC) framework (MVC). The Document Object Model (DOM) is abstracted in React, resulting in a simple, fast, and reliable application development experience. React mostly renders on the server using NodeJS, with React Native providing support for native mobile apps. React has a unidirectional data flow, which reduces boilerplate and makes it more easier to use than traditional data binding [99].

React native

React Native is used to create cross-platform phone/tablet apps with a single code base. This means you can easily build code that runs on iPhones, iPads, and Android phones and tablets. without the need to rewrite it in two or more languages, only one. That one language is also simple to learn.If you're familiar with React and JavaScript,

because it's both. Furthermore, these apps are natively designed and run, as a result, they're more efficient and dependable [100].

Axios

Axios is a Javascript library that implements the Promise API inherent to JS ES6 and is used to make HTTP requests using node.js or XMLHttpRequests from the browser. It allows client-side protection against XSRF by intercepting HTTP requests and answers.

Fabric sdk

Applications can communicate with a Fabric blockchain network using the Hyperledger Fabric SDK. With minimum code, it provides a basic API for submitting transactions to a ledger or querying the contents of a ledger [101].

Fabric-ca-client

The Hyperledger Fabric CA is a Hyperledger Fabric Certificate Authority (CA). It has capabilities like identity registration and connects to LDAP as the user registry. Certificate renewal and revocation, as well as the issuing of Enrollment Certificates (ECerts) [101].

Fabric-network

to create APIs for connecting to a Fabric network, submitting transactions, and querying the ledger [101].

8 Hardware configuration

Materials	**Laptop**	**Desktop**
CPU	i5-6200u @ 2.50 GHz	i5 9400f
RAM :	8GO	16 GO
GPU: :	NVIDIA GeForce GTX 950m TI	NVIDIA GeForce GTX 1660 super
OS:	ARCH LINUX	Windows 10
STORAGE :	1Tb HDD ,125Go SDD	500 Go SDD

Table 4.2: Hardware Environment.

9 Blockchain Implementation

9.1 Chain code

The smart contract, or chain code in our example, can be found in the ***chaincode folder***, the typescript code can be found in the ***src folder***, which is divided into three files, the most important of which is **patient.ts**, and **fabric.ts**.

patient.ts: The block structure was defined in here. As shown in the figure 4.4. **fabcar.ts**: This is where logic and methods are developed. The methods in this file are:

1. `AssetExists(ctx, assetID)`
2. `checkPermissions(ctx: Context, patientID, DoctorID)`
3. `queryAsset(ctx: Context, patientID: string)`
4. `createAssets(ctx, assetID)`
5. `queryAllAssets(ctx, assetID)`
6. `DeleteAsset(ctx, assetID)`
7. `UpdateAsset(ctx, assetID)`
8. `GetAssetHistory(ctx, assetID)`

```
export class Patient {
    public value: string;
    public bloodGroup: string;
    public bloodGroupprivate: Boolean;
    public Allergies: string;
    public Allergiesprivate: Boolean;
    public Diagnosis: string;
    public Diagnosisprivate: Boolean;
    public treatment: string;
    public treatmentprivate: Boolean;
    public lastVisits: string;
    public lastVisitsprivate: Boolean;
    public doctorsWithpermission: string;
    public doctorsWithpermissionprivate: Boolean;
    public report: string;
    public reportprivate: Boolean;
    public radio: string;
    public radioprivate: Boolean;
    public symptoms: string;
    public symptomsprivate: Boolean;

}
```

Figure 4.4: Block structure pseudo-code

9.2 BlockChain deployement

To start the Blockchain network and deploy the chaincode, go to the ***fabcar folder*** folder and execute the following command.

```
./startFabric.sh  typescript
```

It will execute a bash script that we wrote and specify the language in which it was written with

Deployment timelines for the chain code

- Creating channel.
- Generating CCP files for the peers.
- Create and start docker images.
- Confirm creation of the channel.

- Compiling TypeScript code into JavaScript
- Package the chaincode
- Install the chaincode on peers
- confirm instalation
- Approve chaincode definition
- Success message

9.3 Setting up node SDK

First and foremost, we need the JSON file provided by the blockchain in 9.2 which contains the information to connect to the network, this file will help us to establish a connection to the gateway.

```
const ccpPath = path.resolve(
    __dirname,
    "..",
    "..",
    "..",
    "..",
    "..",
    "test-network",
    "organizations",
    "peerOrganizations",
    "org1.example.com",
    "connection-org1.json"
);
let ccp = JSON.parse(fs.readFileSync(ccpPath, "utf8"));
```

Figure 4.5: Reading CCP file

Then we need to check if the user who submitted the request has enrolled a wallet as a second security check.

```
const test = await wallet.list();

const identity = await wallet.get(currentUser);
if (!identity) {
    console.log(
        `An identity for the user ${currentUser} does not exist in the wallet`
    );
    console.log("Run the registerUser.js application before retrying");
    return;
}
```

Figure 4.6: Check to see if user wallet enrolled

Next we connect to the network, get the network **mychannel**, and the contract **fabcar** as shown in the figure 4.7.

```
const gateway = new Gateway();
await gateway.connect(ccp, {
    wallet,
    identity: currentUser,
    discovery: { enabled: true, asLocalhost: true },
});

// Get the network (channel) our contract is deployed to.
const network = await gateway.getNetwork("mychannel");

// Get the contract from the network.
const contract = network.getContract("fabcar");
```

Figure 4.7: Connect to the network

We call chaincode method by mentioning them in the *submitTransction* method followed by arguments, illustrated in the figure 4.8

```
await contract.submitTransaction(
  "createAssets",
  patientID,
  `${JSON.stringify(data)}`
);
```

Figure 4.8: Calling chaincode methodes

The final step is to disconnect from the gateway, code in figure 4.9

```
// Disconnect from the gateway.
await gateway.disconnect();
```

Figure 4.9: disconnect from the network

10 System interface

To better explain our proposed scenario, we assume a system having four actors, a patient, a doctor, and a lab representative (x-rays and analyses). Initially, The patient goes to the doctor seeking a treatment. So, he has to grant access to his doctor. In case the doctor suspects any issue, he addresses the patient to a lab and, or gets a full X-ray. After that, once the patient gets his X-rays, again, he grants another access to the lab to update his EMR. Then, the doctor gets notified. And he reviews the patient's medical history and to make decisions accordingly. This can be happen without the need for the patient to move to the doctor or carrying any sheet of paper.
Next, we'll look at the interface and a full overview of the system.

10.1 Patient part

The best way to make our system more practical is to run the patient application on mobile device, which we consider that will be helpful and handy, particularly for elder people.

Based on the proposed scenario we introduce our application by showing the most important user interfaces, thus we start by the authentication user interface illustrated in Figure 4.10 . Figure 4.11 shows the home page of the application where patients can see there previous medical records.

By using the navigation in the bottom, the user can find out which facilities and doctors are using this system.

In the doctors page, patient can choose from many doctors in the list. When he clicks on the doctor he wants, a pop-up window will appear with doctor information and a button to give this doctor access to the patient's medical records this process is illustrated in figures 4.12 and 4.13

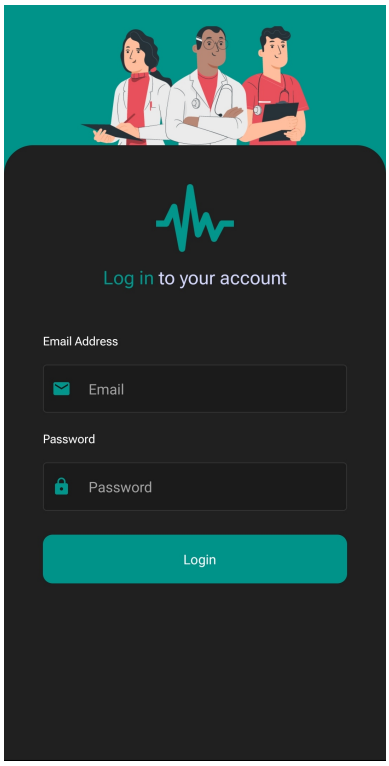

Figure 4.10: Login interface

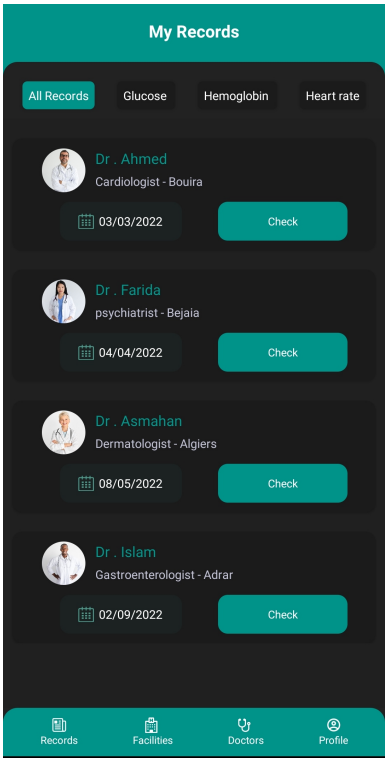

Figure 4.11: Home Interface

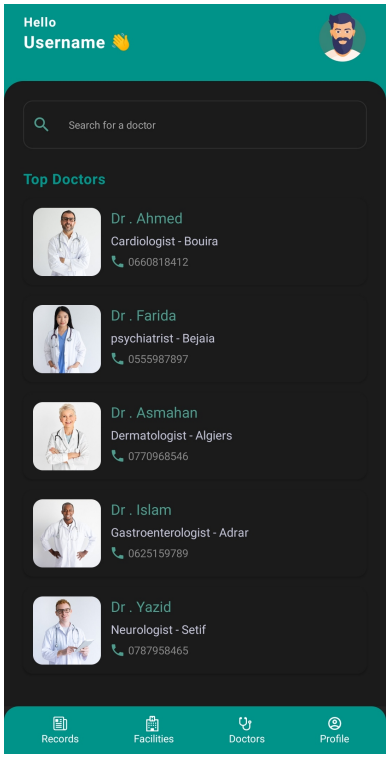

Figure 4.12: List of doctors

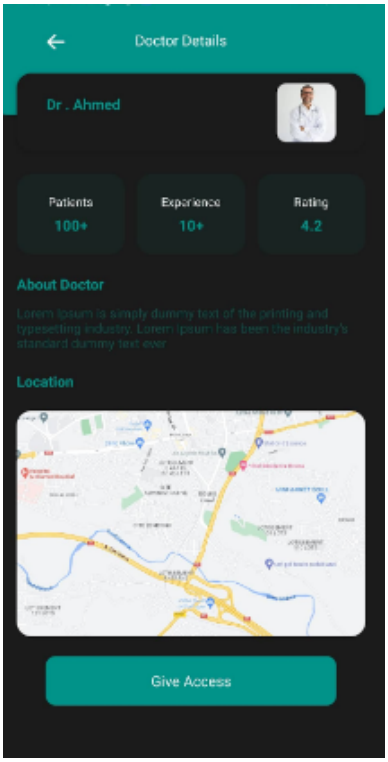

Figure 4.13: Doctor information

10.2 Doctor part

When a patient grants access to a doctor, the doctor can find him in his dashboard interface, as shown in figure 4.14, and when he clicks on a patient, he can see his personal stats see figure 4.15.

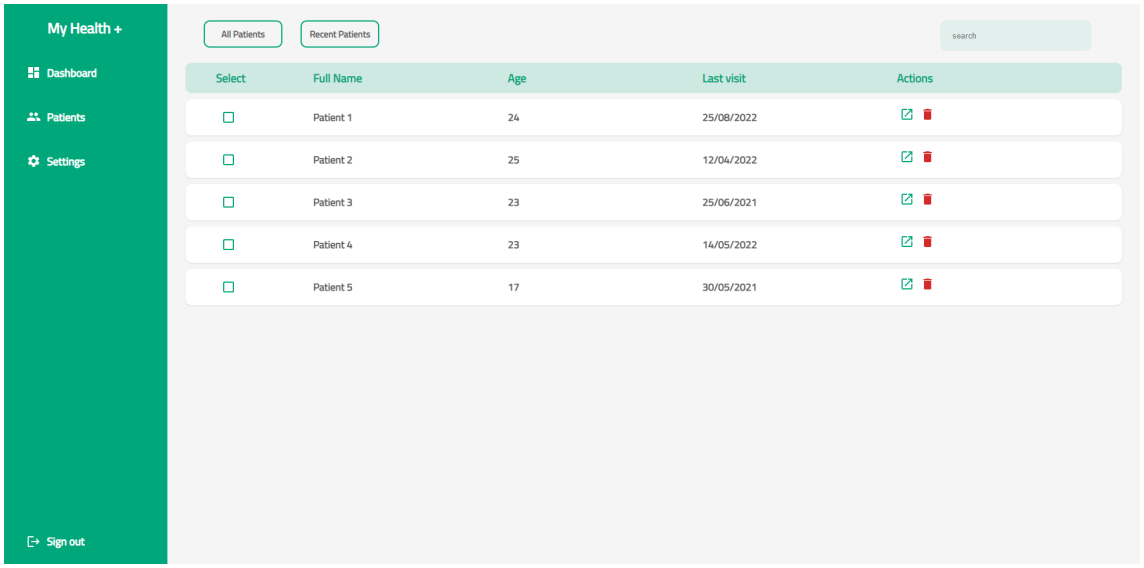

Figure 4.14: Doctor's dashboard interface

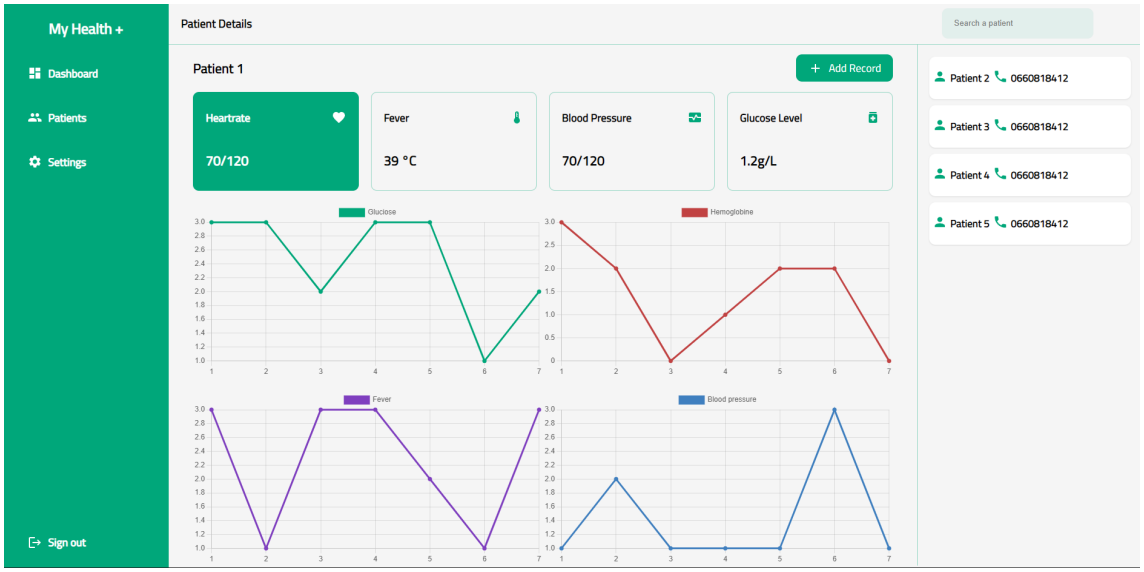

Figure 4.15: Patient health stats

The doctor can update and write in the medical record after the diagnosis, using the input fields offered to help with the process. like shown in figure 4.16.

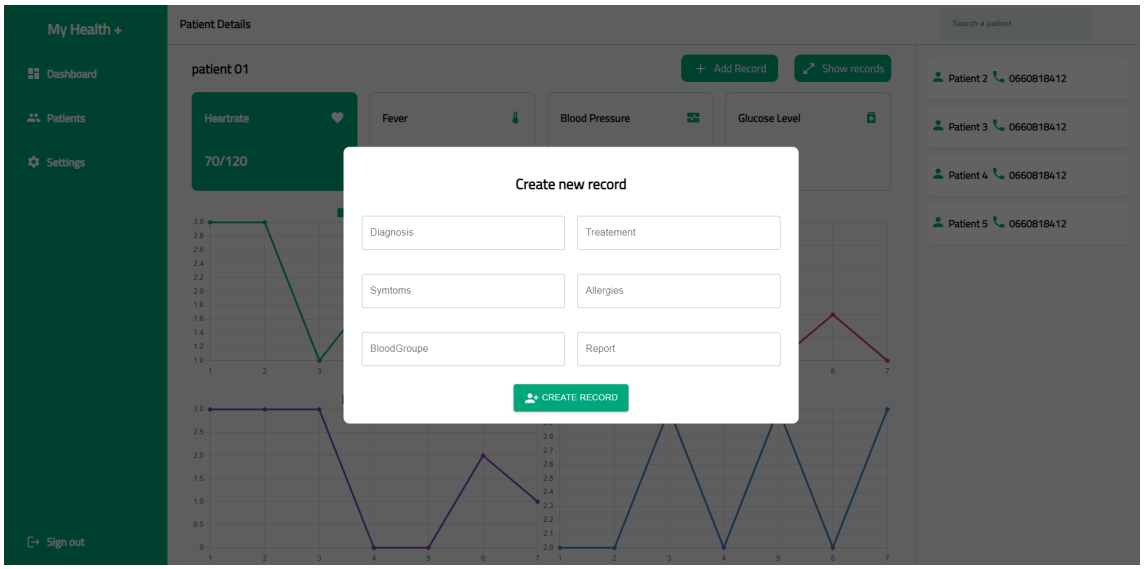

Figure 4.16: Doctor inputs fields

10.3 Lab Part

Finally, the Lab, he got the same dashboard as the doctor (figure 4.14). He can only edit two fields in the medical record, the radio image link and the lab report shown in the figure 4.17.

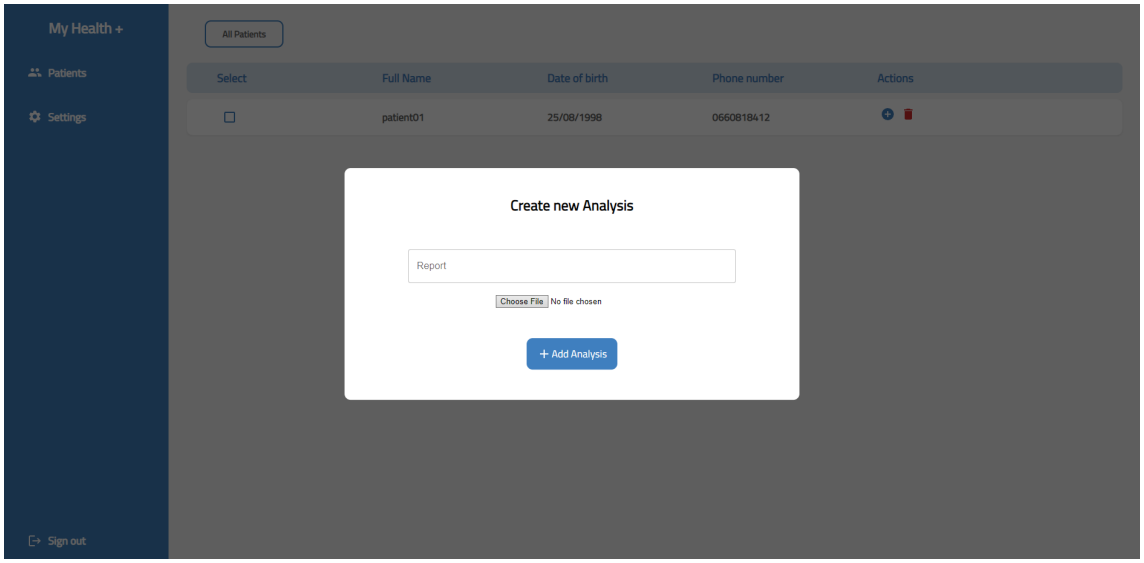

Figure 4.17: laboratory inputs fields

11 Test environment and results

We used Linux as an operating system, docker with 4 CPUs and 8 GB of RAM, and hyperledger fabic 2.2 with default peers storage to test our system.

11.1 Metrics of evaluation

We consider both Latency and Throughput when evaluating the performance of our proposed design.

11.1.1 Latency

The latency of a distributed system generally consists of three components, as shown in the following formula: the time necessary for the transaction request data to be transferred over the network (TRequest), the time required for the witness nodes to establish a consensus (TConsensus), and the time required for the processing result to be returned (TResponse) [102] [103].

$$DelayTransaction = TRequest + TConsensus + TResponse \quad [103].$$

11.1.2 Throughput

For the evaluation of distributed systems, transaction throughput is an important output parameter.

The number of simultaneous transactions and the number of transactions per second are used to calculate the system's throughput (TPS). The time spent on a transaction is the time it takes from the client's request to the server's response. The system's overall efficiency is determined by the module with the lowest transaction processing capacity. TPS refers to the number of transactions that a distributed system can handle in a given amount of time. [102] [103].

$$Tps(Dt) = SumDt(Transactions)/Dt \quad [103].$$

Where Dt is the amount of time spent processing transactions, SumDt(Transactions) denotes the number of transactions completed during Dt, and Tps(Dt) denotes the

amount of TPS earned during Dt [102] [103].

11.2 Scalability performance evaluatin

For both blockchain and centralized systems, 5000 test is performed with various send rate to determine latency , table 4.3, and 4.4 show the test results.

Send Rate	Succ	Throughput (TPS)	Latency (s)
100	5000	100	0,06
500	5000	162	0,07
1000	5000	162	0,07
2000	5000	163	0,05
3000	5000	163	0,07

Table 4.3: Throughput and Latency per number of Send Rate in blockchain

Send Rate	Succ	Throughput (TPS)	Latency (s)
100	5000	99	0,06
500	5000	100	0,1
1000	5000	91	0,27
2000	5000	70	0,58
3000	5000	37	0,68

Table 4.4: Throughput and Latency per number of Send Rate in a centralized system

As illustrated in Figure 4.18, the average latency between the two systems .The latency in the blockchain system appears to be constant at 0.07S, whereas the delay in the centralized system is increasing as the send rate increases, indicating that due to the nature, differences, and architecture of both systems,the operation in a centralized system is performed on a single server, and the more load on that server, the longer it takes to complete a transaction. On the other hand, the operation is performed on several nodes.

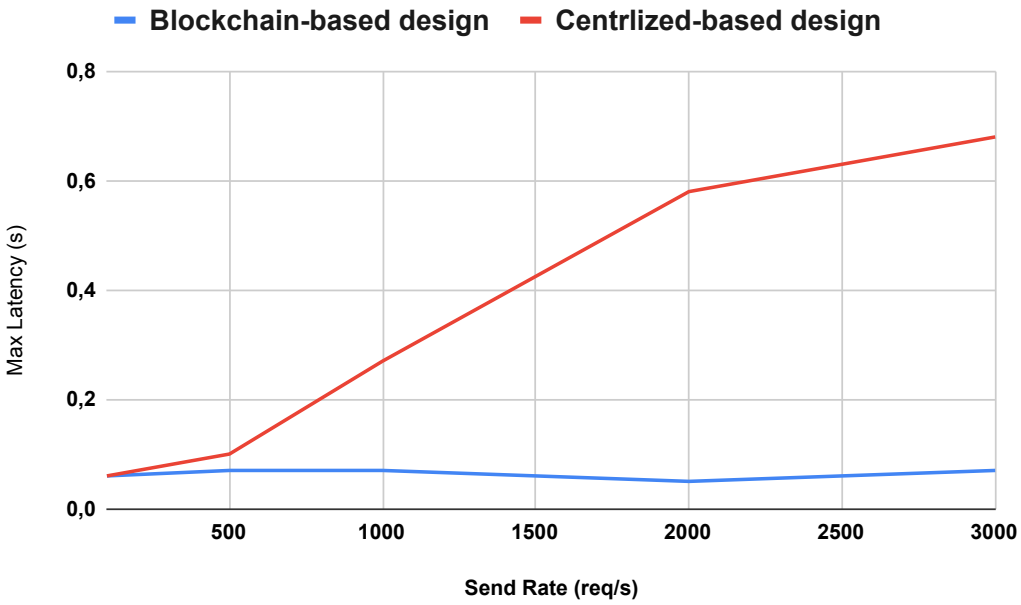

Figure 4.18: Latency in centralized vs blockchain

11.3 Storage efficiency evaluation

For the second test, we wanted to demonstrate how well our system handled a lot of data, particularly images (x-rays). We took some images with an average file size of 50 kilobytes, and we measured how much space the medical record will take up when the image is hosted from the lab and when it's converted to a blob and saved in the record. The table 4.5 shows the outcomes.

Number of image in the medical record	Size of Medical record with image links (bytes)	Size of Medical record with blobs (bytes)
1	750	60870
2	857	121103
5	1185	301791
10	1725	602937
15	2265	904083
20	2805	1205229

Table 4.5: Size of medical record with different number of X-ray images

Figure 4.19 shows the difference between the two techniques, we can see that when images are stored in the blockchain, a large space is required even for a single image and can take up to 1.1 MB if the patient performed different analyses, the total size depends on the size of the original image, if the original image is large in size ,then the total size will increase. This has an impact on the blockchain system's performance, slowing it down and interfering with doctors' work, particularly with patients suffering from complex illnesses.

However, in our the size is particularly modest and that's because we developed a mechanism where the images are hosted in the laboratory peer, so when a doctor requests something from the blockchain, he will simply query links, from which he can obtain photographs. this will make the response from the network very fast due to the small size of the medical record, and that's make our system more lightweight.

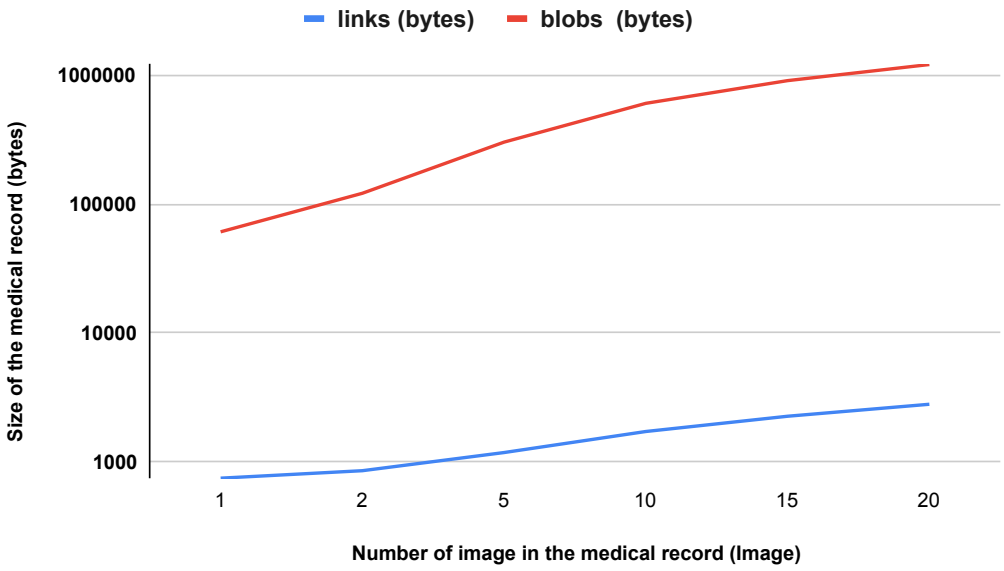

Figure 4.19: Size of Medical record with image links and with blobs (bytes)

12 Conclusion

In this chapter, we implemented the electronic health record using the tools and programming languages mentioned previously, and we successfully presented a blockchain-based EHR system that respects patient privacy, as well as a comparison between a blockchain app and a traditional app.

Conclusion and Future Work

In our thesis, we explored the issue of storing private and sensitive information across multiple facilities, in healthcare systems which has led to a lack of control over data collection and storage, making it hard for patients to get their medical records from different organizations and for doctors to have a precise stats about their health.

In order to find a solution, we looked into blockchain which allow for a secure and fully transparent storage and transmission of data without the need to edit or erase the data.

We were able to deploy a blockchain-based EHR network and implement basic functionalities as part of our task of developing a system for managing electronic patient health records using blockchain technology. We developed a system that includes a mobile app for the patient and a web app for the healthcare provider.

A decentralized application for EHRs was created using Hyperledger Fabric that meet some requirements such as information privacy, secure data access, and information sharing. We were able to minimize the size of the medical record by hosting a serving images from nodes.

We were successful in accomplishing the primary goal of this thesis, which was to secure electronic health records and protect patients' privacy using the primary properties of blockchain, namely cryptography/hashing and decentralization.

Although there are many ways to improve the solution, we concentrated on information exchange between patients and hospitals. However, a comprehensive EHR system should incorporate not just patients and hospitals, but also numerous government medical departments. More features and roles, as well as more intensive cloud infrastructure testing we can try to expand this system, which relevant government medical departments and. Electronic payment.

we can extend the current smart contact and the addition of others to improve the lookup and support the additional features required by an EHRs management solu-

tion. A messaging system can be implemented for more data sharing.

More improvements could be made, such as incorporating IA for better personalized treatment and decision support. The use of machine learning to prevent chronic disease ,Big Data Analytics, which helps in the creation of a continually learning ecosystem and IOT for just in time.

REFERENCES

[1] H. Dalianis, "The history of the patient record and the paper record," pp. 5–12, 2018. doi 10.1007/978-3-319-78503-5_2 , Springer.

[2] P. Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks*. ASIN : B000TQB7JS, Jan 1964.

[3] S. Jaganathan and K. Veeramani, "A quick synopsis of blockchain technology," *International Journal of Blockchains and Cryptocurrencies*, vol. 1, p. 1, 01 2019. doi : 10.1504/IJBC.2019.10021396.

[4] K. Salah and M. Khan, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, 11 2017. doi : 10.1016/j.future.2017.11.022.

[5] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T.-Y. Ni, *A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption*, pp. 988–1003. 01 2020. doi : 10.1007/978-3-030-12385-7_67.

[6] M. E. Wegrzyn and E. Wang, "Types of blockchain: Public, private, or something in between." `https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-betwee`.

[7] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021. doi : https://doi.org/10.1016/j.ijin.2021.09.005.

[8] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, p. 326, 01 2019. doi : 10.3390/s19020326.

[9] "What is hyperledger foundation?." `https://www.hyperledger.org/about`. Accessed: 2022-04-12.

[10] L. Foundation, "Hyperledger architecture, volume 1 introduction to hyperledger business blockchain design philosophy and consensus," 2018.

[11] D. A. M. A.-S. . S. Alasady, *Network Distributed Computing/ Lecture : 11*. University of Babylon/College of Information Technology/ Information Network Dept, 2017.

[12] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," *Frankfurt School Blockchain Center*, vol. 8, pp. 1–8, 2017.

[13] C. Nnamdi, "Top 6 blockchain development frameworks." `https://blog.logrocket.com/top-blockchain-development-frameworks/`. Accessed: 2022-04-15.

[14] "Dupage medical group notifying 600,000 patients about a data breach." `https://chicago.suntimes.com/business/2021/8/30/22649201/dupage-medical-group-notifying-patients-data-breach/`. Accessed: 2022-06-14.

[15] "The role of electronic management in improving public health services.." `http://dspace.univ-msila.dz:8080//xmlui/handle/123456789/10985`.

[16] "Algeria population." `https://www.worldometers.info/world-population/algeria-population//`. Accessed: 2022-05-12.

[17] "Digital 2021: Algeria." `https://datareportal.com/reports/digital-2021-algeria/`. Accessed: 2022-04-12.

[18] W. R. Hersh, "The electronic medical record: Promises and problems," *Journal of the American Society for Information Science*, vol. 46, no. 10, pp. 772–776, 1995. Wiley Online Library.

[19] G. Eysenbach *et al.*, "What is e-health?," *Journal of medical Internet research*, vol. 3, no. 2, p. e833, 2001. JMIR Publications Inc., Toronto, Canada.

[20] T. Seymour, D. Frantsvog, T. Graeber, *et al.*, "Electronic health records (ehr)," *American Journal of Health Sciences (AJHS)*, vol. 3, no. 3, pp. 201–210, 2012. doi : 10.19030/ajhs.v3i3.7139.

[21] T. Kelley, *Electronic Health Records for Quality Nursing and Health Care*. 2016. DEStech Publications, Inc.

[22] "What are the differences between electronic medical records, electronic health records, and personal health records?." `https://www.healthit.gov/faq/`

what-are-differences-between-electronic-medical-records-electronic-health-reco
Accessed: 2022-03-30.

[23] C. P. Waegemann, "Ehr vs. cpr vs. emr," *Healthcare Informatics online*, vol. 1, 2003.

[24] Y. Yamada, "The electronic health record as a primary source of clinical phenotype for genetic epidemiological studies," *Genomic Medicine*, vol. 2, no. 1, pp. 5–5, 2008. SpringerOpen.

[25] I. Hoden, "Advantages and disadvantages of ehrs." https://www.wheel.com/companies-blog/advantages-and-disadvantages-of-ehrs. Accessed: 2022-03-30.

[26] M. Chet Tharpe, "Types of ehr systems." https://www.wheel.com/companies-blog/types-of-ehr-systems. Accessed: 2022-03-30.

[27] E. Adel, S. El-Sappagh, S. Barakat, and M. Elmogy, "Distributed electronic health record based on semantic interoperability using fuzzy ontology: a survey," *International Journal of Computers and Applications*, vol. 40, no. 4, pp. 223–241, 2018. doi 10.1080/1206212X.2017.1418237 , Taylor Francis.

[28] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," *Journal of medical systems*, vol. 41, no. 8, pp. 1–9, 2017. Springer.

[29] W. Bani-Issa, A. Ibrahim, A. Akour, A. Marzouqi, Abbas, Hisham, and griffith, "Confidentiality, security and patient safety concerns about electronic health records," *International Nursing Review*, vol. 67, 04 2020. doi 10.1111/inr.12585.

[30] C. A. Ardagna, S. D. C. Di Vimercati, S. Foresti, T. W. Grandison, S. Jajodia, and P. Samarati, "Access control for smarter healthcare using policy spaces," *Computers & Security*, vol. 29, no. 8, pp. 848–858, 2010. Elsevier.

[31] Y.-Y. Chen, J.-C. Lu, and J.-K. Jan, "A secure ehr system based on hybrid clouds," *Journal of medical systems*, vol. 36, no. 5, pp. 3375–3384, 2012. Springer.

[32] R. S. Sumant Ugalmugle, "Electronic health record (ehr) market." https://www.gminsights.com/industry-analysis/electronic-health-record-market. Accessed: 2022-03-30.

[33] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in *2010 Second International Conference on eHealth, Telemedicine, and Social Medicine*, pp. 95–99, IEEE, 2010.

[34] A. H. Mayer, C. A. da Costa, and R. da Rosa Righi, "Electronic health records in a blockchain: A systematic review," *Health Informatics Journal*, vol. 26, no. 2, pp. 1273–1288, 2020. doi :10.1177/1460458219866350.

[35] A. Samad, M. Shuaib, and M. R. Beg, "Monitoring of military base station using flooding and aco technique: An efficient approach.," *International Journal of Computer Network & Information Security*, vol. 9, no. 12, 2017.

[36] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of things (iot) enabling technologies, requirements, and security challenges," in *Advances in data and information sciences*, pp. 119–126, 2020. Springer.

[37] A. Samad, S. Alam, S. Mohammed, and M. Bhukhari, "Internet of vehicles (iov) requirements, attacks and countermeasures," in *Proceedings of 12th INDIACom; INDIACom-2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi*, 2018.

[38] S. T. Siddiqui, S. Alam, Z. A. Khan, and A. Gupta, "Cloud-based e-learning: using cloud computing platform for an effective e-learning," in *Smart Innovations in Communication and Computational Sciences*, pp. 335–346, Springer, 2019.

[39] F. BOIANI, "Blockchain based electronic health record management for mass crisis scenarios," *KTH ROYAL INSTITUTE OF TECHNOLOGY SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE*.

[40] M. Van Steen and A. S. Tanenbaum, *Distributed systems*. Maarten van Steen Leiden, The Netherlands journal=Network, volume=2,, 2017.

[41] M. Rahman, R. Ranjan, and R. Buyya, "Decentralization in distributed systems: Challenges, technologies, and opportunities," *Advancements in Distributed Computing and Internet Technologies: Trends and Issues*, pp. 386–399, 01 2011. doi : 10.4018/978-1-61350-110-8.ch018.

[42] J.-P. Vergne, "Decentralized vs. distributed organization: Blockchain, machine learning, and the future of the digital platform," *Organization Theory*, vol. 1, pp. 1–26, 10 2020. doi : 10.1177/2631787720977052.

[43] "peer-to-peer file sharing." `https://itservices.usc.edu/files/2013/11/USC_P2P_brochuresingles.pdf`. Accessed: 2022-04-15.

[44] S. Jo, J. Lee, J. Han, and S. Ghose, "P2p computing for intelligence of things," *Peer-to-Peer Networking and Applications*, vol. 13, 02 2020. doi : 10.1007/s12083-020-00887-5.

[45] T. K. Sharma, "Role of p2p in blockchain." `https://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/`. Accessed: 2022-04-15.

[46] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, "Focus on blockchain: A comprehensive survey on academic and application," 2020. IEEE.

[47] S. Fosso Wamba, J. R. Kala Kamdjoug, R. Epie Bawack, and J. G. Keogh, "Bitcoin, blockchain and fintech: a systematic review and case studies in the supply chain," *Production Planning & Control*, vol. 31, no. 2-3, pp. 115–142, 2020.

[48] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," *International Journal of Production Economics*, vol. 231, p. 107831, 2021.

[49] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, pp. 533–546, 2016.

[50] A. Songara and L. Chouhan, "Blockchain: a decentralized technique for securing internet of things," in *Conference on Emerging Trends in Engineering Innovations & Technology Management (ICET: EITM-2017)*, 2017.

[51] A. Songara and L. Chouhan, "Blockchain: a decentralized technique for securing internet of things," in *Conference on Emerging Trends in Engineering Innovations & Technology Management (ICET: EITM-2017)*, 2017.

[52] H. Natarajan, S. Krause, and H. Gradstein, "Distributed ledger technology and blockchain," 2017.

[53] M. Alharby and A. van Moorsel, "Blockchain based smart contracts : A systematic mapping study," pp. 125–140, 08 2017. doi : 10.5121/csit.2017.71011.

[54] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. PP, pp. 1–1, 03 2021. doi : 10.1109/ACCESS.2021.3065880.

[55] R. Patgiri, I. Acharjamayum, and D. Devi, "Blockchain: A tale of peer to peer security," 01 2019. doi : 10.1109/SSCI.2018.8628826.

[56] X. W. . M. A. M. Matt Zand, *Hands-On Smart Contract Development with Hyperledger Fabric V2 /Building Enterprise Blockchain Applications.* O'REILLY.

[57] T. Ncube, N. Dlodlo, and A. Terzoli, "Private blockchain networks: A solution for data privacy," 12 2020. doi : 10.1109/IMITEC50163.2020.9334132.

[58] A. Ben Ayed and M. Belhajji, "The blockchain technology: Applications and threats," *International Journal of Hyperconnectivity and the Internet of Things*, vol. 1, pp. 1–11, 07 2017. doi : 10.4018/IJHIoT.2017070101.

[59] H. Monem and A. M. FUND, "Using blockchain in financial services," *Arab Monetary Fund*, vol. 54, p. 2019, 2019.

[60] "Algeria health sector market profile." `https://www.tradecommissioner.gc.ca/algeria-algerie/market-reports-etudes-de-marches/0006431.aspx?lang=eng`.

[61] M. Wehde, "Healthcare 4.0," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 24–28, 2019. IEEE.

[62] B. Mccluskey, "Wear it well," *Engineering & Technology*, vol. 12, no. 1, pp. 32–35, 2017. IET.

[63] M. C. Paganoni, *Big Data and Healthcare*. Springer, 2019.

[64] P. Esmaeilzadeh and T. Mirzaei, "The potential of blockchain technology for health information exchange: Experimental study from patients' perspectives," *J Med Internet Res*, vol. 21, p. e14184, Jun 2019.

[65] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, pp. 1–16, 2021.

[66] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?," *Future Internet*, vol. 10, no. 2, 2018. doi : 10.3390/fi10020020.

[67] R. Fekih and M. Lahami, "Application of blockchain technology in healthcare: A comprehensive study," pp. 268–276, 06 2020. doi : 10.1007/978-3-030-51517-1_23.

[68] L. Zhou, L. Wang, and Y. Sun, "MIStore: a Blockchain-Based medical insurance storage system," vol. 42, p. 149, July 2018.

[69] D. Ichikawa, M. Kashiyama, T. Ueno, *et al.*, "Tamper-resistant mobile health using blockchain technology," *JMIR mHealth and uHealth*, vol. 5, no. 7, p. e7938, 2017.

[70] U. Barchetti, A. Bucciero, A. Guido, L. Mainetti, and L. Patrono, *Supply Chain Management and Automatic Identification Management Convergence: Experiences in the Pharmaceutical Scenario*. 04 2011. doi : 10.5772/14726.

[71] L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, "Applications of blockchain within healthcare," *Blockchain in healthcare today*, 2018.

[72] Chronicled, "Live solutions." hhttps://www.mediledger.com/#Live-Solutions. Accessed: 2022-04-15.

[73] M. Niemerg, "Blockchain: The ultimate electronic health record." https://pharmaphorum.com/digital/blockchain-healthcare-electronic-medical-records/#:~:text=When%20put%20to,up%20to%20date. Accessed: 2022-04-15.

[74] M. R. Patra, R. K. Das, and R. P. Padhy, "Crhis: Cloud based rural healthcare information system," in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, pp. 402–405, 2012.

[75] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, pp. 1–8, 2016.

[76] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016. doi : 10.1109/OBD.2016.11.

[77] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA ... Annual Symposium proceedings. AMIA Symposium*, vol. 2017, 08 2017.

[78] I. C. of the Red Cross., "Health care in danger the responsibilities of health-care personnel working in armed conflicts and other emergencies." https://healthcareindanger.org/wp-content/uploads/2015/09/icrc-002-4104-the-responsibilities-health-care-personnel.pdf/. Accessed: 2022-04-15.

[79] L. J. Kish and E. J. Topol, "Unpatients—why patients should own their medical data," *Nature Biotechnology*, vol. 33, pp. 921–924, Sep 2015.

[80] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, pp. 1–10, NIST Gaithersburg, MD, USA, 2016.

[81] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," in *Blockchain enabled applications*, pp. 139–149, Springer, 2017.

[82] *Cybrosys Limited Edition BLOCKCHAIN E-BOOK*. www.blockchainexpert.uk.

[83] S. Aggarwal and N. Kumar, "Chapter sixteen - hyperledgerworking model.," in *The Blockchain Technology for Secure and Smart Applications across Industry Verticals* (S. Aggarwal, N. Kumar, and P. Raj, eds.), vol. 121 of *Advances in Computers*, pp. 323–343, Elsevier, 2021. doi : https://doi.org/10.1016/bs.adcom.2020.08.016.

[84] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, pp. 1–15, 2018.

[85] "Top hyperledger frameworks hyperledger tools for blockchain technology." `https://www.upgrad.com/blog/hyperledger-frameworks-hyperledger-tools-blockchain-technology/`. Accessed: 2022-04-12.

[86] "Hyperledger indy." `https://hyperledger-indy.readthedocs.io/en/latest/`. Accessed: 2022-04-12.

[87] "Hyperledger caliper." `https://www.hyperledger.org/use/caliper#:~:text=Hyperledger%20Caliper%20is%20a%20blockchain,set%20of%20predefined%20use%20cases./`. Accessed: 2022-04-12.

[88] "Hyperledger cello." `https://www.hyperledger.org/use/cello`. Accessed: 2022-04-12.

[89] V. Vijayakumar, K. Sabarivelan, J. Tamizhselvan, B. Ranjith, and B. Varunkumar, "Utilization of blockchain in medical healthcare record using hyperledger fabric," *Int J Res Advent Technol*, vol. 7, no. 4, pp. 414–419, 2019.

[90] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, IEEE, 2017.

[91] "Membership service providers (msp)." `https://hyperledger-fabric.readthedocs.io/en/release-2.2/msp.html#:~:text=Membership%20Service%20Provider,standards%20and%20architectures.` Accessed: 2022-04-25.

[92] J. Rask, F. Madsen, N. Battle, H. Macedo, and P. Larsen, "Visual studio code vdm support," 12 2020.

[93] B. B. Rad, H. J. Bhatti, and M. Ahmadi, "An introduction to docker and analysis of its performance," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 3, p. 228, 2017.

[94] J. C. Anderson, J. Lehnardt, and N. Slater, *CouchDB: the definitive guide: time to relax*. " O'Reilly Media, Inc.", 2010.

[95] N. Nurseitov, M. Paulson, R. Reynolds, and C. Izurieta, "Comparison of json and xml data interchange formats: a case study.," *Caine*, vol. 9, pp. 157–162, 2009.

[96] O. Ben-Kiki, C. Evans, and B. Ingerson, "Yaml ain't markup language (yaml™) version 1.1," *Working Draft 2008-05*, vol. 11, 2009.

[97] C. Ramey, "Bash, the bourne- again shell," in *Proceedings of The Romanian Open Systems Conference & Exhibition (ROSE 1994), The Romanian UNIX User's Group (GURU)*, pp. 3–5, 1994.

[98] M. Satheesh, B. J. D'mello, and J. Krol, *Web development with MongoDB and NodeJs*. Packt Publishing Ltd, 2015.

[99] S. Aggarwal, "Modern web-development using reactjs," *International Journal of Recent Research Aspects*, vol. 5, no. 1, pp. 133–137, 2018.

[100] R. Native, "React native," *línea]. Disponible en: https://reactnative. dev/.[Último acceso: 2 de noviembre 2019]*, 2020.

[101] "fabric-sdk-node." `https://hyperledger.github.io/fabric-sdk-node/`. Accessed: 2022-04-25.

[102] Y. Wu, P. Song, and F. Wang, "Hybrid consensus algorithm optimization: A mathematical method based on pos and pbft and its application in blockchain," *Mathematical Problems in Engineering*, vol. 2020, 2020.

[103] M. M. M. A. BOUDISSA Dahmane Lyes, "Designing and implementation of smart contracts system for internet of things application," 2019.

[104] office of information security, "Electronic health record systems," *leadership for it securty privacy across hhs*.

Abstract

Recently, a large amount of data can be generated by healthcare systems, can be transformed to valuable information. The medical record of patient is the fundamental parts of healthcare data, It takes many forms, such as Vital signs (Body Temperature, Pulse Rate, Respiration Rate, Blood Pressure), diagnoses, blood analysis and prescriptions...etc. Several limitations have been addressed in this work, First, in most existing systems, Privacy and trust are the main issues that concerns patients when dealing with their medical personal data. Therefore, The patient needs to have the entire and the exclusive control on his own data. Second, Governing healthcare data management by only one entity exposes the system to multiple vulnerabilities such as Single Point of Failure (SPOF). To fill such technical gaps, Our goal is to implement an efficient platform that supports privacy while maintaining a decentralized management of data. Our objective is achieved by designing a system based on Blockchain technology. The proposed system has been developed using Hyperledger Fabric framework as a private blockchain, which has been tested to demonstrate data privacy, and its performance is evaluated against competing blockchain approaches. The results we obtained showed the performance and the efficiency of our proposal in maintaining data privacy and terms storage capacity management.

Key words: Blockchain, P2P, Privacy, Decentralization,Distributed Ledger, Smart contract, Chain code, IOT, E-health...

Resume

Récemment, une grande quantité de données peut être générée par les systèmes de santé, peut être transformée en informations précieuses. Le dossier médical du patient est les parties fondamentales des données de santé, Il prend de nombreuses formes, telles que les signes vitaux (température corporelle, pouls, fréquence respiratoire, pression artérielle), diagnostics, analyses sanguines et ordonnances... Plusieurs limites ont été abordées dans ce travail. Premièrement, dans la plupart des systèmes existants, la protection de la vie privée et la confiance sont les principales questions qui préoccupent les patients lorsqu'ils traitent leurs données personnelles médicales. Par conséquent, Le patient doit avoir l'ensemble et le contrôle exclusif sur ses propres données. Deuxièmement, la gestion des données de santé par une seule entité expose le système à de multiples vulnérabilités telles que le point de défaillance unique (SPOF). Pour combler ces lacunes techniques, notre objectif est de mettre en œuvre une plateforme efficace qui appuie la protection de la vie privée tout en maintenant une gestion décentralisée des données. Notre objectif est atteint en concevant un système basé sur la technologie Blockchain. Le système proposé a été développé en utilisant le framework Hyperledger Fabric en tant que blockchain privée, qui a été testé pour démontrer la confidentialité des données, et sa performance est évaluée par rapport à des approches de blockchain concurrentes. Les résultats obtenus ont montré la performance et l'efficacité de notre proposition dans le maintien de la confidentialité des données et la gestion de la capacité de stockage.

Mots Clés: Blockchain, P2P, Confidentialité, Décentralisation, Ledger distribué, Contrat intelligent, IOT, ...