

Democratic and Popular Algerian Republic

Ministry of higher education and Scientific Research

Mohamed Khider University – Biskra

Faculty of Exact Sciences, Natural Sciences and Life

Department of Computer Science



THESIS

Presented for the diploma of

Master in Computer Science

Option: Information and communication networks and technologies

Conception and realization of a Blockchain model for health records

Presented in 28/06 /2022
By **OUSSAMA MEKHATRIA**

Order N°: RTIC01/M2/2022

Board of Examiners:

Mrs.SAOULI Rachida

Prof

President

Mr.ALOUI Ahmed

M.C.B

Supervisor

Ms.ZERARKA Nour Elhouda

M.A.B

Examiner

Promotion 2021/2022

Dedication

*First, I dedicate my dissertation work to the sake of **Allah**, my Creator and my Master. My great teacher and messenger, Mohammed (May **Allah** bless and grant him), who taught us the purpose of life.*

I dedicate my dissertation to all my family. A special feeling of gratitude to my loving parents, whose words of encouragement and push for tenacity ring in my ears. My sisters and my brother have never left my side and are very special.

I also dedicate this dissertation to all friends who have supported me throughout the process. I will always appreciate all they have done.

May ALLAH grant them Jannah Firdaus. Ameen

Knowledgegements

*Prima facie, I am grateful to **ALLAH** for the guidance, good health, wellness and willpower that were necessary to complete this thesis.*

*I would like to thank **my Parents**, who always believed in me. It is thanks to their support and prayers that I accomplished this work, they already know how much I owe them.*

*I also would like to thank my supervisor, Professor **Aloui Ahmed**, whose expertise was invaluable in formulating the research methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.*

I also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture. Finally, I also want to thank the jurors for agreeing to review and judge my work.

MEKHATRIA OUSSAMA

Abstract

Nowadays, it is difficult to have a clear view of all the data related to a patient and accumulated during the course of his or her care. This information usually comes from a wide variety of sources, such as city doctors, hospitals, insurance companies, pharmacists or medical analysis laboratories. Ideally, we would like to have a list of all the places where the medical data of the same patient can be found in order to be able to quickly retrieve it. This list would be accessible, to any health professional who requests it. Thus, instead of having access only to the database of the establishment where one is, one could have access to all the sources of information dispersed in all the databases of the network. Blockchain technology provides just such a solution in the form of a distributed and secure registry that allows patients to have visibility over their data.

Key words: Blockchain, health records, Trust, Electronic health Records,EHRs.

Résumé

De nos jours, il est difficile de visualiser de manière claire toutes les données liées à un patient et accumulées au cours de son parcours de soins. Ces informations proviennent habituellement de sources très variées, comme les médecins de ville, l'hôpital, les assurances, les pharmaciens ou les laboratoires d'analyses médicales. L'idéal serait donc d'avoir une liste qui répertorie tous les lieux où se trouvent les données médicales d'un même patient afin de pouvoir rapidement les récupérer. Cette liste serait accessible, à tout professionnel de santé qui en ferait la demande. Ainsi, plutôt que de n'avoir accès qu'à la base de données de l'établissement où l'on se trouve, on pourrait avoir accès à toutes les sources d'informations dispersées dans toutes les bases de données du réseau. La technologie Blockchain apporte justement cette solution sous la forme d'un registre distribué et sécurisé qui permet au patient d'avoir une visibilité sur ses données.

Mots clés: Blockchain, Confiance, Santé, Dossier Médical électronique.

ملخص

في الوقت الحاضر ، من الصعب تصور جميع البيانات المتعلقة بالمريض والمتراكمة خلال مسار رعايته. عادة ما تأتي هذه المعلومات من مجموعة واسعة من المصادر ، مثل أطباء أو المستشفيات أو شركات التأمين أو الصيدلة أو مختبرات التحليل الطبي. وبالتالي فإن الحل الأمثل هو أن يكون لديك قائمة تسرد جميع الأماكن التي توجد فيها البيانات الطبية لنفس المريض حتى تتمكن من استعادتها بسرعة ستكون هذه القائمة متاحة ، لأي أخصائي صحي يطلبها. وبالتالي، بدلا من الوصول فقط إلى قاعدة بيانات المؤسسة التي توجد فيها واحدة، يمكن للمرء أن يتمكن من الوصول إلى جميع مصادر المعلومات المنتشرة في جميع قواعد بيانات الشبكة. توفر تقنية سلسلة الكتل هذا الحل على وجه التحديد في شكل سجل صحي مشترك وآمن يسمح للمريض برؤية بياناته.

الكلمات المفتاحية : سلسلة الكتل، الصحة، الثقة، سجل طبي مشترك آمن

Summary

Dedication	I
Knowledgements	II
Abstract	III
Résumé	IV
Abstract in arabic	V
List of Figures	XI
List of Tables	XII
Acronyms	XIII
General introduction	1
1 Blockchain Technology	4
1.1 Introduction	4
1.2 Blockchain Definition	5
1.3 History of blockchain	5
1.4 Features of Blockchain	7
1.5 Structure of a blockchain	8
1.5.1 Transaction	8
1.5.2 Blocks	10
1.5.3 Consensus process	10
1.5.3.1 Proof of Work (PoW)	11
1.5.3.2 Proof of Stake (PoS)	11
1.5.3.3 Proof of Authority (PoA)	12
1.6 The Hash	13

1.7	Miners or nodes	13
1.8	Generic chain of blocks	13
1.9	Smart contracts	14
1.10	Cryptography in Blockchain	15
1.10.1	Type of cryptography in Blockchain	15
1.10.1.1	Symmetric cryptography	15
1.10.1.2	Asymmetric cryptography	16
1.10.1.3	Hash function	17
1.10.1.4	Digital signature	17
1.11	Types of blockchains	17
1.11.1	Public blockchains	17
1.11.2	Private blockchain	18
1.11.3	Consortium Blockchains	19
1.11.4	Hybrid Blockchains	19
1.12	Advantages and disadvantages of blockchain	20
1.12.1	Advantages of Blockchain	20
1.12.2	Disadvantages of Blockchain	20
1.13	Blockchain uses	21
1.14	Blockchain today	22
1.14.1	Cryptocurrencies	22
1.14.2	Bitcoin	23
1.14.3	Ethereum	23
1.14.4	Hyperledger Fabric	24
1.15	Conclusion	25
2	Blockchain Applications in Healthcare	26
2.1	Introduction	26
2.2	Blockchain Applications in Healthcare	26
2.2.1	Blockchains in Clinical Research	27
2.2.2	Blockchains in medical fraud detection	28
2.2.3	Blockchains in the pharmaceutical industry and research	28
2.2.4	Blockchain in Claim and Billing Management	29
2.2.5	Blockchain For Electronic Health Records	29
2.3	Management and sharing of health data	30
2.3.1	Health data sharing	30
2.3.2	Health data management	31
2.4	Communication of health data between the various actors of patient care	33
2.5	Comparison between the classic solution and the blockchain solution	33
2.6	Emerging blockchain-based healthcare solutions	34

2.7	Related work	35
2.8	Conclusion	36
3	Design a Blockchain approach for Health Record Secure Shared	37
3.1	Introduction	37
3.2	Global architecture	37
3.2.1	Steps of development	37
3.2.2	The EHR system's global architecture	40
3.3	Overall operation	41
3.3.1	Functional flowchart of EHR system	41
3.3.2	Use case diagram	43
3.3.3	Sequence diagrams	44
3.4	Architecture of each subsystem	48
3.4.1	Registration	48
3.4.2	Administrator	49
3.4.3	Blockchain network	49
3.4.4	Add a new health record	50
3.5	Conclusion	51
4	Implementation and Results	52
4.1	Introduction	52
4.2	System Configuration and Operating System	52
4.3	Tools and Programming Languages	52
4.3.1	Visual Studio Code	52
4.3.2	JavaScript	53
4.3.3	Bootstrap	53
4.3.4	JQuery	54
4.3.5	HTML and CSS	54
4.3.6	Google Firebase	54
4.3.6.1	Firebase products	55
4.4	Implementation and realization of the system	57
4.4.1	System Description	57
4.4.2	Mining algorithm	60
4.5	System Interface	61
4.5.1	Home page	61
4.5.2	Access as a Patient	62
4.5.3	Access as a health professional or doctor	64
4.5.4	Access as an administrator	69
4.6	Conclusion	71

General Conclusion	74
Bibliography	74

List of Figures

- 1.1 Blockchain structure [12] 8
- 1.2 Simplified transaction life cycle [13] 9
- 1.3 Components of Block 10
- 1.4 Proof of Work[16] 11
- 1.5 Proof of Stake[16] 12
- 1.6 Generic chain of blocks [21] 13
- 1.7 Smart contracts system [23] 14
- 1.8 Public Blockchain [28] 18
- 1.9 Private Blockchain [28] 18
- 1.10 Consortium Blockchain [28] 19
- 1.11 Overview of Bitcoin system [13] 23
- 1.12 Overview of Hyperledger Fabric system[13] 24

- 2.1 Applications of blockchains in healthcare [40] 27
- 2.2 A simplified example of blockchain-based patient record management [49] 32
- 2.3 Blockchain-enabled healthcare systems [49] 33
- 2.4 Emerging blockchain solutions for healthcare [51, 52] 35

- 3.1 Blockchain decision tree [55] 39
- 3.2 Global architecture of the EHR system 40
- 3.3 Functional flowchart of EHR system 42
- 3.4 Use case diagram of our application 43
- 3.5 "Patient" sequence diagram 44
- 3.6 "Consultation" sequence diagram 45
- 3.7 "Health professional" sequence diagram 46
- 3.8 "Administrator" sequence diagram 47
- 3.9 "Architecture module "Patient Registration " 48
- 3.10 "Architecture module "Health Professional registration" 48
- 3.11 "Architecture module "Administrator " 49

3.12	"Architecture module "Blockchain Network"	50
3.13	"Architecture module "Add a new health record"	51
4.1	Visual Studio Code logo	53
4.2	JavaScript logo	53
4.3	Bootstrap logo	53
4.4	jQuery logo	54
4.5	HTML and CSS logo	54
4.6	Google Firebase logo	55
4.7	Firebase console	55
4.8	Authentication	56
4.9	Realtime database	56
4.10	EHR System logo	57
4.11	The Genesis block	58
4.12	Block describing a prescription	59
4.13	check validity algorithm	60
4.14	Mining algorithm (proof of work)	61
4.15	Home page	61
4.16	List of My health records "Patient Profile"	62
4.17	Health record represents a "prescription"	63
4.18	List of my doctors	63
4.19	Edit profile (patient profile)	64
4.20	Register form	65
4.21	Dashboard doctor	66
4.22	List of my patients	66
4.23	Add a new record	67
4.24	List of patient documents	67
4.25	Blockchain	68
4.26	List of all patients	69
4.27	List of all doctors	69
4.28	Add a new admin	70
4.29	Chat page	70

List of Tables

2.1	Comparison table between classic solution versus blockchain solution . . .	34
-----	--	----

Acronyms

EHR	<i>Electronic Health Record</i>
PoW	<i>Proof of Work</i>
PoS	<i>Proof of Stake</i>
PoA	<i>Proof of Authority</i>
RPoW	<i>Reusable Proof Of Work</i>
DApps	<i>Decentralized Applications</i>
EVM	<i>Ethereum Virtual Machine</i>
P2P	<i>Peer-to-Peer</i>
ECDSA	<i>Elliptic Curve Digital Signature Algorithm</i>
HIPAA	<i>Health Insurance Portability and Accountability Act</i>
SMR	<i>Shared Medical Record</i>
BaaS	<i>Backend-as-a-Service</i>

General Introduction

The recent advent of technology affects every part of human life and changes how we use and perceive things in the past. Just as change technology has offered in a variety of other areas of life, so too has it found new ways to improve the health care sector. The main benefits of advances in technology are improvements in safety, user experience and other aspects of the healthcare industry.

In the world of technology, "blockchain" has become an omnipresent term. Many markets have exploded as a result of this technology during a period of distrust and dissatisfaction with third parties, traditional mediators, institutions, banks, and governments. Blockchain technology, which promises disintermediation and transparency, is both appealing and intriguing. The Blockchain promises to revolutionize the way we do transactions, just as the computer revolutionized the way we process data today and just as the Internet has revolutionized the way we share information on every level. The first instantiation of Blockchain technology is Cryptocurrency Bitcoin as an innovative payment network and a new form of money functioning without a central authority, it is free and open.

In a Blockchain model, there is no need to store information with third parties. Records are on many computers with information identical, so that the breaches do not make sense and if the data of a computer's Blockchain are breached, the system rejects such breach. Even if a hacker breaks into a network and tries to steal money from an account, multiple redundant and identical copies of the same ledger are stored in the whole world. In case of violation, there are many others in the form of backups that can provide the funds of the hacked account. In other words, Blockchain data is distributed around many nested computers. For hacking efforts to be successful, more than 50% of security systems network must be hacked.

Problematic and motivation

The health sector is a particularly promising area for Blockchain technology because it involves sharing patient information and health data, which is extremely sensitive. One of the biggest problems in healthcare today is that the organizations hold a multiple and fragmented health records about patient, it is the responsibility of healthcare professionals to ensure that sensitive medical records are accurate, complete and accessible only to authorized individuals. This can be challenging when healthcare providers all have different systems in place to store information. Just imagine if a patient's prescription information was left vulnerable to manipulation by hackers. Simply put, the more quality and secure that health information is, the better quality of care.

Aim of the work

In this work, we have attempted to adopt the Blockchain technology and cloud database to facilitate sharing private health data securely. As defined, our proposal : a system architecture contribution that adopts the Blockchain, where our system aims to manage health data using Electronic medical records. A Blockchain is made up of an ever-growing collection of records known as blocks, each of which represents a consultation and, as a result, a health record (document). Each block is cryptographically linked to the one before it, creating in a chain. The Blockchain is controlled by a peer-to-peer network of nodes. All network nodes that are attached to the same patient contain the same replica of the data belonging to such a patient. This eliminates the requirement for a centrally trusted authority.

Organization of the thesis

The thesis is organized as follows:

- **General Introduction** : We will begin our thesis with a general introduction on the context of this work, problematic and motivation, and aim of the work.
- **Chapter 1 Blockchain technology** : This chapter presents the general notions of Blockchain technology, including history, domain of application, structure and features of this technology.
- **Chapter 2 Blockchain applications in healthcare** : This chapter discusses the applications of blockchain in healthcare, ending with a comparative study between classic solution versus blockchain solution and related works.

- **Chapter 3 System design :** This chapter offers the design of the proposed system and therefore the steps of development.
- **Chapter 4 Implementation and results :** This chapter mentions the implementation tools, describes the code and discussions the result obtained.
- **General Conclusion :** We end our thesis with a general conclusion and gives insights into future work.

Blockchain Technology

1.1 Introduction

Blockchain has become a ubiquitous word that includes a social promise and new technology. Originally proposed as a solution to Bitcoin cryptocurrency record keeping system, blockchain are now used to store records of all kinds of applications. Blockchain means something more in many people's minds. The promise that many associate with blockchain applications is that they are going to collapse all centralized systems.

Centralized systems are everywhere and people need to trust counterparties, but don't have the resources to do it on their own. An easy way to identify where to apply blockchain technology is to look for areas that need an intermediary to encourage trust. Trust is essential for things such as the transfer of money, voting, land records, IP rights, and identity. Blockchain software can be programmed to take the place of the middleman by becoming the trusted record keeping system.[1]. In this chapter, we will be learning about all the major sides of Blockchain technology.

1.2 Blockchain Definition

The notion of Blockchain was appeared in 2008 when creating Bitcoin, as its best known case, by a stranger whose pseudonym is Satoshi Nakamoto. There are currently several definitions for Blockchain have been proposed, among these definitions, we cite the following:

- A blockchain is a distributed database that is shared between the nodes of a computer network. As a database, a blockchain stores information electronically in numerical form. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party[2].
- A blockchain is a peer-to-peer digital ledger of transactions that may be publicly or privately distributed to all users (and therefore is said to be decentralized and distributed). Blockchain technology uses cryptography and a consensus mechanism to verify transactions, which ensures the legitimacy of a transaction, prevents double spending, and allows for high-value transactions in a trustless environment. A blockchain offers transparency and eliminates the need for intermediaries or third-party administrators[3].
- Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not only financial transactions, but virtually anything of value[4].
- A blockchain is a chain of blocks that are connected together and keep growing as they store transactions on blocks. This platform uses a decentralized approach that enables the dissemination of information and that every piece of information distributed or commonly called data has a shared property[5].

1.3 History of blockchain

Blockchain technology has to be one of the biggest innovations of the 21st century given the ripple effect it is having on various sectors, from financial to manufacturing as well as education. Unknown to many, is that the history of Blockchain dates back to the early 1990s.

in 1991 :

The blockchain technology was described in 1991 by the research scientist Stuart Haber and W. Scott Stornetta. They wanted to introduce a computationally practical solution

for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of cryptographically secured chain of blocks to store the time-stamped documents[6].

In 1992, Merkle Trees were incorporated into the design, which makes blockchain more efficient by allowing several documents to be collected into one block. Merkle Trees are used to create a 'secured chain of blocks.' It stored a series of data records, and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain[6].

in 2004 :

computer scientist and cryptographic activist Hal Finney (Harold Thomas Finney II) introduced a system called RPoW, Reusable Proof Of Work. The system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token and in return created an RSA-signed token that could then be transferred from person to person[7].

RPoW solved the double spending problem by keeping the ownership of tokens registered on a trusted server that was designed to allow users throughout the world to verify its correctness and integrity in real time. RPoW can be considered as an early prototype and a significant early step in the history of cryptocurrencies[7].

in 2008 :

Satoshi Nakamoto conceptualized the theory of distributed blockchains. He improves the design uniquely to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure history of data exchanges. It utilizes a peer-to-peer network for timestamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes blockchains as the backbone of cryptocurrencies[6].

in 2013 :

Vitalik Buterin, a programmer and a co-founder of the Bitcoin Magazine, stated that Bitcoin needed a scripting language for building decentralized applications. Failing to gain agreement in the community, Vitalik started the development of a new blockchain-based distributed computing platform, Ethereum, that featured a scripting functionality, called smart contracts[7].

Smart contracts are programs or scripts that are deployed and executed on the Ethereum blockchain, they can be used for example to make a transaction if certain conditions are met. Smart contracts are written in specific programming languages and compiled into bytecode, which a decentralized Turing-complete virtual machine, called the Ethereum virtual machine (EVM) can then read and execute[7].

Developers are also able to create and publish applications that run inside Ethereum blockchain. These applications are usually referred to as DApps (decentralized applications) and there are already hundreds of DApps running in the Ethereum blockchain,

including social media platforms, gambling applications, and financial exchanges. The cryptocurrency of Ethereum is called Ether, it can be transferred between accounts and is used to pay the fees for the computational power used when executing smart contracts[7].

1.4 Features of Blockchain

Several characteristics are associated with the blockchain : peer-to-peer network, decentralized, transparency, distributed consensus, inefaceable, distributed structure, resilience, autonomy, security and trust [8]. All these characteristics constitute the innovative potential and modern possibilities of the blockchain. We mention the most important characteristics of the Blockchain are :

1. **Peer-to-Peer Network** : The peer-to-peer is a group of independent computers called nodes which are interconnected with each other to share data without use of the centralized computer [9]. In a blockchain network, transactions take place directly between two nodes in the network, meaning no third party is required. It is verified by all other nodes in the blockchain. This is known as the Peer-to-Peer network.
2. **Decentralization** : Blockchain system is decentralized and distributed. There is no central entity that controls and manages the blockchain, but network node can be access and check all the transactions because each node has a copy of the public ledger. This is advantage makes blockchain more secured.

With blockchain, the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data that was before concentrated at one central point is now handled by many trusted entities[5].

3. **Security and privacy**: Blockchain technology utilizes cryptographic features to ensure the security of nodes connected to its network.It uses the SHA-256 cryptographic algorithm for hashes that are stored in blocks. SHA means secure hash algorithm, these hashes provide the security of the blockchain that data integrity is assured by them. Cryptographic hashes are strong one way functions that generate checksum for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by the cryptographic approaches, which makes it to be a good option for privacy protection of certain applications[5].

4. **Autonomy** : The computing strength and hosting space is supplied by network nodes, i.e. users themselves. So there is no need for central infrastructure. Within the blockchain, the infrastructure is no longer concentrated in the hands of an enterprise, on the contrary, it is dispersed at all points of the network [8].
5. **Transparency** : The blockchain is called transparent because anyone can download it in its entirety and check its honesty at any time [10]. All blockchain users can thus view actual and past transactions[8]. If transparency is ensured for transactions, user anonymization calls into question this characteristic. In fact, the possible anonymity on the blockchain can be used for deceitful activities, hard or even impossible to disclose and regulate.
6. **Immutability** : Immutable refers to something that can't be changed or deleted. Creating immutable ledgers is one of the significant features of blockchain technology. In the blockchain, if the transaction log created by the consensus amongst the participants is checked, then it cannot be replaced or changed[11].

1.5 Structure of a blockchain

The structure of the Blockchain technology is represented by a list of blocks with transaction in a specific order. Transaction data is stored in blocks, which are linked together to create a chain. The more transactions there are, the greater the size of the blockchain. Architectural components were generalized and then modified by various companies, leading to different Blockchain projects such as Bitcoin, Ethereum, Hyperledger, ..., etc. there are the major components of Blockchain architecture. illustrated in Figure 1.1.

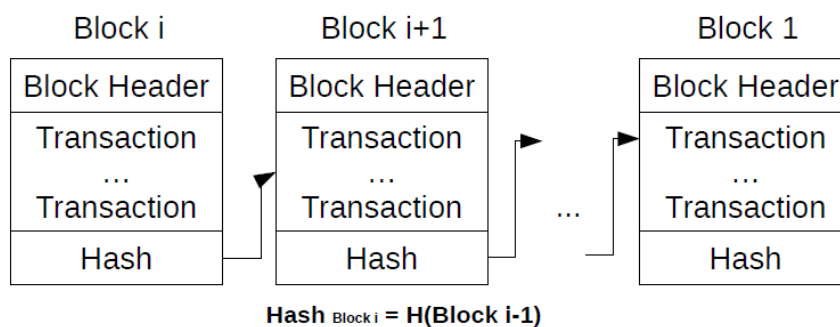


Figure 1.1: Blockchain structure [12]

1.5.1 Transaction

A transaction is a series of exchanges of information and related activities Such as updating the database, which is treated as a unit for the purpose of satisfying an application

and ensuring the integrity of the database. In the blockchain, a transaction is a transfer value which is transmitted over the network and collected in blocks. Transactions contain one-or-more inputs and one-or-more outputs.

- An input is a reference to an output from a previous transaction.
- An output specifies an amount and an address.

A transaction usually references past transaction outputs as new transaction inputs and devotes all input values to new outputs. Transactions are not encrypted, so it is possible to scan and view every transaction ever collected into a block. With just enough confirmations of transactions, they can be considered irreversible.

A simplified life cycle of transactions is shown in Fig. 1.2. Once created, the transaction is signed with the signature of the transaction's initiator, which provides the authorization to spend the money, create a contract, or pass the data parameters associated with the transactions. A signed transaction should contain all the information needed to be executed[13].

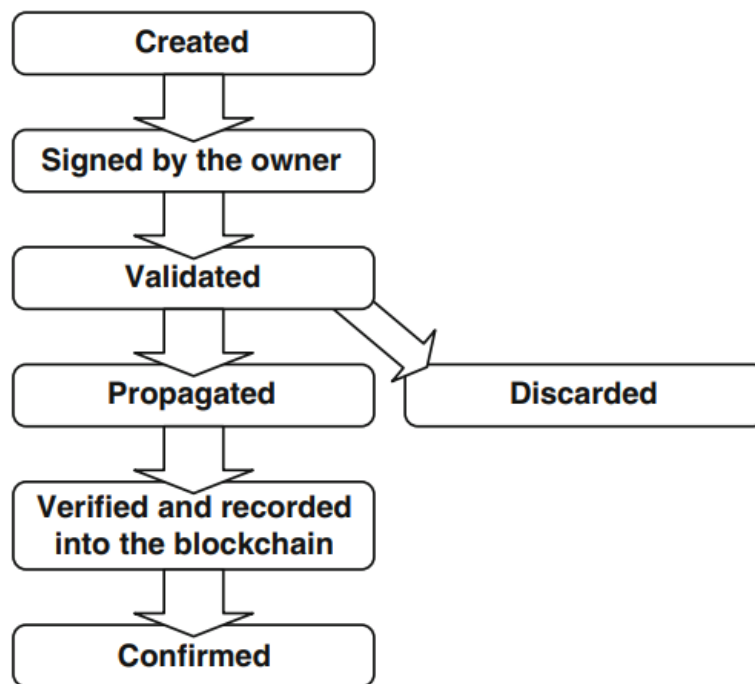


Figure 1.2: Simplified transaction life cycle [13]

1.5.2 Blocks

Blockchain are formed together by a number of blocks interconnected together in a peer-to-peer network, making it a decentralized application. The heading of these blocks contains hatching of previous blocks. A block contains three things in it which are data, hash of current block and hash of previous block. The data could be anything, as it depends on the type of blockchain. As in the case of bitcoin, the data consists of coins that are actually electronic cash. The hash that is stored in these blocks contains a SHA-256 cryptographic algorithm, which is used for unique identification of a block on the chain[5]. Figure 1.3 shown components of Block.

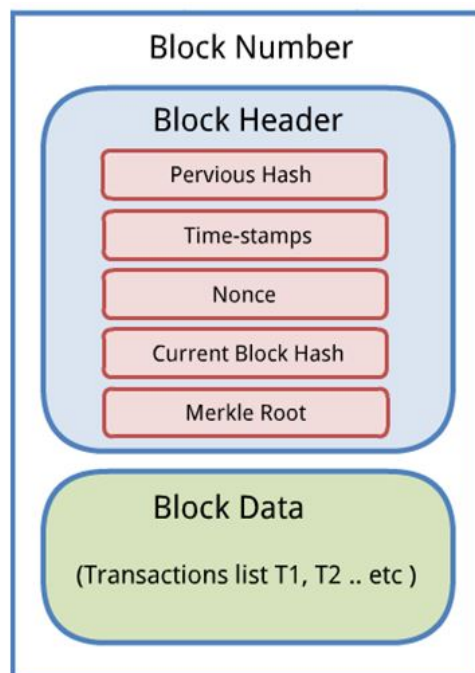


Figure 1.3: Components of Block

1.5.3 Consensus process

A consensus algorithm [14] is a mechanism which enables users or machines to coordinate within a distributed setting. He must make sure that all agents in the system can agree on only one source of truth, even if some agents fail. In other words, the system must be fault-tolerant.

In a centralized setup, a single entity has power over the system. In most cases, they can make changes as they please – there isn't some complex governance system for reaching consensus amongst many administrators. But in a decentralized setup, it's a whole other story. Say we're working with a distributed database – how do we reach an agreement on what entries get added?

Overcoming this challenge in an environment where strangers don't trust each other

was perhaps the most crucial development paving the way for blockchains. We will describe some consensus mechanisms below[15].

1.5.3.1 Proof of Work (PoW)

Proof of work has been the first consensus algorithm to be created and used by Bitcoin and other cryptocurrencies, it is a vital algorithm in the mining process. Where proof of work is dependent on blockchain members to reach consensus[16]. PoW selects an issue that cannot be solved without guessing. For example, when it is time to create and validate a full block, the problem is to guess a nonce value such that when using the transaction data and the nonce value as inputs for a hash function, its hash output needs to match the difficulty, e.g., beginning with four leading zeros. Every node (also called mining node) on the network is now guessing different nonce values randomly until one node first happens to find the nonce value that matches the difficulty. So a mining node has to spend a lot of computational resources on it (hence called as “work”) and solves the problem faster than others in order to succeed in creating a block to link to the Blockchain, and obtain an incentive mining reward, which is often cryptocurrency. On the other hand, hash functions are important as one cryptographic puzzle at the center of the PoW consensus algorithm. Bitcoin network adopts the cryptographic hash function SHA-256[17]. Figure 1.4 shown process of proof of work.



Figure 1.4: Proof of Work[16]

1.5.3.2 Proof of Stake (PoS)

The PoS consensus algorithm was developed in 2011 as a PoW alternative. While PoS and PoW share similar objectives, they provide some basic differences and features. Especially during checking new blocks. It is currently being developed in Ethereum Blockchain. Proof of Stake consensus algorithm replaces PoW mining with a mechanism by which the blocks are verified according to the share of the participants.

The validator for each block is determined by development of the cryptocurrency itself and not by the amount of computational power specified. Each PoS system may execute

the algorithm in several ways, but in general, an individual can either be mining or agree to a transaction based on the number of currencies he holds by voting[16].

This means that the more Bitcoin or altcoin used by the wallet, the more voting power the user will have. Figure 1.5 shows the process of proof of stake.

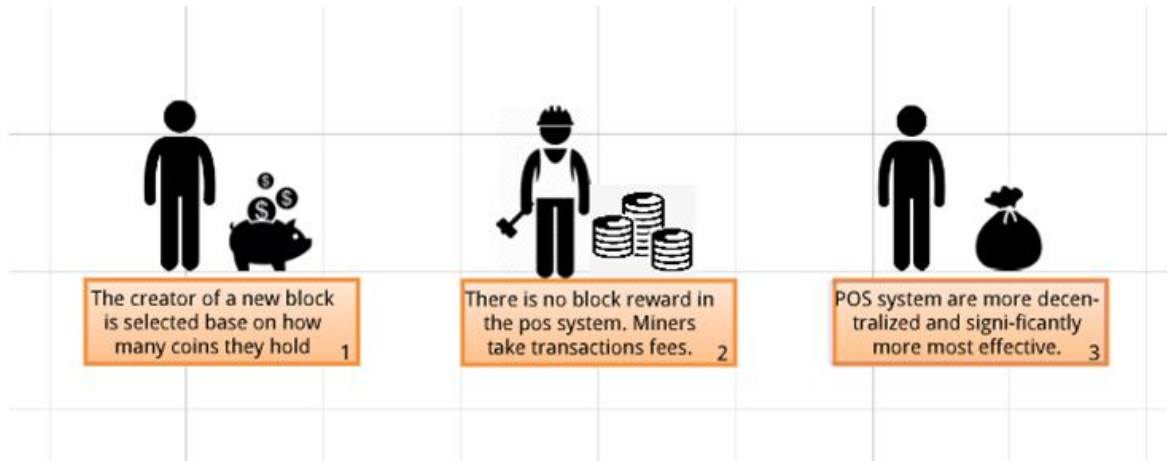


Figure 1.5: Proof of Stake[16]

1.5.3.3 Proof of Authority (PoA)

Proof of Authority [18] (PoA) is a Byzantine Fault Tolerant (BFT) consensus algorithm for permission and private blockchains. The algorithm relies on a set of trusted entities known as validators (i.e., authorities). The validators are responsible for collecting the transactions from the clients, creating and adding the blocks onto the chain. The algorithm runs in rounds, where in each round a validator is allowed to propose a block. A validator proposes a block in its respective round. The other validators verify the proposed block and add the block to their local copy of the blockchain if it is found to be valid. Once a block is added, a global consensus is reached. However, if a validator proposes an invalid block or proposes more than one block in a round, the other validators in the network call for voting. And if a majority of votes are against the validator, then the validator is considered to be malicious and is removed from the system; thus, it is no longer authorized for proposing any more blocks. PoA is an ideal consensus algorithm for private and permission blockchains, where the participants are authenticated and are limited in numbers. It is often considered as a compromise between truly decentralized and efficient centralized systems. Unlike, PoW algorithm, PoA is not resource-intensive. It is lightweight and has higher throughput; hence, an ideal consensus mechanism for localized IoT blockchain implementation such as smart homes where power consumption is critical and devices have bounds on their computational and storage capacity.

1.6 The Hash

When it comes to blockchain technology, the term "hashing" or "hash" is commonly used. Hashing is the process of transforming and generating any length of input data into a fixed-length string using a specific algorithm. The Bitcoin hash algorithm is SHA-256, which stands for Secure Hashing Algorithm 256 bits. Because the original data cannot be decrypted, this algorithm is a one-way cryptographic function[19].

1.7 Miners or nodes

A miner or a node is a CPU that attempts to solve a difficult mathematical problem in order to find a new block. It has the ability to add new blocks to the chain by creating and submitting them. Which miner is allowed to produce a specific block may be predetermined, or miners may simultaneously compete to add the next block to the chain, e.g. In the case of the Bitcoin network, miners perform similar work to a bank cashier, verifying that a particular transfer of bitcoins is between two valid accounts, validating that the sender's signatures are original and that the sender has ownership of the currency being transmitted.[16].

1.8 Generic chain of blocks

The blocks are chained together through each block containing the hash digest header of the preceding block, thus forming the blockchain. If a previously released block was changed, there would be a different hash. This in turn would cause all the following blocks to also have different hashes, as they include hashing from the previous block. This makes it possible to easily detect and reject altered blocks. Figure 1.6 shows a generic chain of blocks[20].

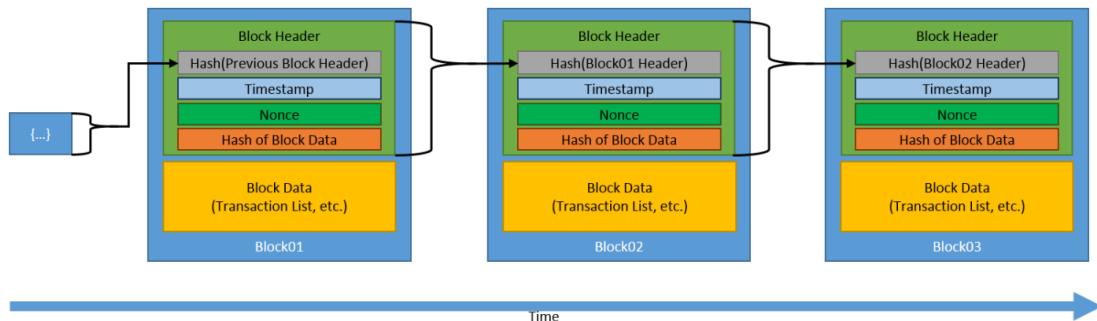


Figure 1.6: Generic chain of blocks [21]

1.9 Smart contracts

“A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises”[22].

A smart contract is an executable code that run on the blockchain to facilitate, execute and implement the terms of an agreement. The main purpose of a smart contract is to automatically execute the terms of an agreement when the specified conditions are satisfied. Thus, smart contracts promise low transaction fees compared to traditional systems that require a trusted third party to enforce and execute the terms of an agreement. The idea of smart contracts came from Szabo in 1994. However, the idea did not see the light till the emergence of blockchain technology. A smart contract can be thought of as a system that releases digital assets to all or some of the involved parties once arbitrary, pre-defined rules have been met[23]. The smart contract system is illustrated in figure 1.7.

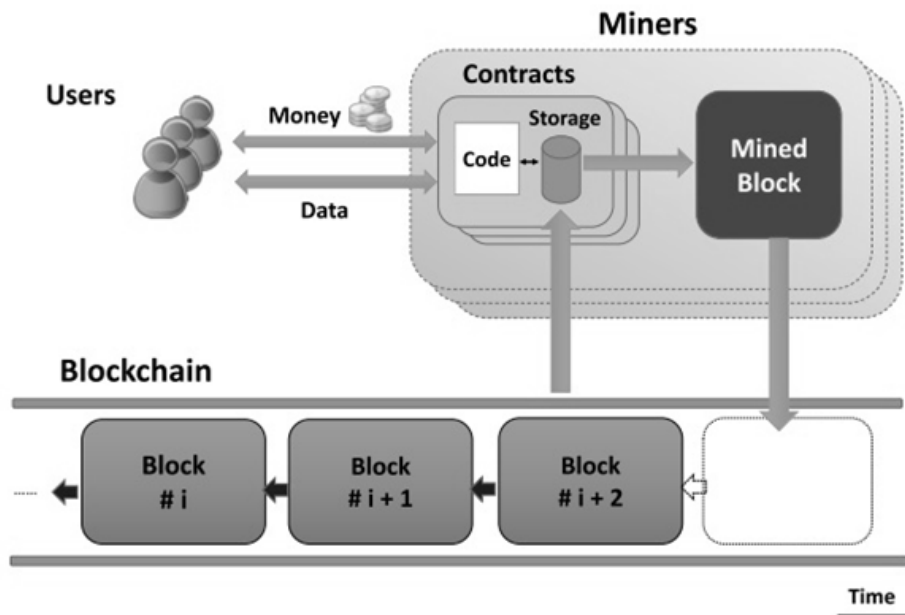


Figure 1.7: Smart contracts system [23]

A smart contract consists of an account balance, private storage and executable code. The contract’s state comprises the storage and the balance of the contract. The status is stored in the blockchain, and it is updated with every contract call. Figure 1.5 depicts the smart contract system. Each contract will be assigned to a unique address of 20 bytes. Once the contract is deployed into the blockchain, the contract code cannot be changed. To run a contract, users can simply send a transaction to the contract’s address. This transaction will then be executed by every consensus node (called miners) in the network to reach a consensus on its output. The contract’s state will then be updated accordingly. The contract can, based on the transaction it receives, read/write to

its private storage, store money into its account balance, send/receive messages or money from users/other contracts or even create new contracts.

There are two types of smart contracts, namely [24]:

- deterministic smart contract.
- non-deterministic smart contracts.

A deterministic smart contract is a contract that, when executed, does not need any information from an external party (from outside the blockchain).

A non-deterministic smart contract is a contract that depends on information (called oracles or data feeds) from an external party. For example, a contract that requires the performance of current weather information, which is unavailable on the blockchain.

1.10 Cryptography in Blockchain

Cryptography is a method of concealing and revealing information, often known as encrypting and decrypting data or message content. It builds and uses rules that prevent external parties or the audience from reading encrypted messages for information security. In cryptography, data or a piece of information is converted into a useless or nonsensical piece of text based upon mathematical rules. This is usually done using what is called a key, commonly referred to as a private key. To decrypt or bring the message back to its original form, either the private key or a public key issued by the private key owner is required. This ensures the security of information [15].

Cryptography is used in blockchain for the following two purposes [15]:

- Securing the identity of the transaction sender.
- Ensuring that past records cannot be tampered with.

1.10.1 Type of cryptography in Blockchain

To comprehend blockchain cryptography, one must first comprehend the various types of cryptography. There are primarily three methods for performing cryptographic algorithms: symmetric-key cryptography, asymmetric key cryptography, hash functions, and digital signatures.

1.10.1.1 Symmetric cryptography

The first key cryptography approach to be used in a blockchain network was symmetric cryptography. Both nodes encode and decode using the same key in this approach (or encrypt and decrypt) [25].

Suppose Node A wants to send some confidential information to Node B. To facilitate this transition using the symmetric key method. Node A encrypts information into an illegible encrypted text using a k1 key and sends it to Node B. Node B will receive the ciphertext and decrypt it using the same key, i.e. k1. This means that Node A and Node B must share the same k1 key. Similarly, if Node A wants to communicate with Node C, they will both need a new k2 key between themselves. Or Node B and Node C will require an additional k3 key to complete a transaction[25].

Thus, a major disadvantage of the method, despite being the quickest method, is that a node will need to have many keys to interact with various nodes in the network. In addition, nodes should ensure that they share the key securely, otherwise a third node may know the key. Due to these drawbacks, there came another method of asymmetric key cryptography[25].

1.10.1.2 Asymmetric cryptography

As its name suggests, asymmetric cryptography does not imply the sharing of the same key among two nodes. Rather, in this type of key encryption, there are two keys to a node: a private key and a public key. These keys always exist in a pair, as they work in tandem. That is, we use the public key to encrypt the message and the corresponding private key to decrypt the message[25].

Suppose we have a network of three nodes; A, B, and C. Each node will have its separate pair of private and public keys. The public key is made public, i.e. all other nodes in the network are aware of this key. Whereas, a private key must not be shown to others and kept private by the node like a password.

Now let's take an example of how a transaction is carried out using the key pair between two nodes. Let's say Node A has to send confidential information like bank account details to Node B. Now, Node A will first encrypt the text using its own i.e. A's private key and then again encrypt it using B's public key. When this encrypted text reaches Node B, it will first decrypt it using its own, i.e. B's private key and then again using A's public key.

What we have to understand here is that the first layer of encryption, in which node A uses its own private key to encrypt the message. It is for Node B to verify that the message is actually coming from Node A.

The next layer of encryption ensures the safety of the message in a way that only Node B's public key can code it and only Node B's private key can decode it. By this, the information is protected from any malicious third party attack. This is the way the two-key system works in asymmetrical key cryptography. It is commonly called public key cryptography.[25].

1.10.1.3 Hash function

It is designed to generate a “hash value” (or just “hash”) from a piece of data. Hash is a bit sequence, frequently presented in character string form. Its length is usually set to a specific function. The original data can generally be of any size, they will be matched with a hash of specified length. Changing even one bit in the original data will result in an entirely different hash value for it. This property is used, for example, to check the integrity of any transmitted data. The sender includes the message’s hash value in the message, and the receiver can compute the hash value of the received message and compare it to the one provided by the sender. Any inconsistencies will mean corruption of the message during transfer[26].

1.10.1.4 Digital signature

Digital signatures are key to the security and integrity of data stored on the blockchain. Digital signatures ensure security through encryption and integrity by ensuring that if the data is changed, the signature changes too. This provides immutability in the blockchain. They also ensure authenticity as they can only be bound to one user. Digital signatures are unique to a signer and based on three algorithms [15]:

- Private and public key owned by the user.
- A signing algorithm that combines the private key and data being signed.
- Algorithm that checks and determines whether the message is authentic or not based on the message or data, public key and signature.

1.11 Types of blockchains

There are mainly two kinds of blockchain: private and public blockchain. However, there are also a number of variations, such as the Consortium and hybrid blockchain. Before going into the details of the various types of blockchain, let’s first learn what similarities they share. Every blockchain consists of a cluster of nodes functioning on a peer-to-peer (P2P) network system. Every node in a network has a copy of the shared ledger, which gets updated timely. Each node can verify transactions, initiate or receive transactions and create blocks[27].

Let’s take a look at the four types of blockchain that are available.[27].

1.11.1 Public blockchains

A public blockchain [27] is a non-restrictive, permission-less distributed ledger system. Anyone with access to the Internet may connect to a blockchain platform to become an

authorized node and be part of the blockchain network. A node or user that belongs to the public blockchain is allowed to access current and past records. Check transactions or proof-of-work for an incoming block, and mine. The most basic use of public blockchains is for mining and exchanging cryptocurrencies. Thus, the most common public blockchains are Bitcoin and Litecoin blockchains. Public blockchains are mostly secure if the users strictly follow security rules and methods. However, it is only risky when the participants don't follow the security protocols sincerely. Figure 1.8 shows public Blockchain.

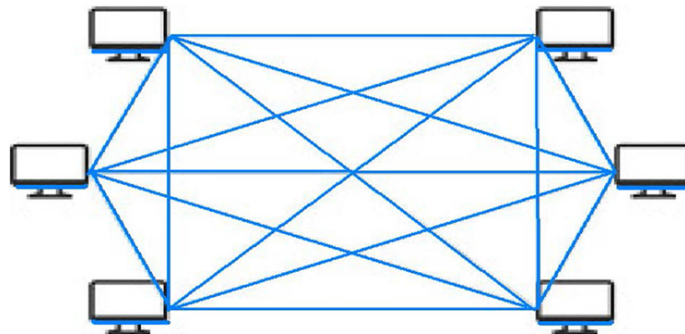


Figure 1.8: Public Blockchain [28]

1.11.2 Private blockchain

A private blockchain [27] is a restrictive or permission blockchain operative only in a closed network. Private blockchains are generally used within an organization or companies, where only selected members are participants in a blockchain network. The level of security, permissions, access is in the hands of the control organization. Thus, private blockchains are similar in use as a public blockchain but have a small and restrictive network. Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc. Figure 1.9 shows private Blockchain.

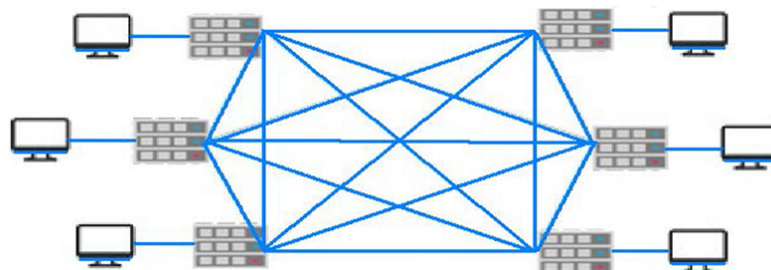


Figure 1.9: Private Blockchain [28]

1.11.3 Consortium Blockchains

A consortium blockchain [27] is a semi-decentralized type where more than one organization manages a blockchain network. This is contrary to what we saw in a private blockchain, which is managed by only a single organization. More than one organization can act as a node in that kind of blockchain and share information or engage in mining. Consortium blockchains are typically used by banks, government organizations, etc. Examples of consortium blockchain are Energy Web Foundation, R3. Figure 1.10 shows Consortium Blockchain.

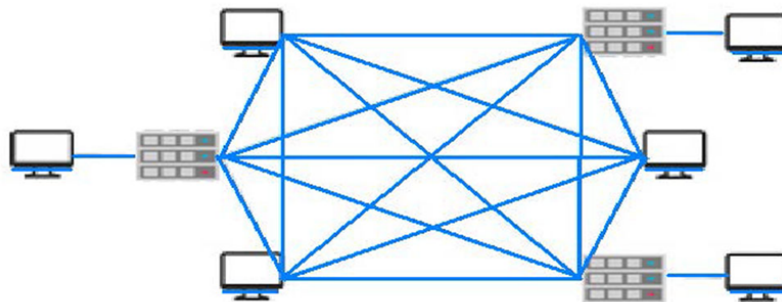


Figure 1.10: Consortium Blockchain [28]

1.11.4 Hybrid Blockchains

A hybrid blockchain [27] is a combination of the private and public blockchain. It uses the characteristics of both types of blockchain, that is, you can have a private permission-based system and a public system without permission. With such a hybrid network, users can control who gets access to which data stored in the blockchain. Only a selected section of data or records from the blockchain can be allowed to go public, keeping the rest as confidential in the private network. The hybrid blockchain system is flexible so that users can easily join a private blockchain with several state-owned blockchains. A transaction in a private network or a hybrid blockchain is usually verified within that network. But users can also release it in the public blockchain to get verified. Public blockchain increases hashing and requires more nodes for verification. This enhances the security and transparency of the blockchain network. An example of hybrid blockchain is Dragonchain.

1.12 Advantages and disadvantages of blockchain

1.12.1 Advantages of Blockchain

The main benefits that the Blockchain provides are :

- **Decentralized structure** : Enables real-time data sharing between suppliers and distributors, while reducing weakness.
- **Trust** : Allows trust between participants who don't know each other.
- **Visibility and traceability** : Tracks the origins of a variety of items, such as medicines, to confirm they're legitimate instead of counterfeit and organic items to confirm they're indeed organic.
- **Security** : Blockchain technology is highly secure due to the reason for each individual entering the Blockchain network is uniquely identified and linked to their account. This ensures that the owner of the account himself is operating the transactions. The block encryption in the chain makes it tougher for any hacker to disturb the traditional setup of the chain[29].
- **Faster processing** : Before the invention of blockchain, the traditional banking organization takes a long time to process and initiate the transaction. but after the blockchain technology, the transaction speed went up to a very high degree. Before this, the overall banking process takes around three days to settle but after the introduction of Blockchain, the time reduced to nearly minutes or even seconds[29].
- **Immutability** : Ensures transactions cannot be edited and deleted.

1.12.2 Disadvantages of Blockchain

The disadvantages of using a blockchain are :

- **High energy consumption** : Power consumption is necessary to maintain a real-time ledger. Every time a new node is created, it connects with the other nodes at the same time. As a result, transparency is created. The network's miners are attempting to solve a lot of solutions per seconds in efforts to validate transactions. They are using substantial amounts of computer power. Every node is giving extreme levels of fault tolerance, ensures zero downtime, and is making data stored on the Blockchain forever unchangeable and censorship-resistant. But these actions burning electricity and time it is wasteful, when each node repeats the achievement of Consensus[30].

- **The signature verification** : Each blockchain transaction needs to be digitally signed using a public-private cryptography scheme such as the Elliptic Curve Digital Signature Algorithm (ECDSA). This is necessary because transactions spread between nodes in a peer-to-peer way, so that their source cannot otherwise be proven. The generation and verification of these signatures is computationally complex, and constitutes the primary bottleneck in products like ours. By contrast, in centralized databases, once a connection has been established, there is no need to individually verify every request that comes over it[31].
- **Cost** : High costs are a major drawback to blockchain. The average cost of the transaction is between 75 and 160 dollars, and most of it is covered by energy consumption. One reason for this situation was described earlier. The second reason is the high initial investment costs for the Blockchain.[31].

1.13 Blockchain uses

Many fields are now interested in developing technical solutions based on Blockchain technology. Because of the enthusiasm and promises of blockchain in terms of speed and security of transactions, it has been embraced in many areas of application. We'll go over the most well-known ones next.

- **Government** : The application of blockchain technology in government systems will reduce bureaucratic, obstacles, red tape, and increases efficiency and transparency in government Operations. The Dubai government has already begun implementation of the technology.[32].
- **Healthcare** : Providers can leverage blockchain to securely store their patients' medical records. Once a medical record is generated and signed, it can be logged in the blockchain, providing patients with proof and assurance that the record cannot be edited. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy[2].
- **Insurance** : The global insurance market relies upon trust management. Blockchain is a new way to handle trust. Blockchain ensures confidence through mutual distrust among participants. 'A eternity' is an example of blockchain based insurance management system[32].
- **Vote** : Blockchain could be used to facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout,

as was tested in the November 2018 midterm elections in West Virginia[33]. Using blockchain in this way would make votes nearly impossible to tamper with. Blockchain protocol would also maintain transparency in the electoral process, reducing the staff required to conduct an election and providing officials with near-instantaneous results. This would remove the need for a recount or any real fear that fraud could threaten elections[2].

- **Banking and Finance** : Perhaps no industry will benefit from blockchain integration in its operations beyond banking. Financial institutions operate only during hours of operation, typically five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes—basically the time required to add a block to the blockchain, regardless of holidays or time of day or week. With blockchain, banks can also exchange funds between institutions faster and safely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if trading internationally), meaning that the money and shares are frozen for that period of time. Given the amount of money involved, even the few days the money is in transit can incur significant costs and risks for the bank.[2].

- **Supply chain management** : Suppliers can use blockchain to track the sources of the materials they buy. This would enable companies to check the validity of not only their own products, but also labels like "Organic," "Local," and "Fair Trade." [2].

1.14 Blockchain today

Blockchain technology is garnering a lot of public attention these days, and it's already being used in a lot of different applications, not just cryptocurrencies.

1.14.1 Cryptocurrencies

Cryptocurrency represents a digital asset, whose main goal is to be a medium in exchange, and at the same time doing that. It uses cryptography so that all transactions are secure, every new one that pops up is controlled by its own system. It can be said that cryptocurrency is a sub-set of digital currencies. The first cryptocurrency ever made was

the Bitcoin, in 2009. After that, a lot of other cryptocurrencies appeared on the market, but they were called the altcoins, as they represented the mix of Bitcoin alternatives[34].

1.14.2 Bitcoin

”Bitcoin is an innovative payment network and a new kind of money”[35]. Bitcoin is a virtual currency or a type of cryptocurrency that dates back to the beginning of 2008. Its creation, transactions, and security are all based on cryptography. Satoshi Nakamoto is the pseudonym of a nameless programmer who is the founder of Bitcoin[35]. Bitcoin has been produced to remove financial accountability and trust from governments, central banks and other third parties. Eliminate risks related to inflationary whims and other economic tools used by central banks and governments.[35]. Figure 1.11 gives an overview of Bitcoin system

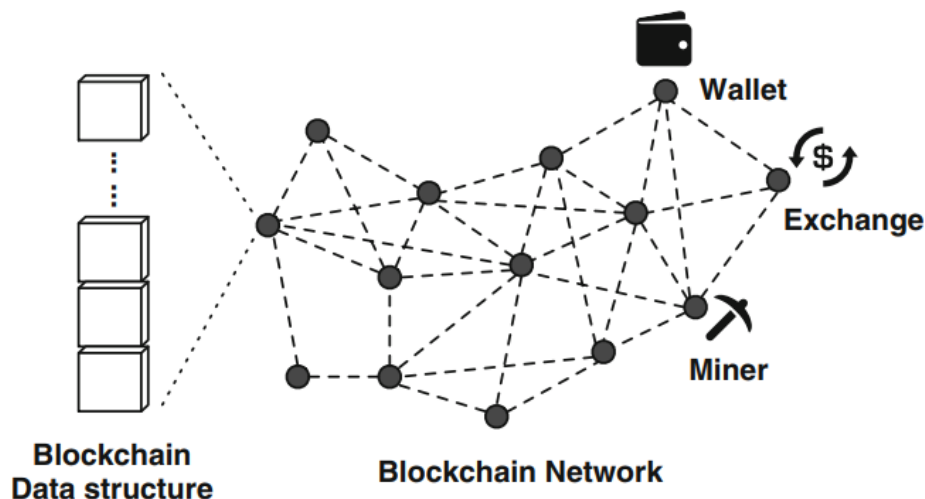


Figure 1.11: Overview of Bitcoin system [13]

1.14.3 Ethereum

Ethereum is an open source Blockchain platform that enables anybody to create and deploy Blockchain applications. Any type of app, including cryptocurrencies, tokens, wallets, and social media apps, can be developed and deployed in a Distributed Environment of Ethereum. In other words, rather than sticking with the cryptocurrency alone, Ethereum opened the possibilities of the ‘blockchain’ and ‘distributed ledger’ technology to other application domains. Ethereum is not a single network, rather it is more like a protocol for internode communication[32].

1.14.4 Hyperledger Fabric

The Hyperledger Project[36] is a collaborative effort to build a distributed ledger framework and open source enterprise-level code base. It aims to advance blockchain technology by identifying and building a standard, cross-sectoral open platform for distributed books that can transform how commercial transactions are conducted on a global scale. Established as a project of the Linux Foundation in early 2016, the Hyperledger Project currently has more than 50 members[37].

Hyperledger Fabric (or simply, Fabric) is a permissioned blockchain deployment and management system aimed towards corporate applications.[38]. It's designed with flexibility and generality in mind, allowing it to support a wide range of non-deterministic smart contracts (also known as chaincodes) and pluggable services. The support for pluggable components gives Fabric an unprecedented level of extensibility and, in particular, enables it to use multiple ordering services for managing the blockchain[12].

In another definition, Hyperledger Fabric is a set-up of a distributed ledger platform. For the execution of smart contracts, taking advantage of familiar and proven technologies, with a modular architecture allowing connectable implementations of different functions.[37]. Figure 1.12 gives an overview of Hyperledger Fabric system

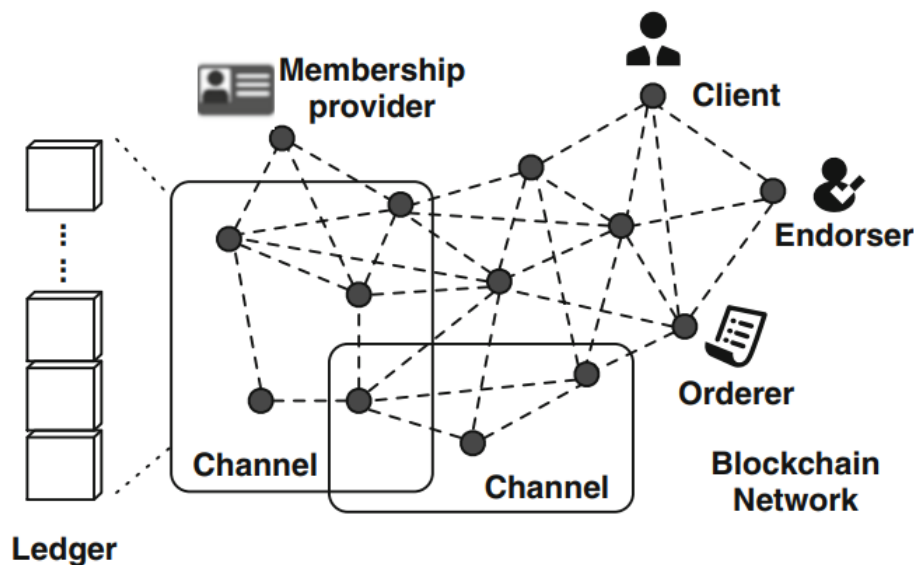


Figure 1.12: Overview of Hyperledger Fabric system[13]

1.15 Conclusion

It seems clear that Blockchain is naturally imposed in areas where the advantages of its use are considerable. Then, gradually, impose oneself on other sectors. But only time will tell how our companies will employ this technology in the future. In the next chapter, the focus is on Blockchain applications in the health sector.

Blockchain Applications in Healthcare

2.1 Introduction

Blockchain is often described as a tool for building trust between actors. Its applications have greatly evolved with technological advances and increasing interest from international companies. Blockchain technology is proving to be an important ally in the field of healthcare by several features: its immutability which makes it excellent support for authenticating sensitive data such as clinical trial consents, the ability to edit smart contracts that automate and facilitate many processes.

2.2 Blockchain Applications in Healthcare

The features of the blockchain, such as its decentralized nature, openness, and permissionless, may provide a one-of-a-kind solution for healthcare. The technology's broader application opens the door to a variety of facets of healthcare, including wearables and medical research development. Healthcare sector has growing demands for blockchain developments, and a recent survey by Deloitte shows that the traditional industry is actively explores new avenues for the use of the blockchain to address its critical needs. (Deloitte, 2018). Immutability of the blockchain is the vital option for healthcare data. It can secure medical records, clinical trial results and ensure regulatory compliance. Employment of smart contracts demonstrate how blockchain can be used to support real-time patient monitoring and medical interventions (Griggs et al., 2018). Such systems ensure security of records while providing access for patients and medical professionals in a Health Insurance Portability and Accountability Act (HIPAA) compliant manner. Further blockchain applications include the pharmaceutical supply chain and the development of anti-counterfeiting mechanisms. While the development of new drugs incur substantial costs related to trials to evaluate safety and efficacy of the drug, the use of smart contracts allow facilitating the procedure of the informed consent as well as improve

identify management and data quality (Razak, 2018). Providing patients with access to manage their own identities allows the informed consent method to be integrated while preserving the privacy of individual health data.[39]. Figure 2.1 show some applications of blockchain technology in healthcare sector.

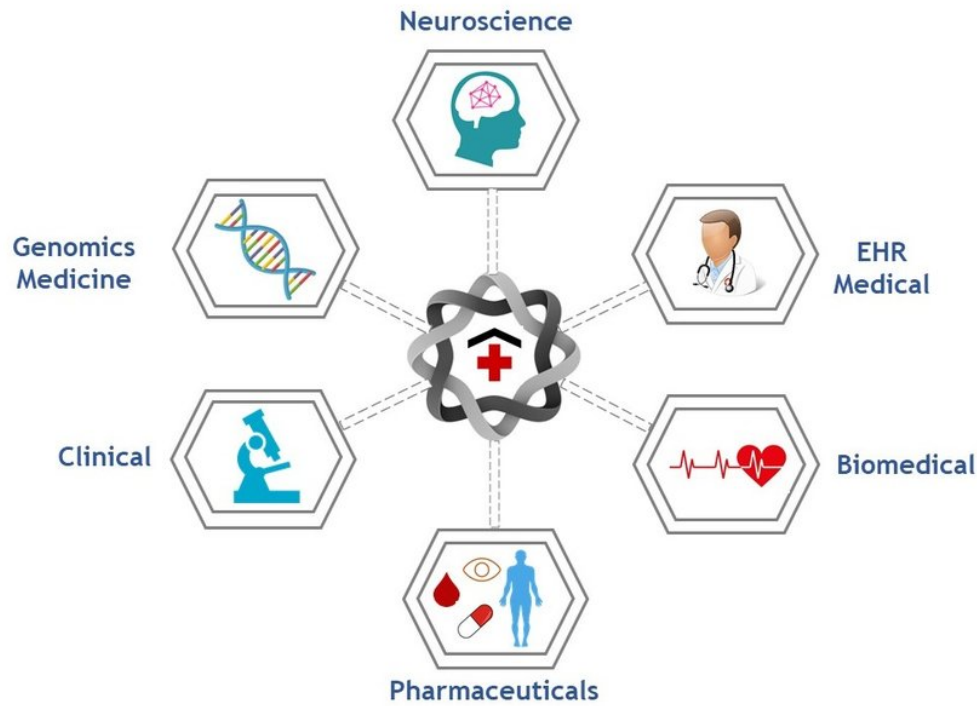


Figure 2.1: Applications of blockchains in healthcare [40]

2.2.1 Blockchains in Clinical Research

While there has been significant progress in the transition of medical data from paper to digital records, the healthcare sector is still grappling with difficulties related to patient data sharing among providers and organizations. Patients may move locations, change health insurance, and change healthcare providers for their treatments throughout their lives. The majority of their comprehensive medical records are kept in silos by each hospital or provider. In addition, each medical entity would have preserved patient data using its own storage structure and semantics. This leads to hurdles when it comes to sharing of the data.

These obstacles exist in part owing to the nature of the data in issue (Protected Health Information) and in order to avoid data blockage during transmission. This has ramifications not just for effectively treating patients across many companies, but also for clinical research, which requires real-world medical data to conduct research and test hypotheses in real-world settings using real-world data. Clinical studies require identified patient data. Consolidating and identifying patient data takes a lot of time and work, and it costs a lot of money.

The availability of huge collections of real-life deidentified raw data, analyzable datasets for secondary analysis, and meta analysis is a significant aspect in achieving improved accuracy in clinical research and trial outcomes. According to polls, the majority of customers are willing to provide their medical records for analysis and study as long as their privacy is protected and the data is kept private.[41].

2.2.2 Blockchains in medical fraud detection

The management of medicinal drug supply chains is one of the most important applications of blockchains in the medical business. Supply management is a critical issue in many industries, but it is especially important in healthcare because of its increasing complexity. This is because every disruption in the healthcare supply chain has an impact on a patient's health.[42].As a result of the numerous moving elements and individuals involved, supply chains are insecure and include openings for fraudulent attacks. By bringing better data transparency and enhanced product traceability, blockchains enable a safe and secure platform to solve this problem and, in certain situations, prevent fraud from occurring. Manipulation of the blockchain is difficult, since a record on a blockchain can only be validated and modified through a smart contract[43].

Another application of blockchain is fraud detection. Fraud detection is the process of verifying a document or other data system to detect any tampering with the data or other malicious conduct, such as preventing the injection of false reviews in online review systems in the form of bad-mouthing and ballot-stuffing, as well as fact-based fraud in the financial sector, such as loan applications.[44].

Another area of research into fraud detection is the relatively new notion of crowdsourcing. Crowdfunding is the practice of having numerous individuals invest money or buy shares in a company in order to build equity for that company. Blockchain can be used in a crowdfunding function by, making transactions and transferring of crowdfunding equities easier, more secure, and efficient, as well as being leveraged as a low-cost platform for registering of stocks and shares, enabling peer-to-peer transactions between investors and entrepreneurs. Blockchain can also be used to develop a voting system for corporate governance among shareholders, and help regulators know about market conditions and protects against investor fraud[44].

2.2.3 Blockchains in the pharmaceutical industry and research

The transparency and security of supply chain management are two major concerns in the pharmaceutical sector. Pharmaceutical companies lose millions of dollars each year owing to counterfeit drugs. Pharma companies deal with products that directly impact the lives of their consumers, which is why efficacy and safety of the product is paramount. The journey of the product from manufacturer to consumer has multiple

stages: transportation, handling, storage, redistribution, retail. Things can go wrong during these stages, from simple human error to malicious intent (fraud). In a traditional system, identifying the problem might be difficult, since supply chain participants typically keep their own records and communicate information just one level up and one level down the chain. Furthermore, if these documents are kept on paper, they are more likely to include mistakes. These variables add to the time it takes to find out what's wrong with the drug supply chain. Additionally, with governments and consumers demanding transparency in the supply chain for such products, companies have worked towards maintaining an open or transparent supply chain system. Depending on one organization to track irregularities still isn't foolproof.

Blockchain helps in addressing the supply chain issues by providing a distributed ledger which is shared among all the stakeholders within the supply chain. The records entered the blockchain at each stage in the supply chain are immutable, permanent and decentralized. This in turn removes the vulnerability of introducing errors or fraud. Counterfeit medications are decreased by keeping a chain of custody log, which allows businesses to follow each stage of the supply chain at the level of a single drug or commodity. With the blockchain system in place, even the end customer now has access to all product information, from manufacture to consumption[41].

2.2.4 Blockchain in Claim and Billing Management

Fraudulent claims and billing are one of the losses in healthcare that must be eliminated and avoided. Medical billing fraud is still prevalent in the healthcare sector. Providers claiming charges for non-performed services, overcharging for actual services, performing unnecessary services for a patient's medical condition, and misrepresenting non-covered medical services as covered medical services in order to obtain claims money and cover financial losses are some of the most common healthcare frauds. Many intermediaries are involved in verifying and adjudicating claim information in order to guarantee that claim processing takes as little time as possible and that administrative costs for providers and payers are minimized. A typical claim adjudication procedure entails a lot of back-and-forth communication between the parties engaged in the claims process. Blockchain system helps reduce most of these challenges faced during claim adjudication and payment processing activities. The blockchain solution can automate the required workflows and then all the parties involved can share a single copy of the contracts and billing related information[41].

2.2.5 Blockchain For Electronic Health Records

The ideal scenario for electronic health records (EHRs) is to keep a permanent medical record that can be accessed by the care team, including doctors, lab technicians,

and others, at the point of treatment and on time. Patient data is currently kept across many organizations throughout the patient's lifetime in current EHR deployments. Few sections of a patient's medical record like medication problems, diagnosis are recorded by the physicians, and they continue to retain stewardship of those sections after a patient's treatment. A patient has stewardship of the medical record in a blockchain implementation, and physicians will be granted access on a need-to-know basis using "smart contracts." One of the key challenges for EHRs is the accurate management of records, which includes the repair of any incorrectly recorded data. Apart from ensuring data integrity, different providers and hospitals system face interoperability challenges leading to ineffective data sharing, if any at all. The lack of coordination in data management and exchange leads to health records being fragmented. Blockchain framework can help alleviate data fragmentation issues across healthcare entities. With blockchain implementations for EHRs, members of a private, peer to peer network can share the block content with appropriate viewership permissions, while the original member maintains ownership of the data shared. In addition, blockchain supports "smart contracts, which are basically self executing contracts with the terms of agreement coded in them. Smart contracts allow automation and tracking of state transitions like viewership rights or new record creation in a system. To guarantee data integrity, blockchain includes cryptographic hashing of records. The care team can add new records to a patient's profile, and the patient can authorize which providers have access to the information. This encourages patient and provider participation and aids in the development of patient records. Blockchain architecture is built on principles of decentralization and cryptography, which could contribute to more secure and highly interoperable EHR systems[41].

2.3 Management and sharing of health data

2.3.1 Health data sharing

Data sharing presents one of the greatest opportunities to improve healthcare.[45]. Blockchain technology has the potential to considerably simplify the process of sharing healthcare data and aid in the resolution of the healthcare industry's interoperability challenge. Patients are identifiable in the permissioned healthcare blockchain by their hash ID, which will be their unique identity.

The hashing allows the ID to be unique and secures the privacy of the user. Patients would oversee sharing the decryption key for their own associated blocks of data with their chosen healthcare provider(s). It improves security, privacy, and interoperability, and it has the potential to place patients at the heart of the ecosystem. Accurate, up-to-date, and thorough medical records would be extremely beneficial to both patients and providers[46].

2.3.2 Health data management

In general, each patient is unique, so similar strategies may not be applied because of inter-individual variability[47]. Therefore, it is essential to have access to complete medical records to provide personalized care. However, sharing such records among the medical community has become a very crucial issue because today's most of the medical systems do not ensure trust, privacy, and security[48].

Patients also cannot claim full ownership of their medical records because they have the ability to edit or erase information from them. In most cases, when patients transfer to another clinic, they must repeat past testing, incurring additional fees. Blockchain is a promising technology that may be able to help with the aforementioned issues. As demonstrated in Fig. 2.2, it stores data on a decentralized peer-to-peer network that can only be accessed via smart contracts. Such data can be transferred from one hospital to another without worrying about misuse. Consequently, it helps new doctors to know about the previous patient history, which leads them to better understand the situation and treat them accordingly.

Furthermore, because patients do not have to repeat diagnostic tests that have already been done, blockchain helps to save further expenditures. So each copy of the patient record is kept on various nodes in the blockchain network, it is transparent and free of corruption.[49].

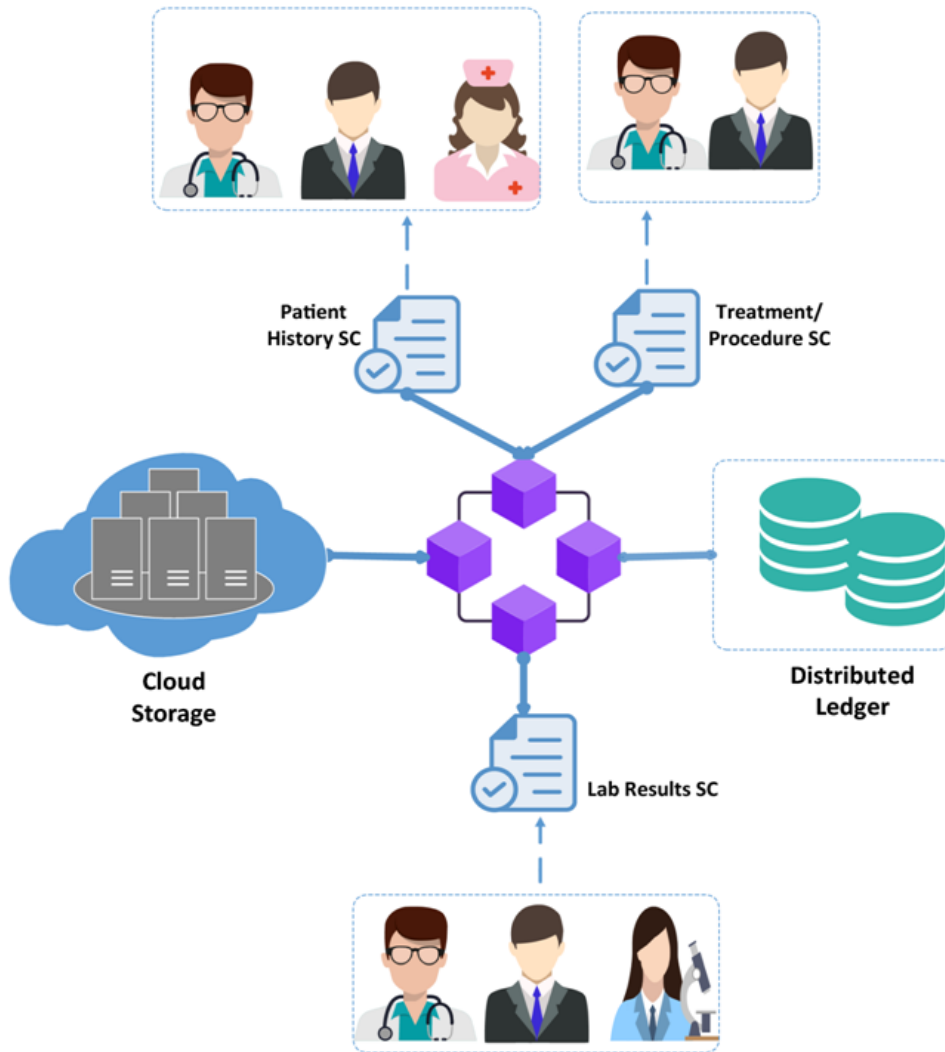


Figure 2.2: A simplified example of blockchain-based patient record management [49]

2.4 Communication of health data between the various actors of patient care

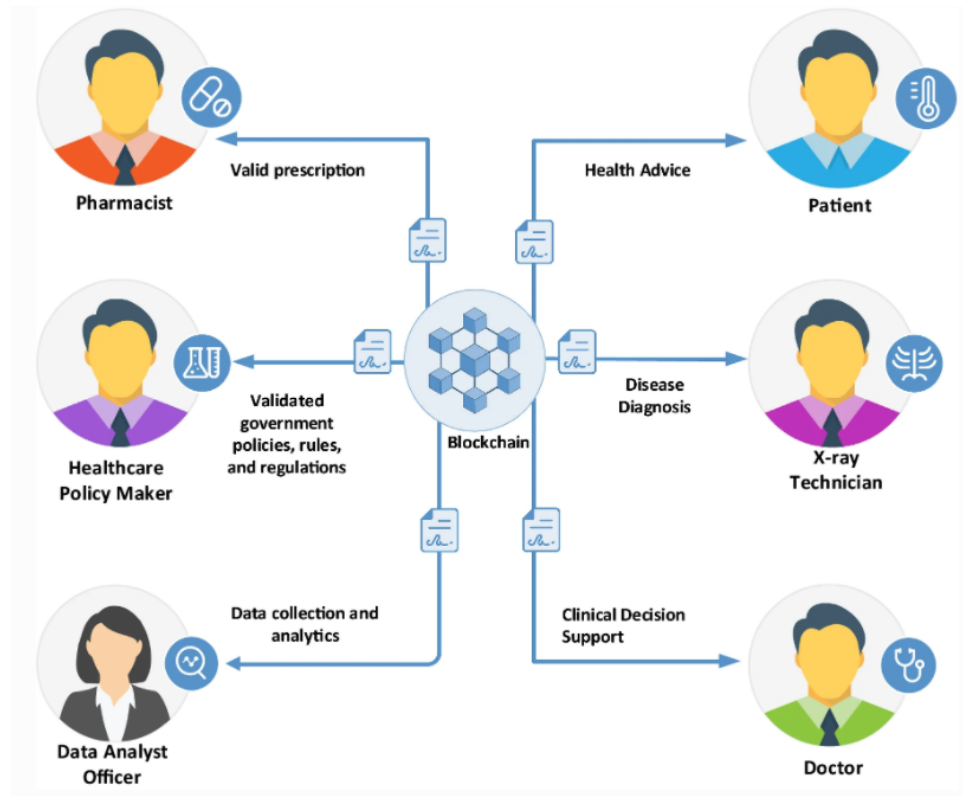


Figure 2.3: Blockchain-enabled healthcare systems [49]

2.5 Comparison between the classic solution and the blockchain solution

We all have a medical record. Then we lose it, or we stop using it, or we don't know how to fill it up correctly - which is not done by the medical professionals. This is terrible since our patient follow-up becomes far more ad hoc: vaccinations, allergies, and other medical histories. There is a lot of information that is important for establishing a diagnosis or handling an emergency, yet it is easy to lose.

In the late 1960s, the notion of employing digital technology to assist store and manage medical data was born. It remained a notion until 2004, when trials to establish a Shared Medical Record were conducted (SMR). The SMR did not meet expectations since there was no motivation to complete it and the service was not clear. At the same time, several companies and research articles offer blockchain-based solutions. Although, this paves the way for many improvements in patient monitoring[50].

Properties	Classic solution	Blockchain solution
Architecture	Client server (master-slave)	Distributed ledger
History of records	It is a snapshot of current status	Real time information along with previous information
Control	Single point of control (administrator)	Decentralized
Confidentiality	Information is only visible to members	Information is secure and visible to everyone on the system
Intermediary	yes	no
Consensus	Distributed transaction (2 phase commit)	Majority of peers agree on the outcome of transactions
Data persistence	Non-persistence	Immutable
Security	Authority	Cryptography
Operations	Write, read, update, delete	Read and write only

Table 2.1: Comparison table between classic solution versus blockchain solution

2.6 Emerging blockchain-based healthcare solutions

Several companies have started developing and disseminating blockchain technology for the healthcare sector. These companies blockchain-based platform and software offer a variety of services, including assisting the healthcare industry in securely storing digital records, improving the way medical data is shared and used, protecting the integrity of health records, and providing a solution to drug traceability and counterfeiting. Table 2.1 lists health-related Blockchain goods and important players who provide unique blockchain solutions for a variety of applications.[46].

Company/ Platform	Industry	Applications
MEDREC	<ul style="list-style-type: none"> • Big Data • Cybersecurity • Software 	<ul style="list-style-type: none"> • Uses blockchain for electronic medical records • It is designed to manage authentication, confidentiality, and data sharing
BURSTIQ	<ul style="list-style-type: none"> • Big Data • Cybersecurity • Software 	<ul style="list-style-type: none"> • Uses blockchain to improve the way medical data is shared and used • It is a HIPPA compliant platform used by large enterprises and government agencies for on-chain data management, complex data ownership, and granular consent
FACTOM	<ul style="list-style-type: none"> • Enterprise Software • Information Tech 	<ul style="list-style-type: none"> • Employs blockchain technology to help the healthcare industry securely store digital records on the company's blockchain platform
MEDICALCHAIN	<ul style="list-style-type: none"> • Electronic Health Record • Medical 	<ul style="list-style-type: none"> • Employs a blockchain-based platform that protects the integrity of health records and maintains a record of the origin and protects the patient identity
GUARDTIME	<ul style="list-style-type: none"> • Cybersecurity • Blockchain 	<ul style="list-style-type: none"> • It helps healthcare companies and governments implement blockchain into their cybersecurity methods
ROBOMED	<ul style="list-style-type: none"> • Blockchain • Medicine 	<ul style="list-style-type: none"> • It uses blockchain to securely gather patient information and share it with a patient's healthcare providers
PATIONTORY	<ul style="list-style-type: none"> • Blockchain • Cybersecurity • Healthcare • Information Tech. 	<ul style="list-style-type: none"> • Uses blockchain platform for the secure storage and transfer of important medical information
BLOCKPHARMA	<ul style="list-style-type: none"> • Blockchain • Pharmaceuticals • Supply Chain 	<ul style="list-style-type: none"> • It uses blockchain technology and offers a solution to drug traceability and counterfeiting
NANOVISION	<ul style="list-style-type: none"> • Blockchain • Cybersecurity 	<ul style="list-style-type: none"> • Combines the power of blockchain with AI to gather data from traditional data silos and incompatible records systems
TIERION	<ul style="list-style-type: none"> • Blockchain • SaaS 	<ul style="list-style-type: none"> • The company uses blockchain to audits documents, records and medicines to keep a clear history of possession and to maintain proof of ownership throughout a medical supply chain
CONNECTINGCARE	<ul style="list-style-type: none"> • Cybersecurity • Blockchain 	<ul style="list-style-type: none"> • Tracks the progress of patients after they leave the hospital
NEBULA GENOMICS	<ul style="list-style-type: none"> • Biotechnology • Genetics 	<ul style="list-style-type: none"> • The company uses blockchain to eliminate unnecessary spending and middlemen in the genetic studying process

Figure 2.4: Emerging blockchain solutions for healthcare [51, 52]

2.7 Related work

Solving the problems with EHR storage and sharing is a popular topic, and there are a variety of ways and techniques that may be applied. Matos et al. proposed a system architecture and solution for managing electronic health records (EHR) through the utilization of cloud services and granular access control[53]. The objective was to develop a secure and scalable EHR solution that would allow a patient or provider to view a record from anywhere in the world. The storage of the EHR is an intercloud, an intercloud is the way of chaining singular clouds together creating a mass of clouds which then is referred to as an intercloud or cloud of clouds. Interclouds provide benefits in the way it supports end-to-end privacy for cloud application, and the ease of migrating data between providers. Furthermore, Matos et al. Their access control approach is based on authentication and a privilege check, according to them. While the system's ultimate purpose was to ensure a patient's privacy, it is nevertheless vulnerable to vulnerabilities

that result in a criminal having access to data he or she shouldn't have.

Action-EHR is a proposed framework by Dubovitskaya et al. [54]. The proposed framework runs on Hyperledger Fabric, Hyperledger Fabric is a private/permissioned based blockchain framework, which gives stronger authentication and authorization rather than the open public blockchain where any node can willingly connect and view transactions [54]. Similar to the Ethereum network, Hyperledger Fabric allows for smart contracts to be made. Action-EHR makes use of the logic in the smart contracts the same way as previously mentioned frameworks, where the main purpose is to store the state variables regarding access control to a certain patient's health record. Action-EHR makes use of HIPAA-compliant cloud storage, instead of a local database. A HIPAA-compliant cloud storage can ensure that they will to the best of their capacity make sure that the information stored keeps its integrity, confidentiality and, availability.

Amazon S3 is the cloud storage solution utilized by Action-EHR. Before uploading a record to storage, it is encrypted with a symmetric key technique, which is then encrypted on the cloud with the patient's public key and the doctor to whom the patient has granted access. Decrypting the records, the doctor uses his private key to retrieve the symmetric key, which then is used to decrypt the data. The researchers propose that just a symmetric key be used, since this would simplify key management and allow the patient to only upload his information once if he has more than one doctor with whom he wants to exchange his records. While with the earlier described approach, the patient would have to upload data for each of the doctors that need access [54]. They finish their study by claiming that the prototype fits the requirements from a medical standpoint, and that their next step will be to build up a test network and put it through its paces in a genuine healthcare context.

2.8 Conclusion

Blockchain technology is a new technology that has the potential to impact not only a few sectors, but also the way companies are conducted. Blockchain technology has begun to be used in healthcare. The majority of blockchain use cases in healthcare are aimed at providing patients with secure and integrated treatment.

In the next chapter, we will propose a new system for securing the distribution of shared medical records using Blockchain technology. The proposed system solves this problem by managing health data using electronic medical records based of Blockchain to create an ecosystem to reduce the challenges and problems faced by traditional EHR systems.

Design a Blockchain approach for Health Record Secure Shared

3.1 Introduction

In the healthcare sector, Blockchain technology has the power to act on the sharing of medical data, by storing the data itself or by indicating who can access this data. This provides patients with proof and certainty that the record cannot be edited, thereby ensuring confidentiality. In this chapter, we introduce the system entities: Health Record Secure Shared, which interact to provide the control service and data protection in the exchange of health information. We put highlights the role of blockchain in the process and briefly describes the blocks created to further secure the process with the use of the cloud database. So, we're going to present the architecture in general of our EHR system, as well as its detailed design applied in the health sector.

3.2 Global architecture

In the healthcare sector, we will incorporate actors involved in patient care into our conceptual model. We consider the doctor, pharmacist, and laboratory analyst., ... etc.

3.2.1 Steps of development

The development of a Blockchain application also requires us to delimit the scope and purpose of the application. The following are the steps involved in developing a Blockchain application:

Step 1 : Clarification of the idea

1. The first question to be answered is :

Why we use Blockchain ?

The main reasons why it is better to use the Blockchain are:

- **Security :** Blockchain technology is more secure than centralized databases. This means that a Blockchain is a lot less likely to be the target of a hacking attempt, because there is no single point of failure. Medical information of the patient will be more secure, which allows the patient not only to have visibility on its data, but also to control access.
- **Interoperability:** Blockchain enhances interoperability among clinics, hospitals and other healthcare providers. This will ensure that service providers can work together on one system.
- **Transparency:** Blockchain systems can also give patients greater levels of transparency over their own healthcare information. It is also possible to provide a further level of security against human error and intentional falsification.

2. The second question is:

Is it necessary to use Blockchain?

The answer without a doubt, yes. And, to demonstrate why a Blockchain is so important, consider the decision tree. Figure 3.1 shows you providing all the answers to the questions you've been given. To begin, we'll need a database where we can write and therefore preserve medical patient information such as prescriptions, analyses, X-rays, and so on. Because we have no faith in the other participants, the Blockchain makes sense for our system. Finally, because we require centralized control, we have chosen to use a private Blockchain.

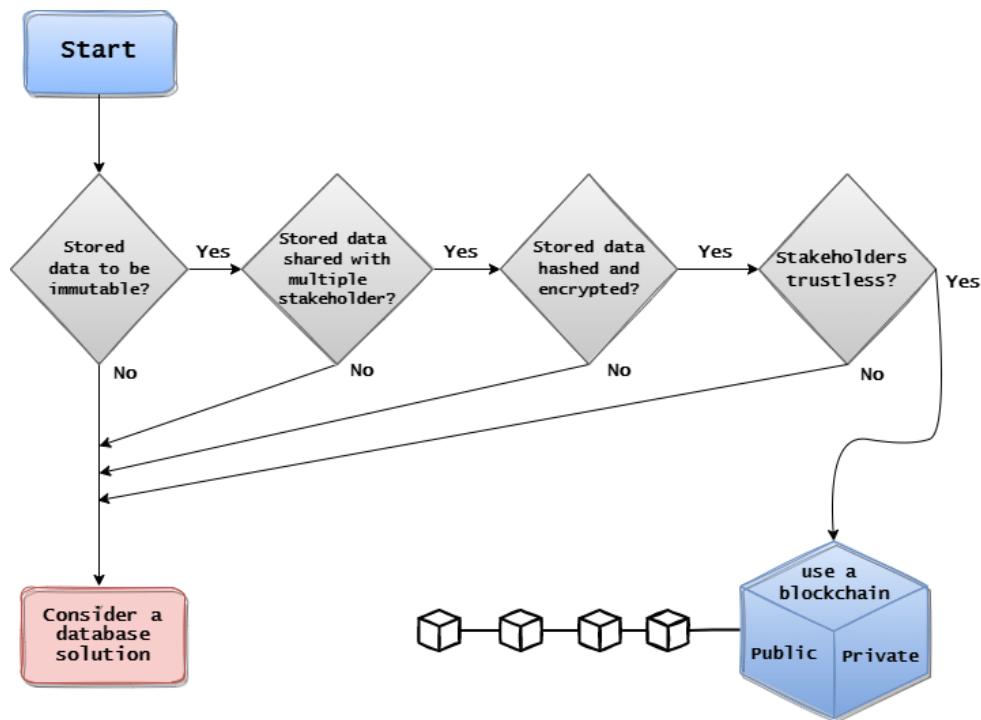


Figure 3.1: Blockchain decision tree [55]

3. the third question is :

why we use cloud database ?

Traditional databases are often limited by their capacity to ingest large quantities of information. Using a cloud database removes the issues of dealing with large datasets by giving you access to data storage that expands to meet your needs.

Cloud databases have several advantages over traditional on-site databases. With a cloud database, organizations can accommodate rising data management needs without increasing infrastructure. They can also manipulate the data quickly—efficiently dividing, delivering, and moving their data closer to their users.

Step 2 : Problem Identification and Purpose

The problem is that seeing all of a patient’s relevant health data is challenging. This information is gathered from a variety of sources, including doctors, hospitals, insurance companies, pharmacists, and medical analysis labs. When a patient is admitted to the hospital. Health professionals may not always have access to its past, and there is no complete visibility on the therapies he receives, his sickness history, and his family history. As a result, by following the antecedents, our approach aims to tackle this problem. Medical history and the patient’s present health. He conducts the tests, analyses, and surgeries, and as a result, the appropriate therapies are mentioned.

Step 3 : Identification of EHR system actors

Obviously, the actors of our system are:

- **Users** : Doctors, hospitals, insurance companies, pharmacies, medical analysis laboratories, and so on, on the one hand. On the other hand, there are the patients.
- **Organizers** : The system administrator is specified here.

Step 4 : Identification of the most appropriate consensus mechanism

The system nodes are known and validated by the administrator for the medical personnel and by the latter for the patients because we chose the private platform for our system. As a result, there is no need to set up an extremely greedy PoW algorithm in comparison to Bitcoin because the number of distributed nodes is modest (in terms of energy consumption). We would thus prefer to use a less powerful PoW mechanism.

The global architecture of the EHR system is presented in the following sections.

3.2.2 The EHR system's global architecture

The proposed architecture of our EHR consists of three entities, which are depicted in Fig 3.2 and mentioned below.

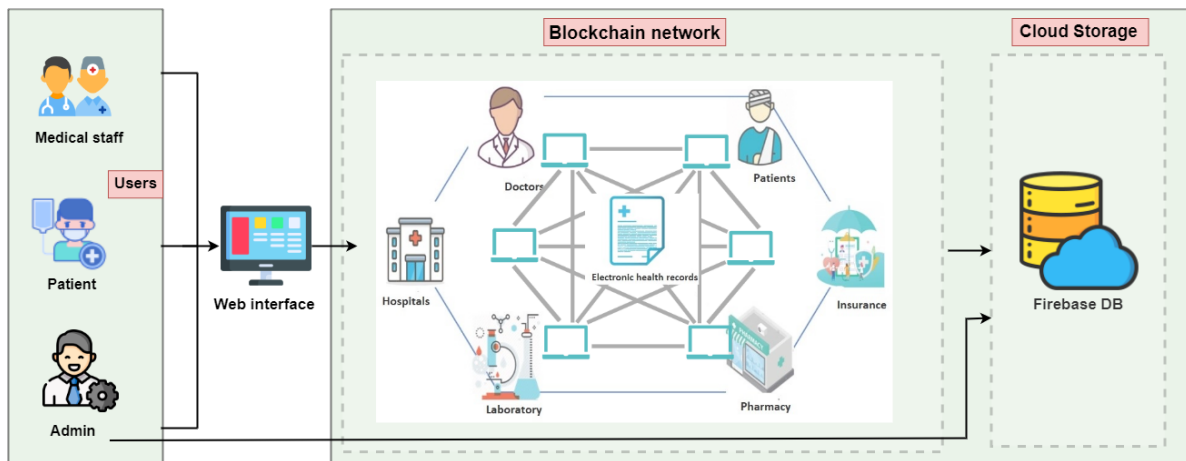


Figure 3.2: Global architecture of the EHR system

- **The EHR actors, which include the :**

1. **Users**, which include all those who need access to data to accomplish their tasks, including here **doctors** and **patients**.
2. **Administrators**, as organizers of the EHR system.

- **Storage**, Store and manage healthcare data in a distributed and decentralized manner. We chose cloud storage for the system because of its advantages, security and gives as the access to the files from anywhere that has an internet connection. In the event of a hard drive failure or other hardware malfunction, we can access the files on the cloud. It acts as a backup solution for our local storage on physical drives. The healthcare professional has full control over his patients' medical records. While a patient can only see their data without having to edit it.
- **The Blockchain network**, which receives and stores consultation logs that have been processed in blocks, as well as each consultation's details.

3.3 Overall operation

In this section of the chapter, we will go over the operational aspects of the EHR system.

3.3.1 Functional flowchart of EHR system

We begin by displaying the proposed system's functional flowchart, Figure 3.3, which depicts the tasks performed by each of its actors.

As a first step, health professionals are registered in the system and have their own account. When a patient goes to a healthcare professional, such as a doctor, the doctor must first create an account for that patient via his or her own account, if not already registered with the system and therefore has a health record. The next step is to add this patient to his patients and access the patient record to obtain a copy of it. From there, the health professional is able to view the various actions carried out on this record by other health professionals, as well as to add new health data.

When adding a new document (prescription, radio, analysis, ... etc.) to an Electronic Health Record, the system must first verify the validity of the Blockchain. The system will detect any damage to the patient record. And since there are multiple copies of this folder in the Blockchain network, the data can be retrieved simply, so we recover the validity of the file. When the validation task is finished, the document will be added to the patient record by creating a new block for that document. Finally, the block will be added after approval of all health professionals sharing the patient's record (add to the system database and the Blockchain network).

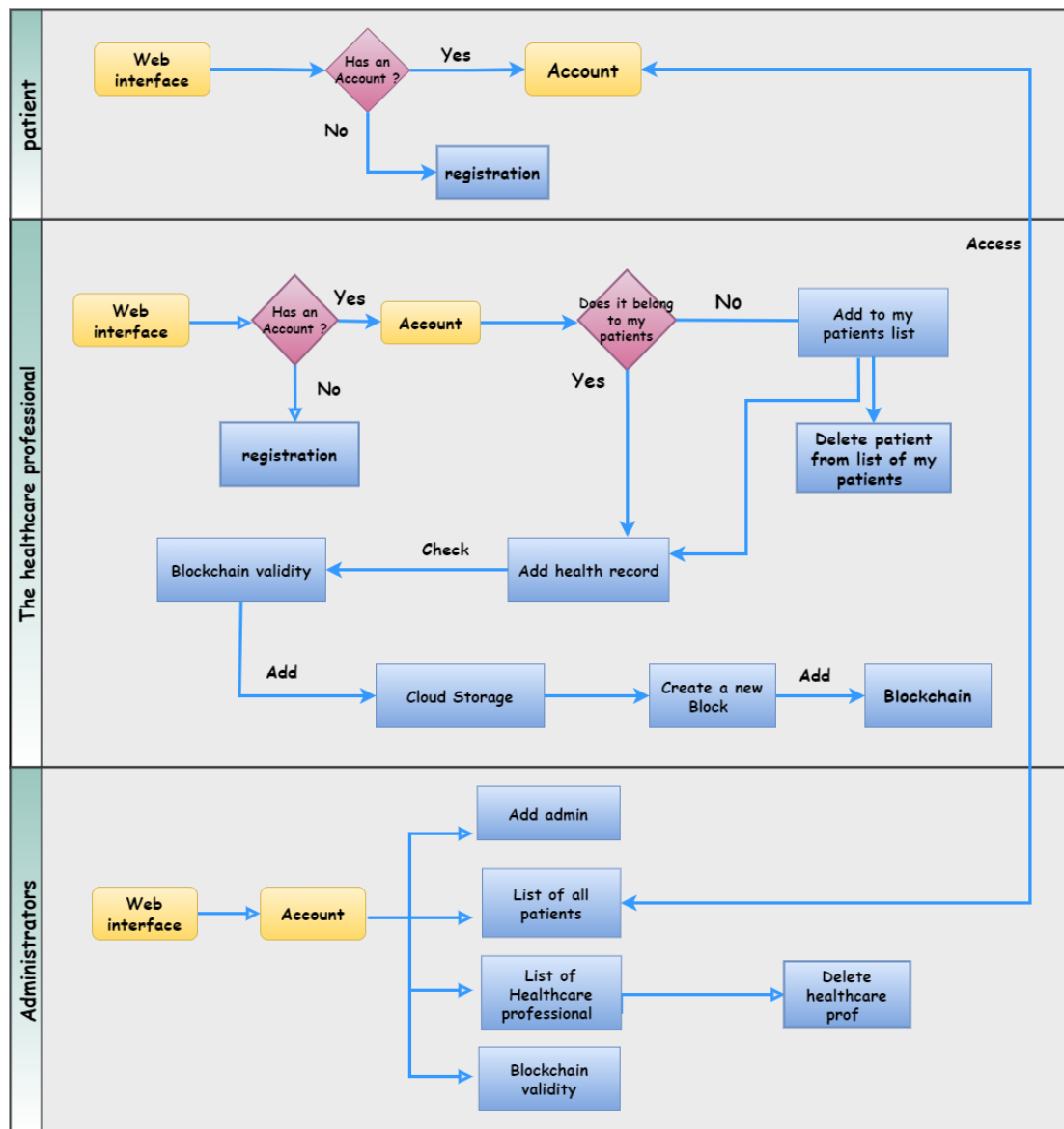


Figure 3.3: Functional flowchart of EHR system

While a patient can only consult his health record and the various actions carried out on it, view or modify his personal data.

All the patient’s medical records, including their personal information, are accessible to the EHR administrator. He can also consult the information of all health professionals, as well as their patient lists and health professional lists. In the event that a health professional dies, the administrator can delete their account from the system. You can have multiple administrators, administrator can add another administrator.

3.3.2 Use case diagram

Use case diagram are described in this subsection of the chapter to define the various interactions between each of the actors and the components of the EHR system.

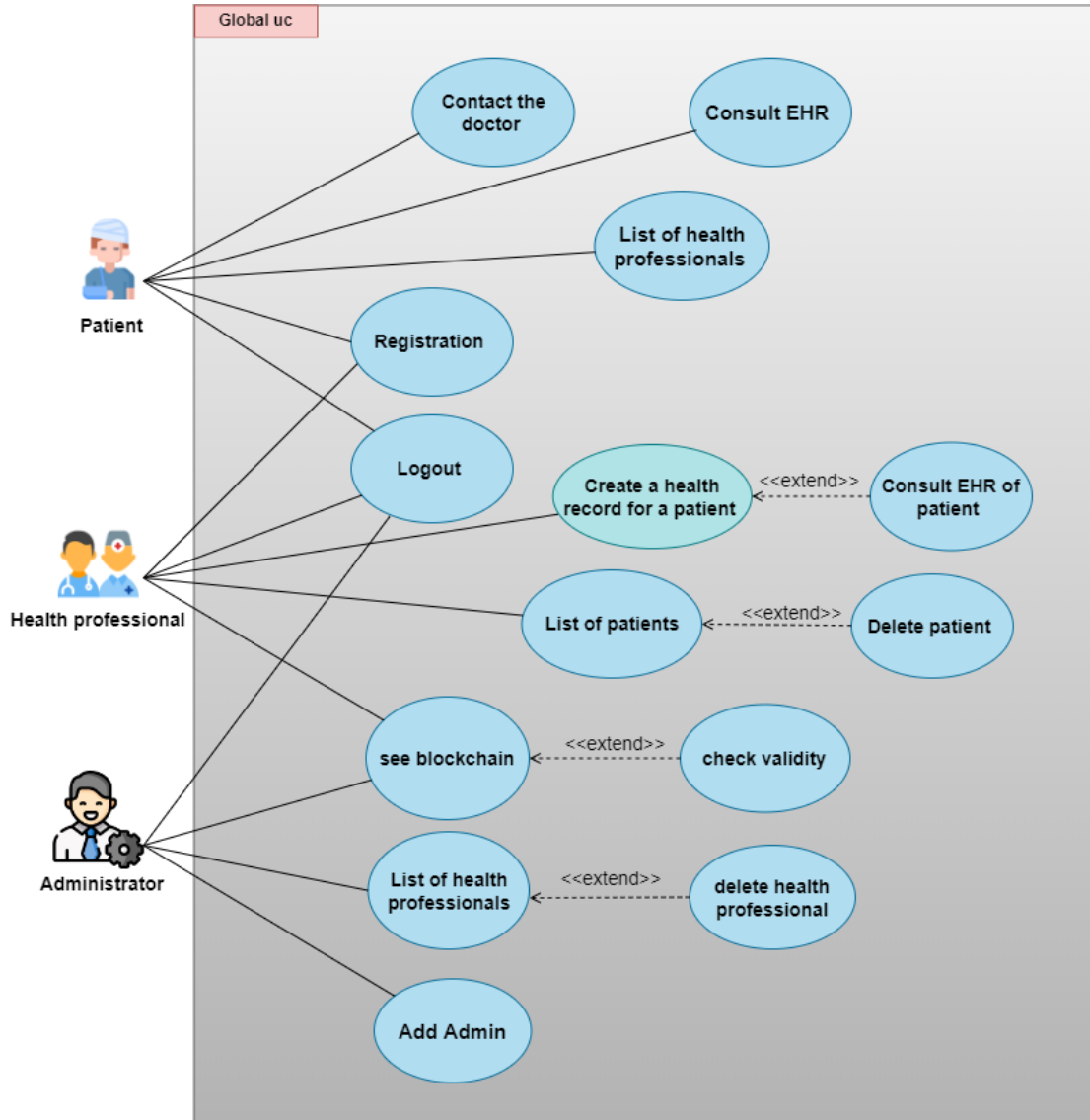


Figure 3.4: Use case diagram of our application

3.3.3 Sequence diagrams

In this part of the chapter, sequence diagrams are displayed to define the different interactions between each of the actors and the parts of the EHR system.

Sequence diagram of patient

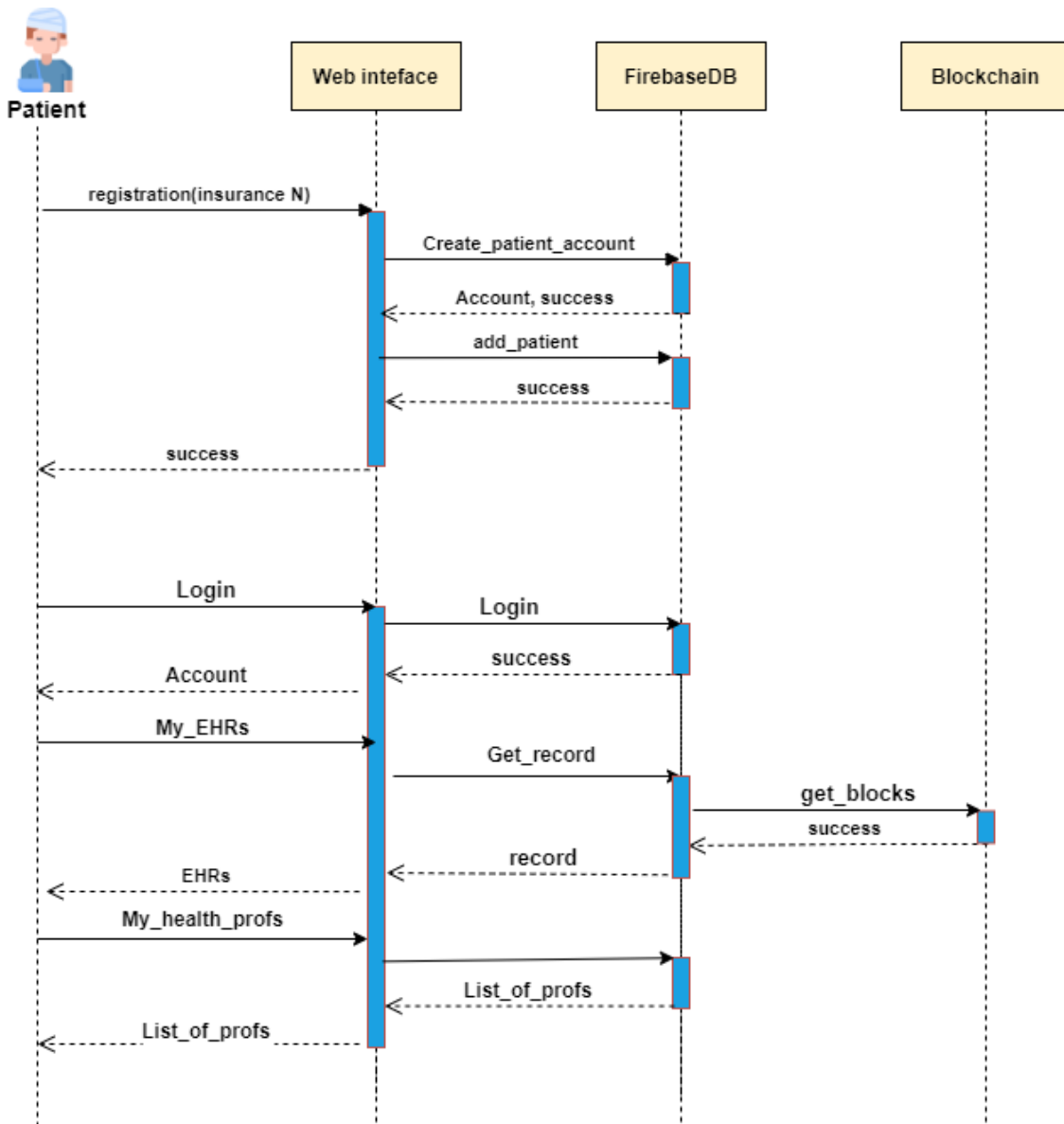


Figure 3.5: "Patient" sequence diagram

As you can see in Figure 3.5, the patient registration scenario. The successful completion of the operation results in the creation of a patient account. After registration, the patient can log in and access his record, his health professionals and view actions performed on it.

Consultation sequence diagram

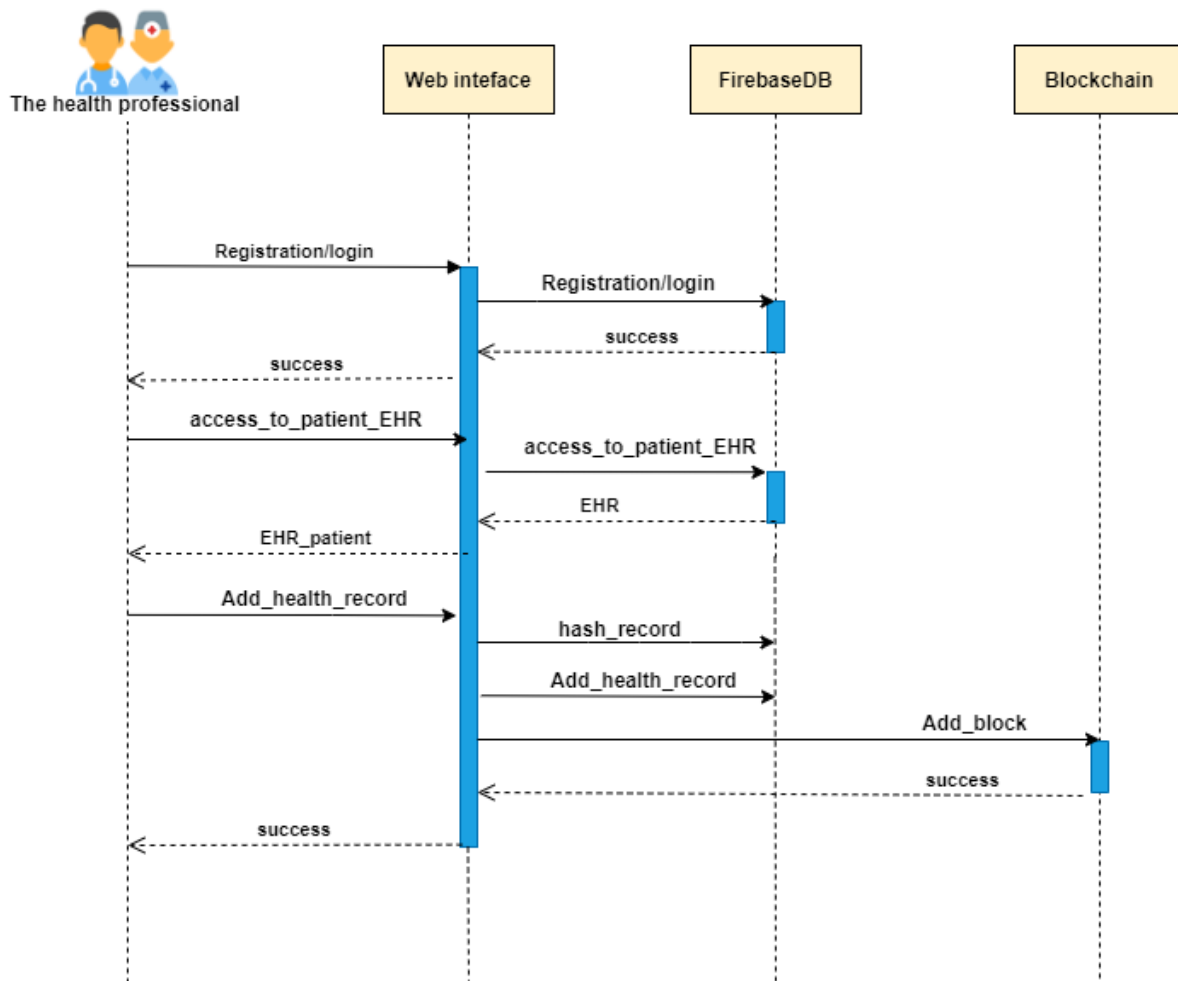


Figure 3.6: "Consultation" sequence diagram

As shown in Figure 3.6, the healthcare professional must first access the patient's medical record, of course after his authentication. Each consultation ends with the creation of a new block that describes it with new data that characterize it such as a prescription, an X-ray, ... etc., and possibly the comments of the health professional.

Sequence diagram of Health Professional

A healthcare professional can register in the EHR system, see Figure 3.7. Also, a new patient may be added to or removed from the list and the patient may be consulted.

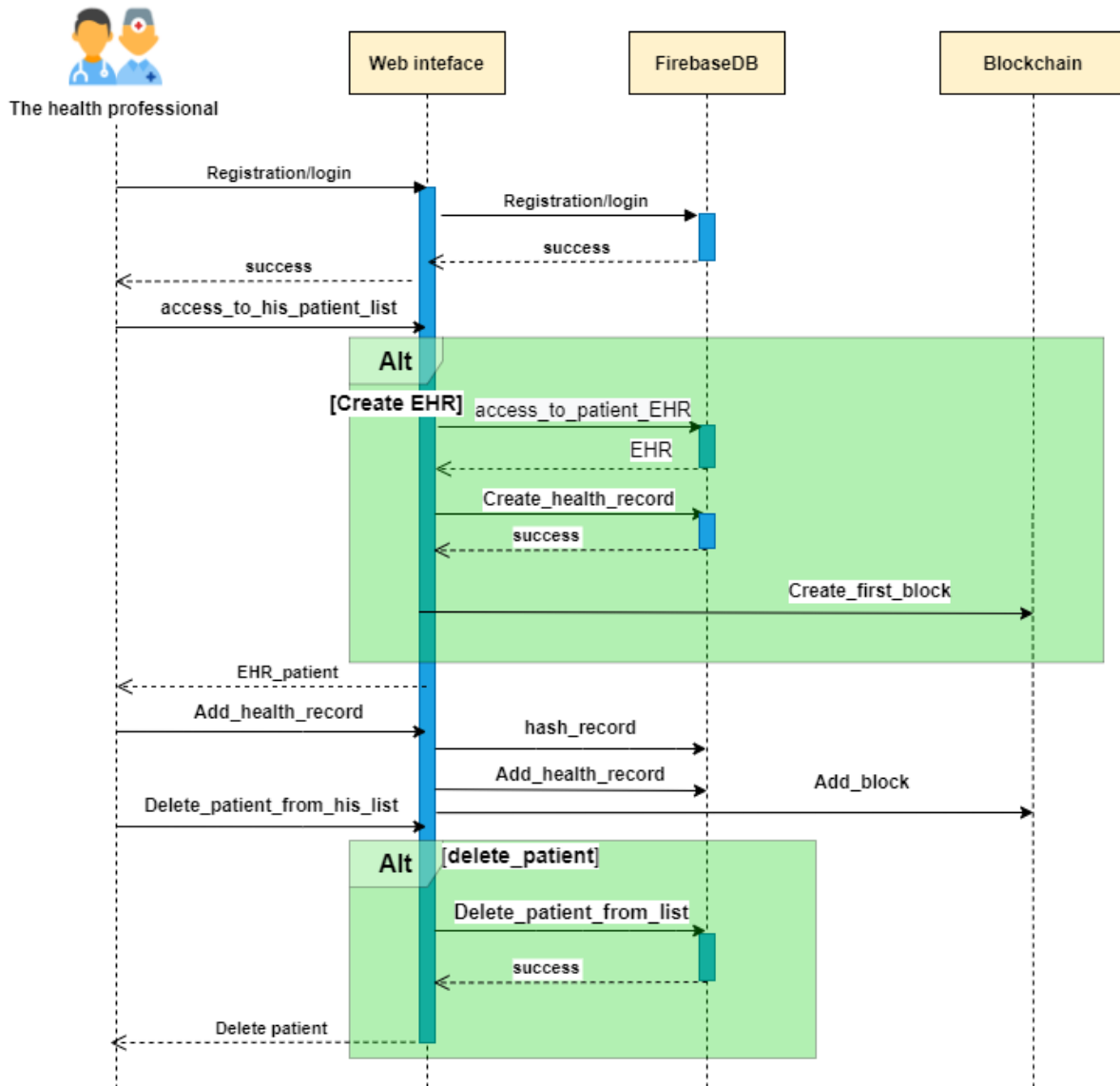


Figure 3.7: "Health professional" sequence diagram

Sequence diagram of Administrator

The administrator (Figure 3.8), like users, is required to login to access the EHR system. As his name indicates, he had the hand to consult the list of health professionals. And their information as well as patient lists and electronic health records, identify other leaders, or access blockchain. Additionally, the administrator can remove a health care professional and remove their account from the system.

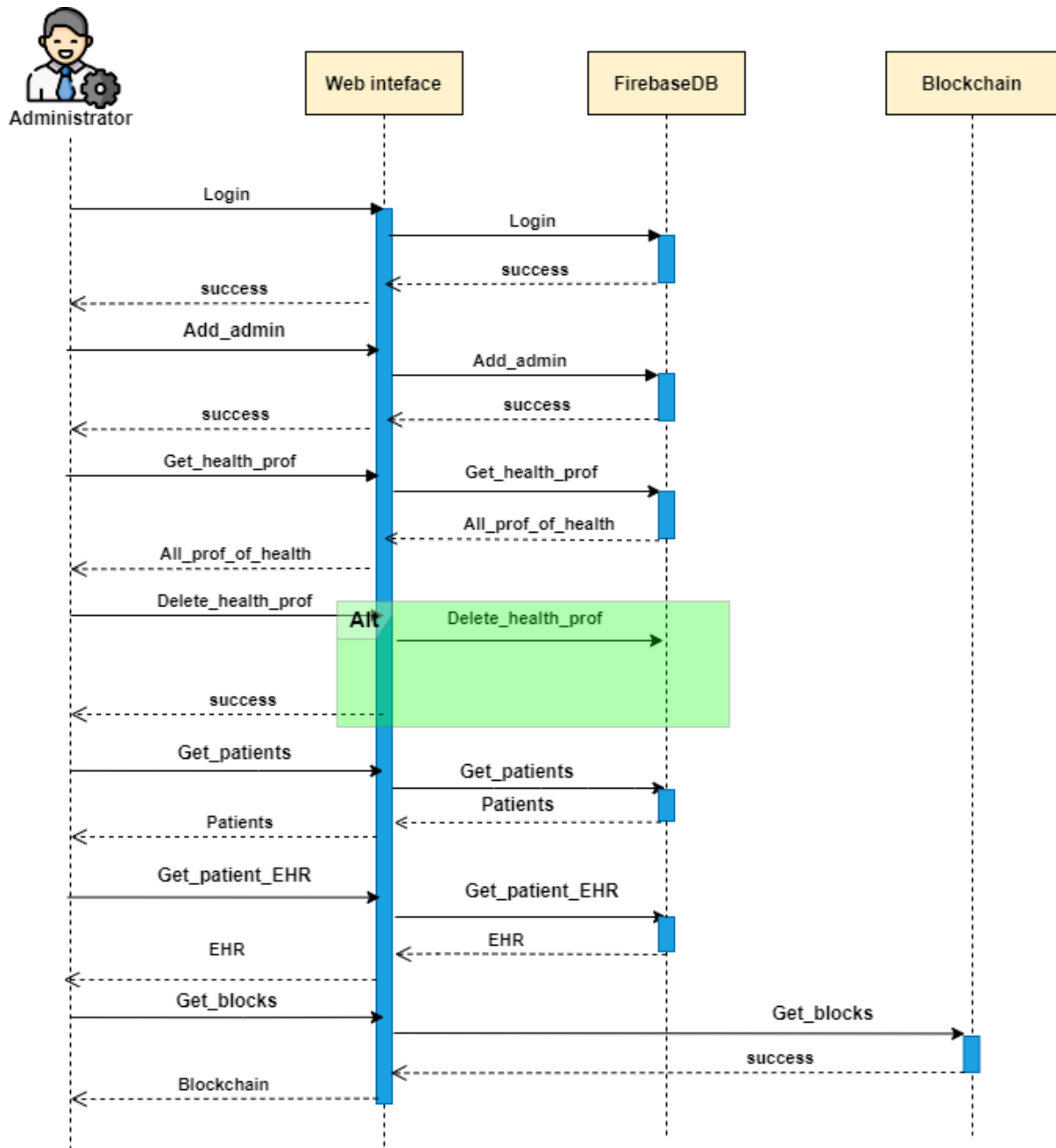


Figure 3.8: "Administrator" sequence diagram

3.4 Architecture of each subsystem

The system represents a set of modules, so we will illustrate all these units.

3.4.1 Registration

The Registration module is designed for those who need to use EHR, such as health-care professionals and patients.

Patient registration, Similarly, a patient can use his insurance number to create an account in the system’s cloud database. patient registration is accompanied by the creation of a medical record stored on blockchain in the system with help of a health professional (Fig 3.9).

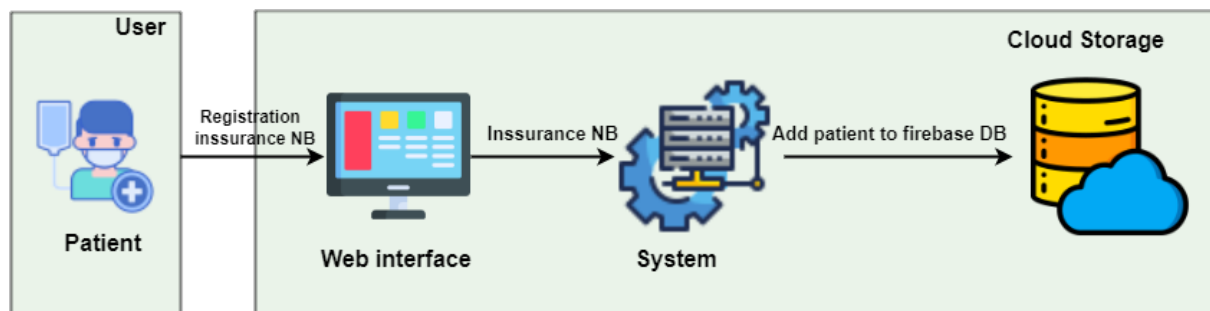


Figure 3.9: "Architecture module "Patient Registration "

Registration of health professional, The web interface allows health professionals to easily register for the EHR system by filling out a form, which is then saved in the system’s cloud database, Also can check for blockchain network (Fig 3.10).

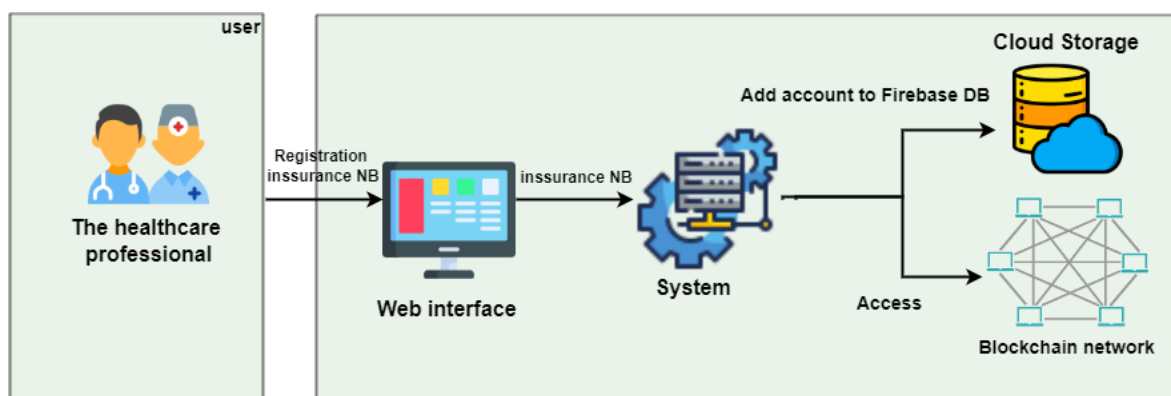


Figure 3.10: "Architecture module "Health Professional registration"

3.4.2 Administrator

The administrator has a complete view of the system. He can view the cloud storage of the EHR by displaying the user's and patients' health records, as well as gain access to the Blockchain network, through a web interface (Figure 3.11).

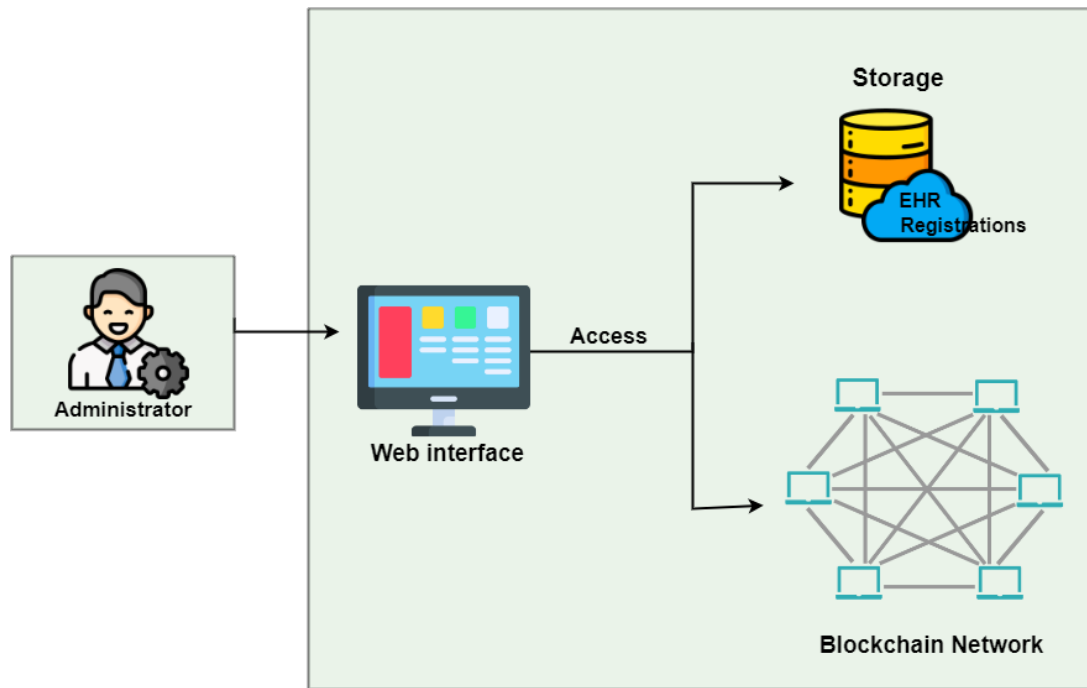


Figure 3.11: "Architecture module "Administrator "

3.4.3 Blockchain network

Patients, doctors, pharmacies, insurance companies, laboratories, and hospitals, among others, all have access to health data, which is frequently stored and shared (Figure 3.12). The health record contains highly sensitive and critical medical information that must be securely stored, shared, treated, and accessed.

Because it maintains a distributed ledger, blockchain adds more transparency between all entities involved in the network. The Blockchain provides a secure and reliable method of data sharing and management where all parties are aware of the transactions.

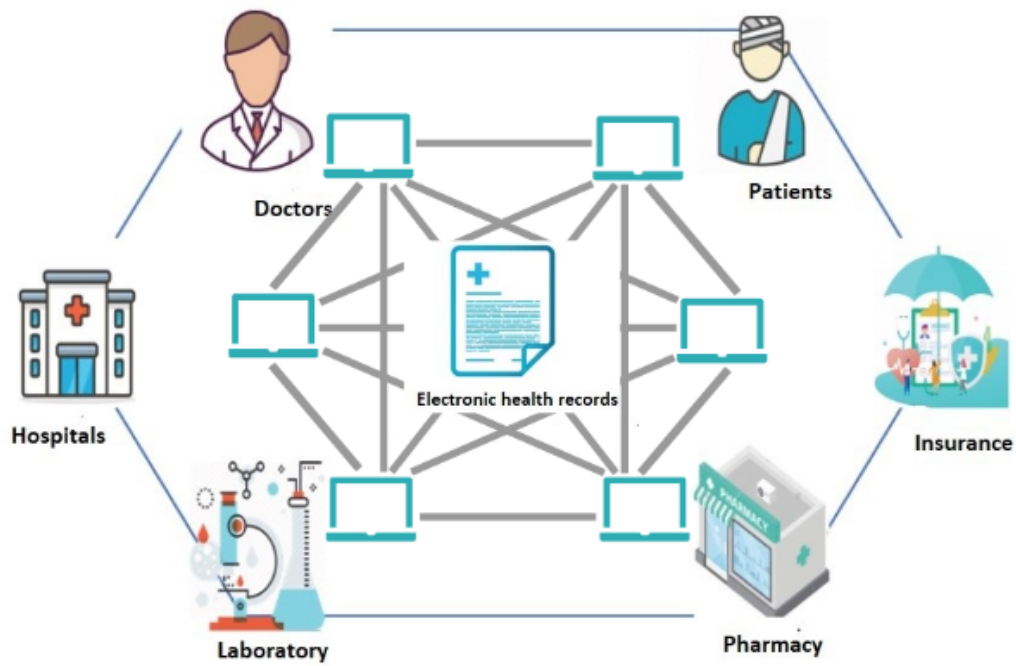


Figure 3.12: "Architecture module "Blockchain Network"

3.4.4 Add a new health record

In order to add a new health record, you must go through three steps (Figure 3.13). The file is first saved to the system cloud database (blockchain) then we calculate the document hash and store it also in the system cloud database (blockchain). The final step in this process is to make a new block for this document. Following its creation, the system distributes this block to all medical staff who have access to this electronic health record.

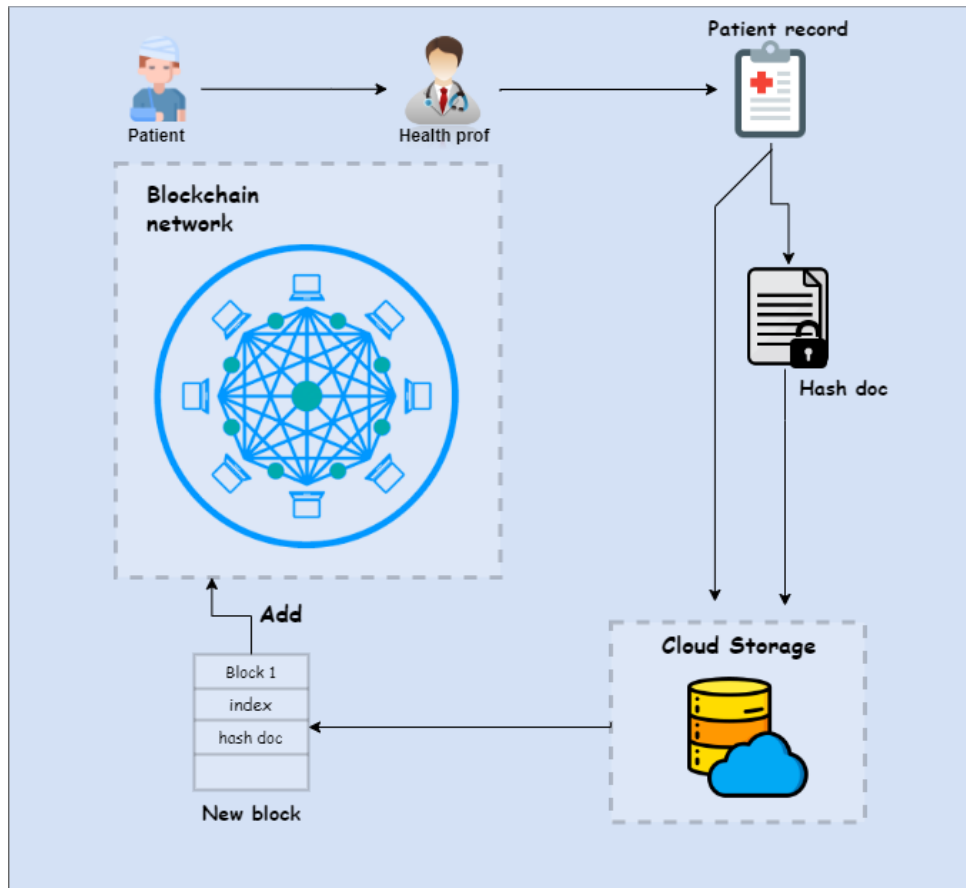


Figure 3.13: "Architecture module "Add a new health record"

3.5 Conclusion

In this chapter, we discussed how we built our EHR system based Blockchain approach to manage health data using electronic health records. The implementation of an effective EHR system is described in the next chapter.

Implementation and Results

4.1 Introduction

In the preceding chapter, the architecture and details of the EHR system and its different components. The implementation of the specified system will be presented in this chapter. We begin by listing the tools and languages that were used to build our system. Then we'll go over the main components of our system.

4.2 System Configuration and Operating System

Our system is developed under the environment:

- Laptop ASUS x560ud Processor Intel® Core™ i7-8550U CPU @ 1.80GHz, 4 Core(s), 8 Logical Processor(s), RAM 12 Go of memory and SSD 256 GB.
- Operating system Windows 10 Pro 64-bit.

4.3 Tools and Programming Languages

Firstly, the main tools we have used to implement our system are the following.

4.3.1 Visual Studio Code

Visual Studio Code is a lightweight but powerful source code editor which runs on your desktop and is available for Windows, macOS and Linux. It comes with built-in support for JavaScript, TypeScript and Node.js and has a rich ecosystem of extensions for other languages (such as C++, C, Java, Python, PHP, Go) and runtimes (such as .NET and Unity)[56].We implement the project with VSCode editor because free and open-source,

(meaning a program's code can be viewed, modified and shared), also it has features like IDE and easy to use.



Figure 4.1: Visual Studio Code logo

4.3.2 JavaScript

JavaScript is a scripting language for creating dynamically updating content, controlling multimedia, and animating images.



Figure 4.2: JavaScript logo

4.3.3 Bootstrap

Bootstrap is the most popular front-end open source toolkit for building websites and web apps, with a responsive grid system, a large number of prebuilt components, and powerful JavaScript plugins.[57].



Figure 4.3: Bootstrap logo

4.3.4 JQuery

jQuery is a feature-rich, fast, and small JavaScript library. With an easy-to-use API that works across a variety of browsers, it simplifies HTML document traversal and manipulation, event handling, animation, and Ajax.[58].



Figure 4.4: jQuery logo

4.3.5 HTML and CSS

- **HTML** is the markup language we use to structure and give meaning to our web content, such as defining paragraphs, headings, and data tables, as well as embedding images and videos in the page.
- **CSS** is a set of style rules that we use to apply styling to HTML content, such as changing background colors and fonts, and arranging content in multiple columns.



Figure 4.5: HTML and CSS logo

4.3.6 Google Firebase

Firebase is a development platform that offers a wide range of services, including hosting, database management, analytics, authentication, and much more.[59].

Firebase is a Backend-as-a-Service (BaaS) app development platform that provides hosted backend services such as a real-time database, cloud storage, authentication, crash reporting, machine learning, remote configuration, and hosting for your static files[60].



Figure 4.6: Google Firebase logo

4.3.6.1 Firebase products

Firebase is designed with the aim of freeing users from the complexity of creating and maintaining a server architecture, while guaranteeing foolproof scalability (several billion users) and ease of use, see figure 4.7 show us Firebase console.

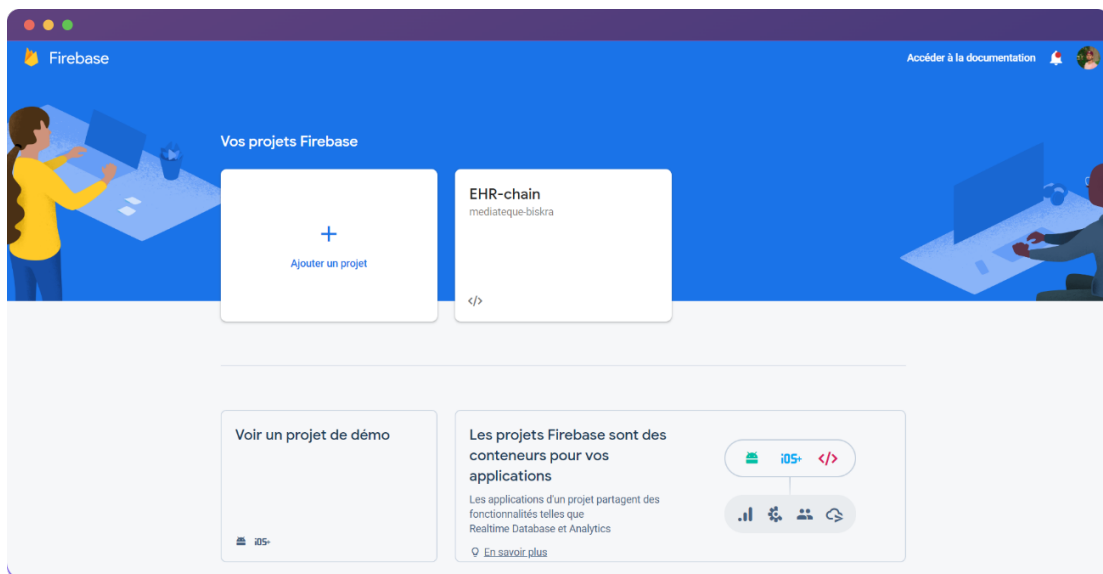


Figure 4.7: Firebase console

For this, Firebase has been broken down into several extremely rich products adapted to the mobile world and web apps, of which we will cite some of them we used in our system.

- **Authentication:** aims to make building secure authentication systems easy, while improving the sign-in and onboarding experience for end users. It provides an end-to-end identity solution, supporting email and password accounts (Figure 4.8).

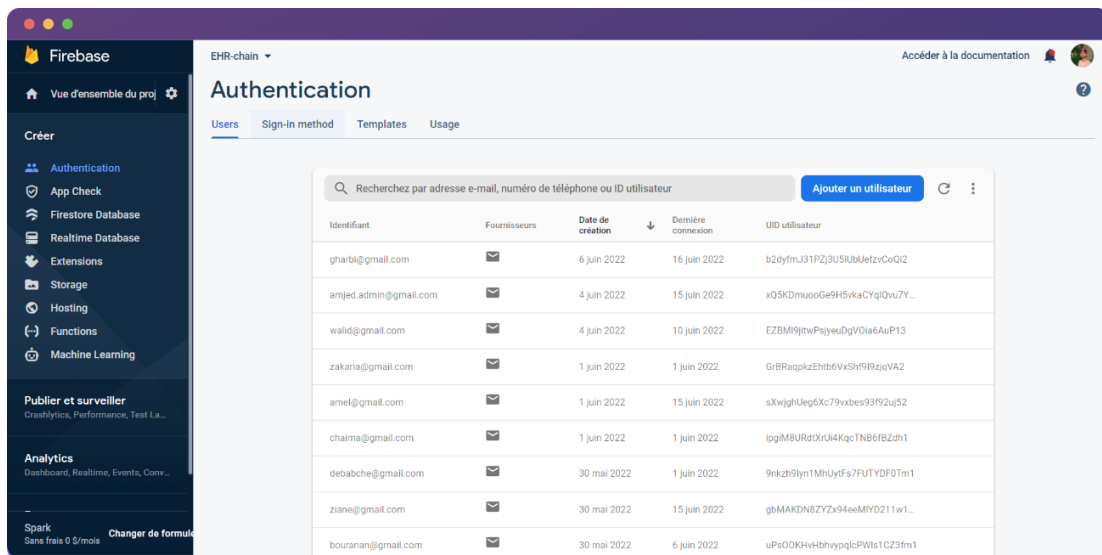


Figure 4.8: Authentication

- Real-time Database:** is a cloud-hosted NoSQL, cloud database that stores data in JSON format. Since data is stored, processed and shared between users in real time, the database always provides synchronized data across users. Firebase facilitates the storage of data in a local cache whenever a user goes offline; the user receives updated and synchronized data from the cache, once he/she is online. All these features are handled by Firebase itself, without the need of any server (Figure 4.9).

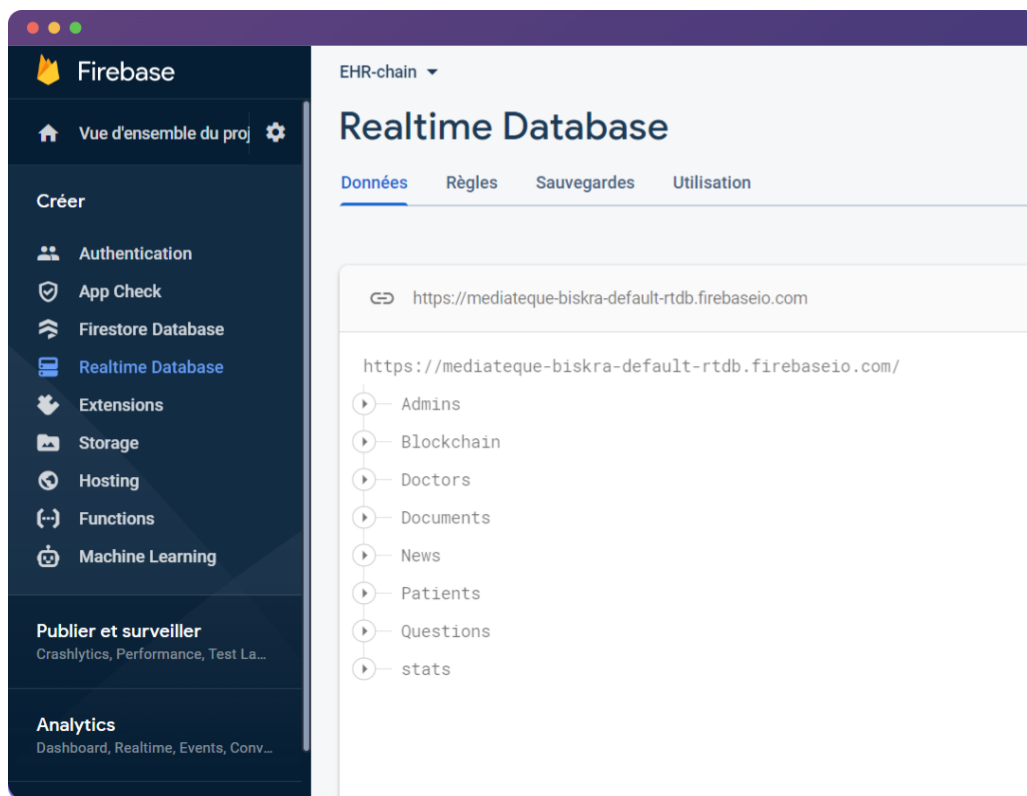


Figure 4.9: Realtime database

- **Cloud Storage:** is a powerful, simple, and cost-effective object storage service built for Google scale. The Firebase SDKs for Cloud Storage add Google security to file uploads and downloads for your Firebase apps, regardless of network quality.

4.4 Implementation and realization of the system

This section of the chapter provides a detailed description of our EHR system, complete with screenshots of its various web pages.

4.4.1 System Description

Our system aims to securely store and share electronic health records in order to manage health data. It also allows other doctors (general practitioners, specialists, or hospitals) to provide healthcare information (medical history, results of blood tests, laboratory, imaging, ongoing treatment, etc.) to a doctor by defining an electronic health record for each patient. In this way, communication between various health professionals (doctor, etc.) involved with the patient is facilitated and done safely. The Electronic Health Record secure shared system is what we're talking about here. The system logo is shown in Figure 4.10.

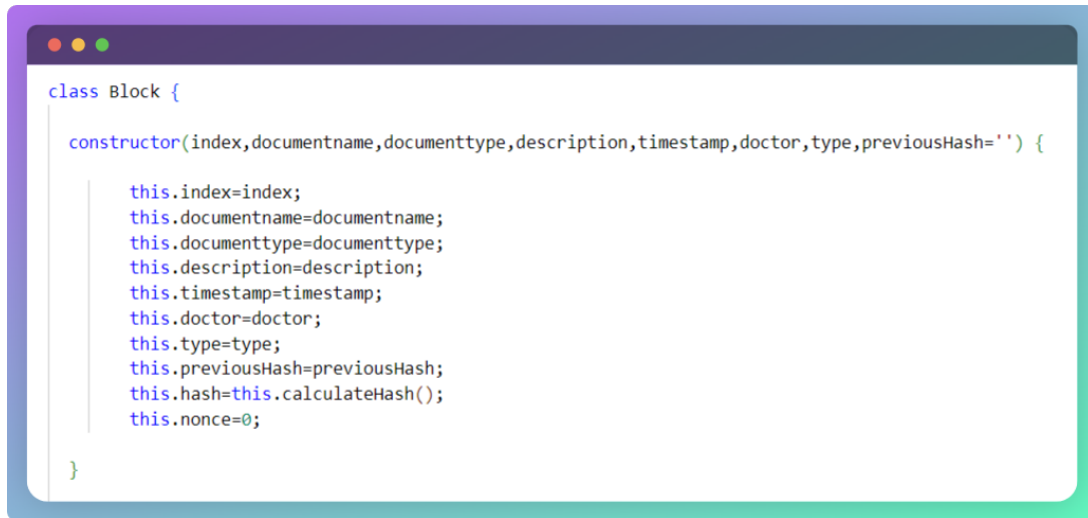


Figure 4.10: EHR System logo

In fact, the EHR system is patient-centric, with the patient at the center of the health-care circle at all times; the Medical Staff, on the other hand, is made up of various health professionals (doctor, pharmacist, laboratory, and so on) who are involved with this patient. Of course, the system is overseen by an administrator with specific responsibilities. The tasks associated with each of them are detailed below.

When a patient is added to a health professional's patient list, he can create a health record, and other health care professionals can access his records by adding him to their patient list as well.

Initially, when the health record is created, it will contain the first block of the chain named "GenesisBlock", Figure 4.11 gives an overview of this block.



```
class Block {  
  constructor(index,documentname,documenttype,description,timestamp,doctor,type,previousHash='') {  
    this.index=index;  
    this.documentname=documentname;  
    this.documenttype=documenttype;  
    this.description=description;  
    this.timestamp=timestamp;  
    this.doctor=doctor;  
    this.type=type;  
    this.previousHash=previousHash;  
    this.hash=this.calculateHash();  
    this.nonce=0;  
  }  
}
```

Figure 4.11: The Genesis block

In this case, what does a Block mean?

- **Block** is a space in a blockchain where a block is defined as a unit containing information from each consultation.
- **Index** is the number of block
- **DocumentName, DocumentType**, to define the type of the document added (created) during the consultation, its type: prescription, X-ray, analysis, etc...
- **Description** Comments added by the Doctors.
- **Doctor and type** define the name and specialty of each Doctor : pediatrician, dental, pharmacist, etc...
- **Timestamp** is a small data stored in each block as a unique serial and whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network.
- **PreviousHash** sets the previous block's hash. The "genesis Block's" previous hash is 0.
- **Hash** is the hash of the current block. In other words, the hash of all the information present in this block,
- **Nonce** is a number added to a hashed—or encrypted—block in a blockchain that, when rehashed, meets the difficulty level restrictions.

As time goes on, there will be Blocks for every patient's health record. Figure 4.12 represents a block describing a consultation, requiring a prescription, of such a patient by Cardiologist **Dr Okbi Ridha**.

The patient can look up his health records and so see what actions have been taken on his file, but it cannot update or delete health records.



```
{
  index="1";
  documentname="Prescription";
  documenttype="Prescription.pdf";
  description="tablet telmisratan 40mg take on by mouth daily in the morning for blood pressure control ";
  timestamp="07/06/2022 09:10:54";
  doctor="Dr Okbi";
  type="cardiologist";
  previousHash="009f269de13ac286d1c905641c0d27e970104cb71729918d55961a0952229a11";
  hash="00271d313a3c82b62f139d79faf3d3e33565fd9c6566be929b5ecb9f690ffaf0";
  nonce="4";
}
```

Figure 4.12: Block describing a prescription

We usually refer to a health professional as a doctor, a pharmacist, or a laboratory. After creating an account in the system, he can access the patient's health record.

A health professional can easily access the patient's file. So he can see all of his patient's information and data, and he can add new medical files but not delete or edit old ones.

When a patient makes an appointment with a healthcare provider. During the consultation, the expert adding a new health record to the patient's file, such as a prescription. To begin, the EHR system ensures that the blockchain has not been tampered with or altered. In other words, the system verifies the blockchain's integrity (Figure 4.13).

```
isChainValid()
{
  for(let i =1;i< this.chain.length;i++)
  {
    const currentBlock = this.chain[i];
    const previousBlock = this.chain[i-1];

    if(currentBlock.hash !== currentBlock.calculateHash())
    {
      return false;
    }
    if(currentBlock.previousHash !== previousBlock.hash)
    {
      return false;
    }
  }
  return true;
}
```

Figure 4.13: check validity algorithm

In the event of pirating or changing a user’s chain, the system will discover this violation because the record is stored on several computers (participants of this health record), so it is easy to handle this problem. As a result, the patient’s record is always protected from penetration or modification.

4.4.2 Mining algorithm

The system calculates the hash of this document using the "Sha256" function after checking the blockchain validity, and creates a new block containing the hash of this document as well as other related information such as the document name, type, consultation date, and also the hash of the previous block. After creating the block, the system validates it using the mining algorithm (see Figure 4.14). Once the block has been authenticated, the system adds it to the chain of all medical staff who have access to this health record.

The process of mining involves the solving of a mathematical problem. The block is validated as a result of the resolution. The mathematical difficulty we present is that a block’s hash must start with two consecutive zeros.

```
proof_of_work(difficulty)
{
  while(this.hash.substring(0,difficulty) !== Array(difficulty+1).join("0"))
  {
    this.nonce++;
    this.hash=this.calculateHash();
  }
}
```

Figure 4.14: Mining algorithm (proof of work)

4.5 System Interface

This part allows you to have an overview of our EHR system, where we are going to show its main web pages (screenshots), starting with the home page.

4.5.1 Home page

The home page (Figure 4.15) of our EHR is where you can identify yourself as a doctor, a patient, or an administrator.

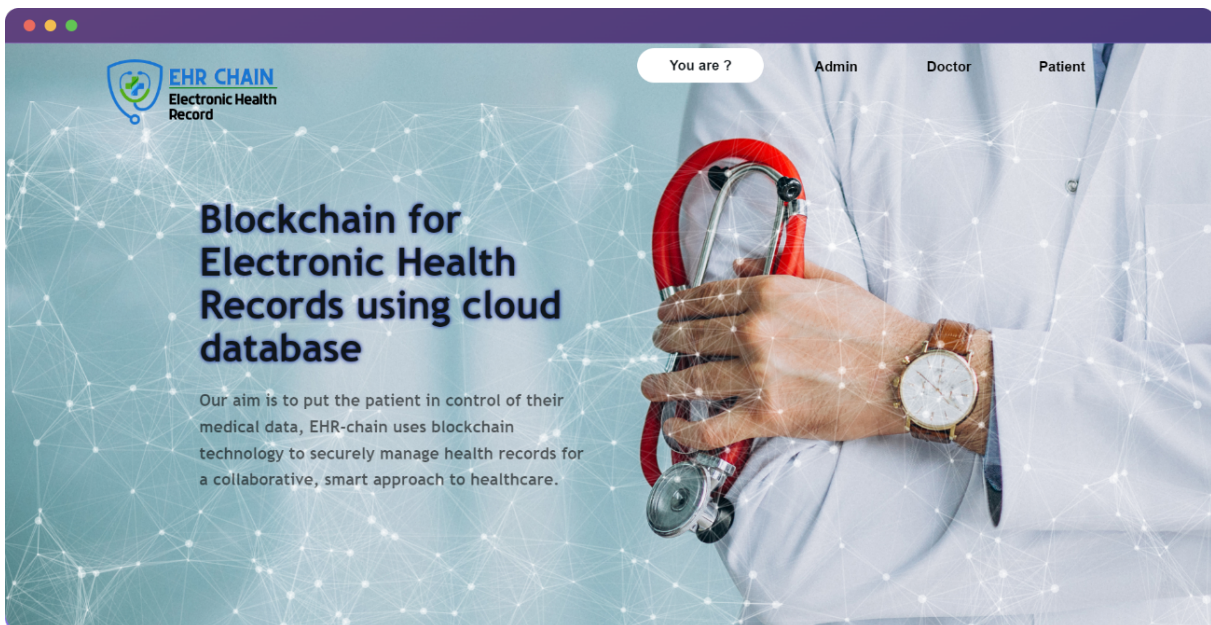


Figure 4.15: Home page

4.5.2 Access as a Patient

When you identify yourself as a patient, login to your EHR, of course, if you are already registered. Once you have connected to your EHR (through the patient button, with your username and your password) you access the patient profile.

As a patient, you can consult the list of your health record: prescription, X-ray, analysis, etc., as shown in Figure 4.16.

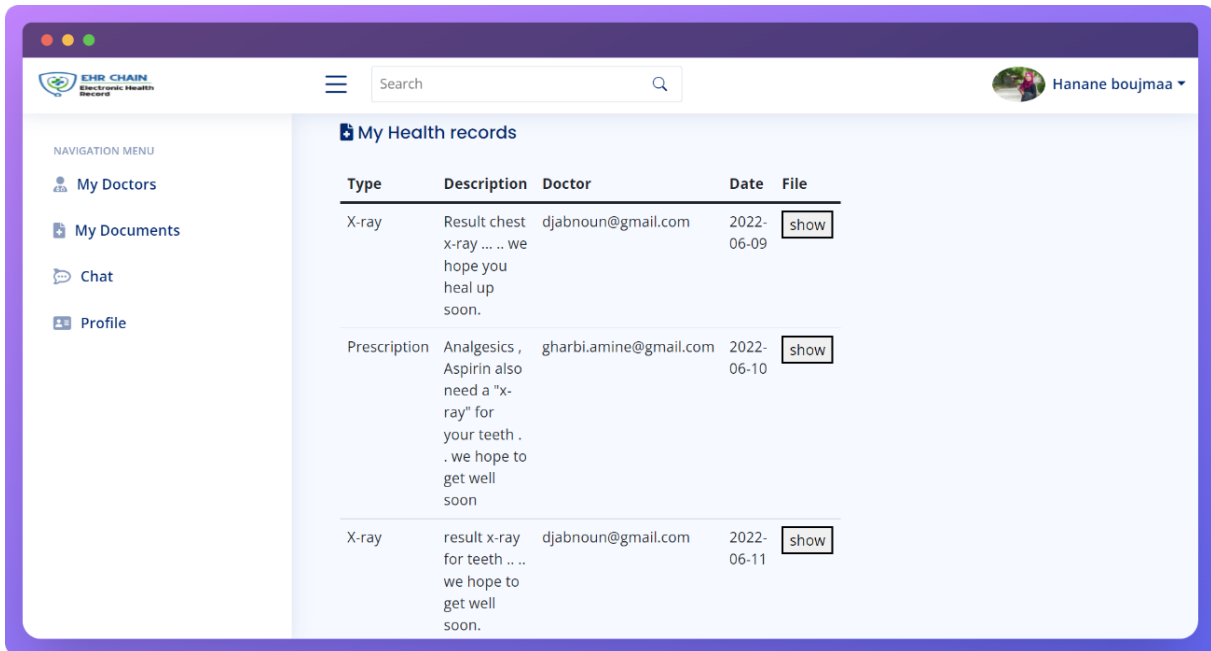


Figure 4.16: List of My health records "Patient Profile"

By clicking on one of your records (show file), for example "prescription", a page selected document is displayed, see Figure 4.17.

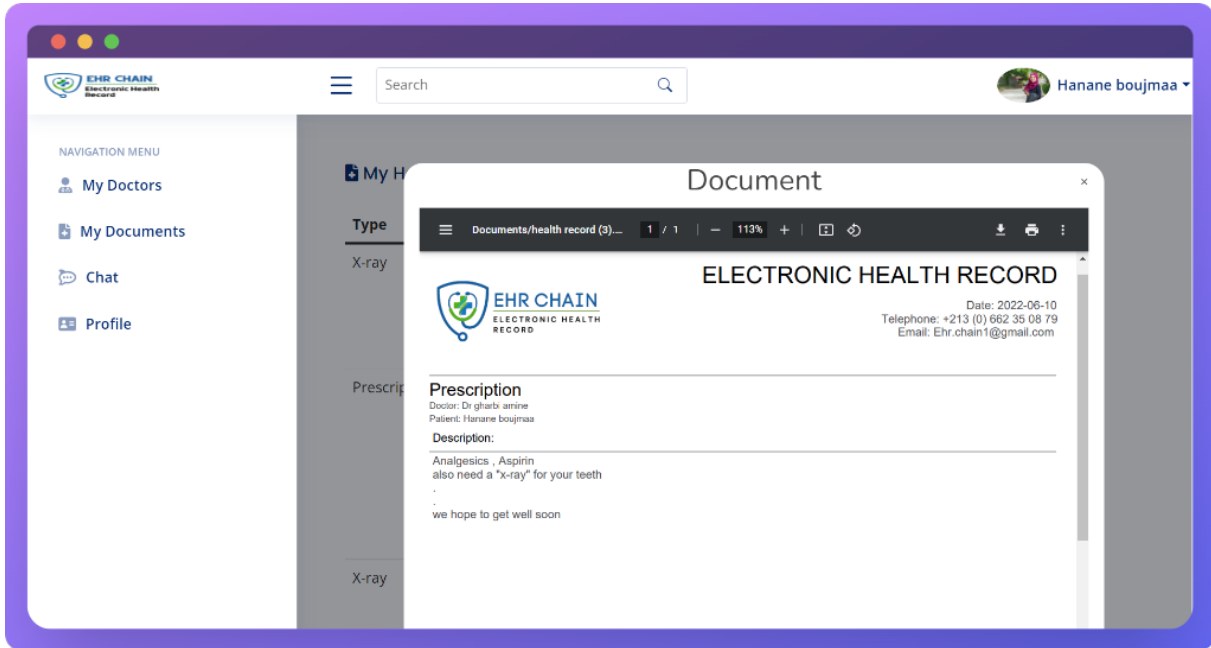


Figure 4.17: Health record represents a "prescription"

Each record is defined by: the Doctor who creates it and his specialty, the date of creation, description if any, and the document oneself.

You can also display your healthcare professionals (Figure 4.18).

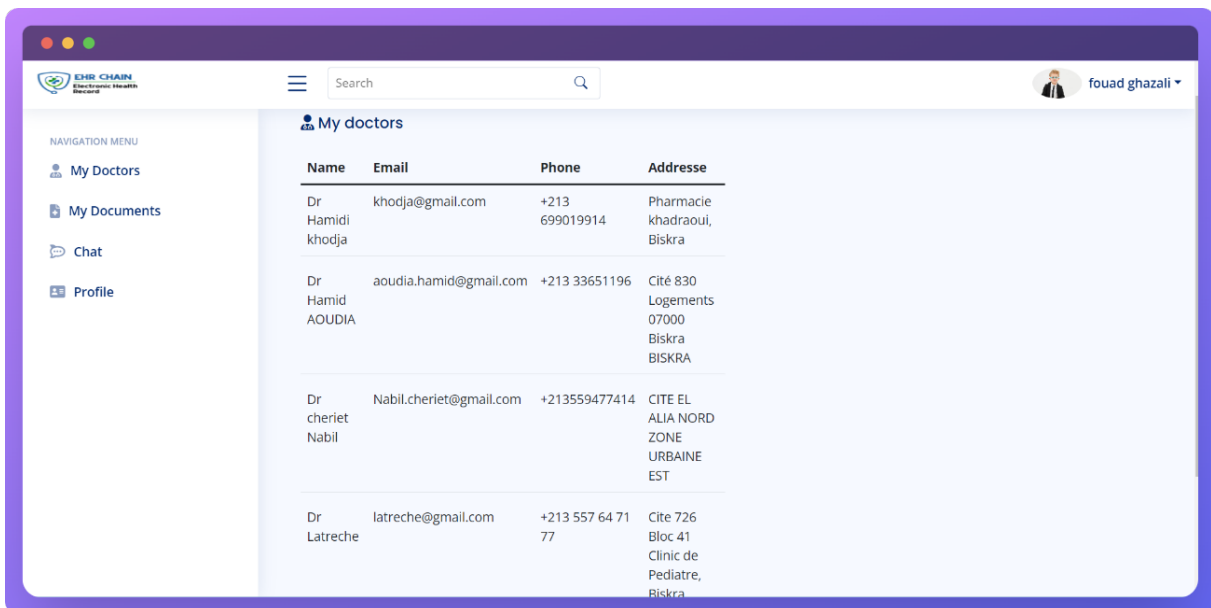


Figure 4.18: List of my doctors

Finally, you can access your profile, here the system gives you the hand to modify them if you want, but you can't change your insurance number (Figure 4.19).

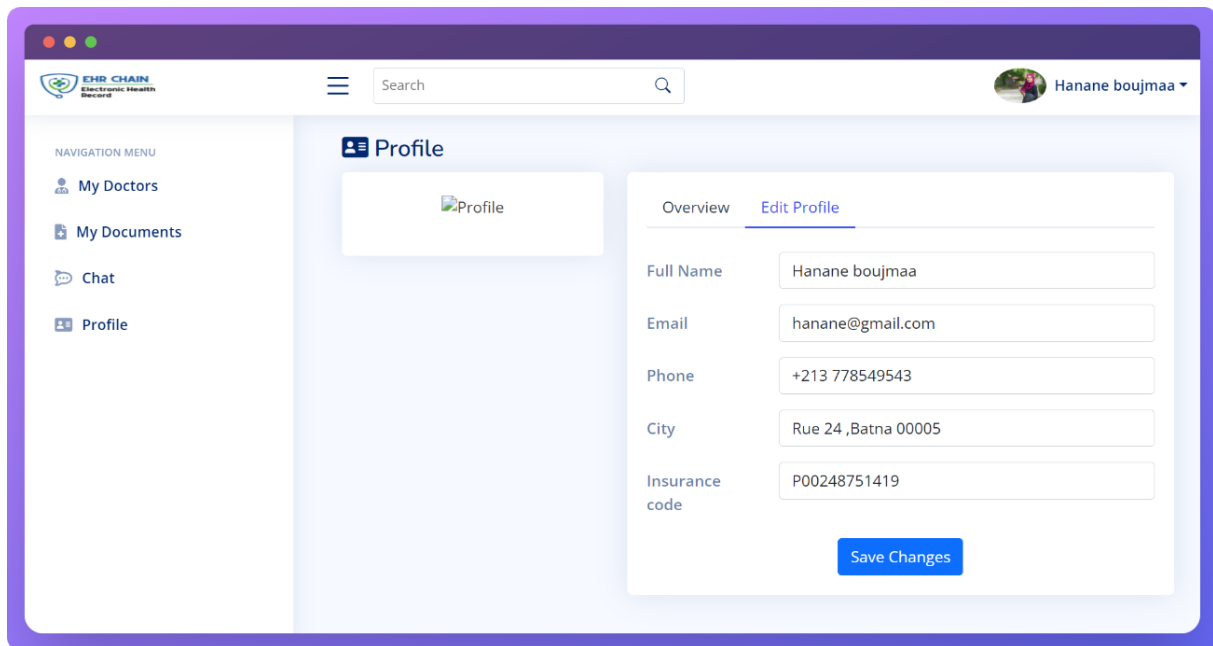
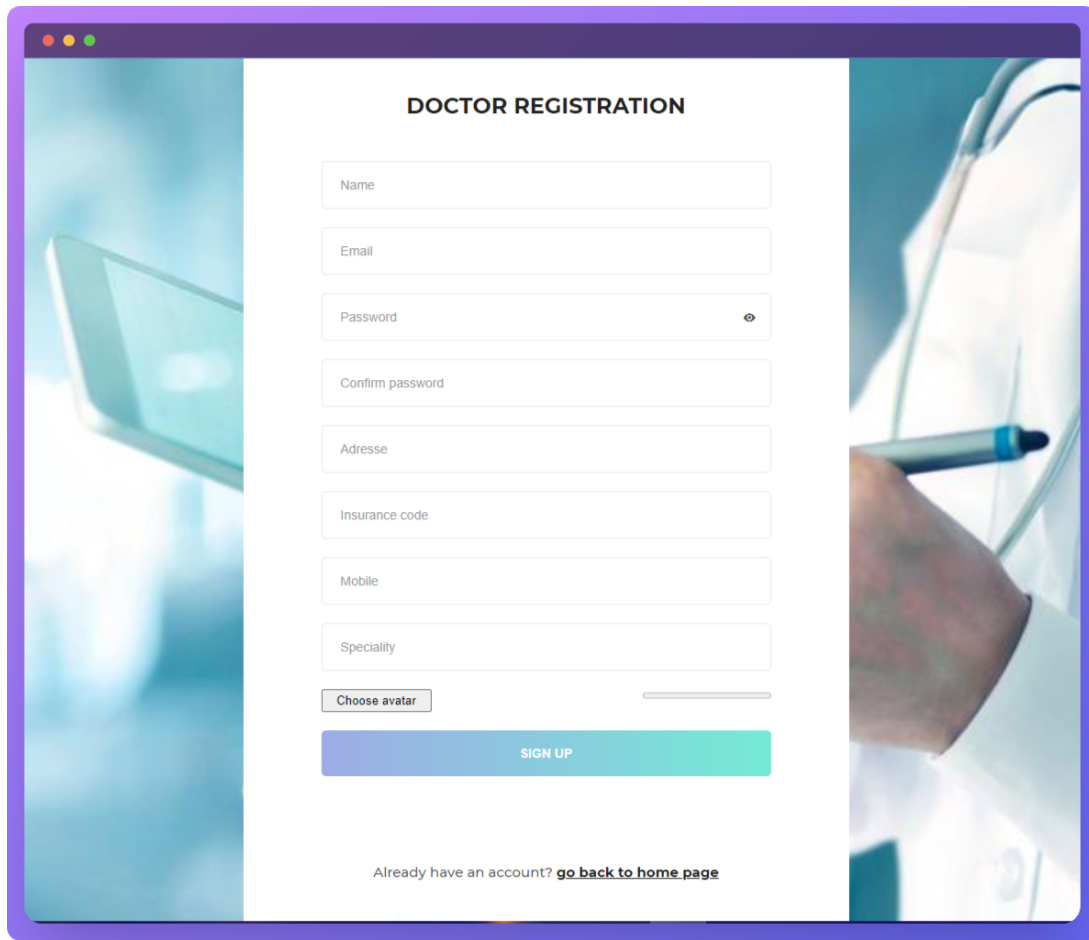


Figure 4.19: Edit profile (patient profile)

4.5.3 Access as a health professional or doctor

When you identify yourself as a healthcare professional, you will have two options:

- Once you already have an account, and in this case, you can Login to your account.
- Or you do not have an account, therefore you must choose the 'Register' option. Here you come to a registration form (Figure 4.20).



The image shows a web browser window with a registration form titled "DOCTOR REGISTRATION". The form is centered on a white background with a light blue border. It contains several input fields: "Name", "Email", "Password" (with a toggle for visibility), "Confirm password", "Adresse", "Insurance code", "Mobile", and "Speciality". Below these fields is a "Choose avatar" button with a horizontal line to its right. A large, rounded "SIGN UP" button is positioned below the "Choose avatar" button. At the bottom of the form, there is a link: "Already have an account? [go back to home page](#)". The background of the browser window is a blurred image of a doctor in a white coat holding a stethoscope and a pen.

Figure 4.20: Register form

It should be noted that such a process requires an insurance code to ensure that you are a real health professional. Your email address must be correct then your account is created. You are then automatically redirected to the professional health profile.

- So, you access to the dashboard (Figure 4.21) of doctor and see some statistics like number of : doctors, patients, documents in the system and a box that displays the recent activities.

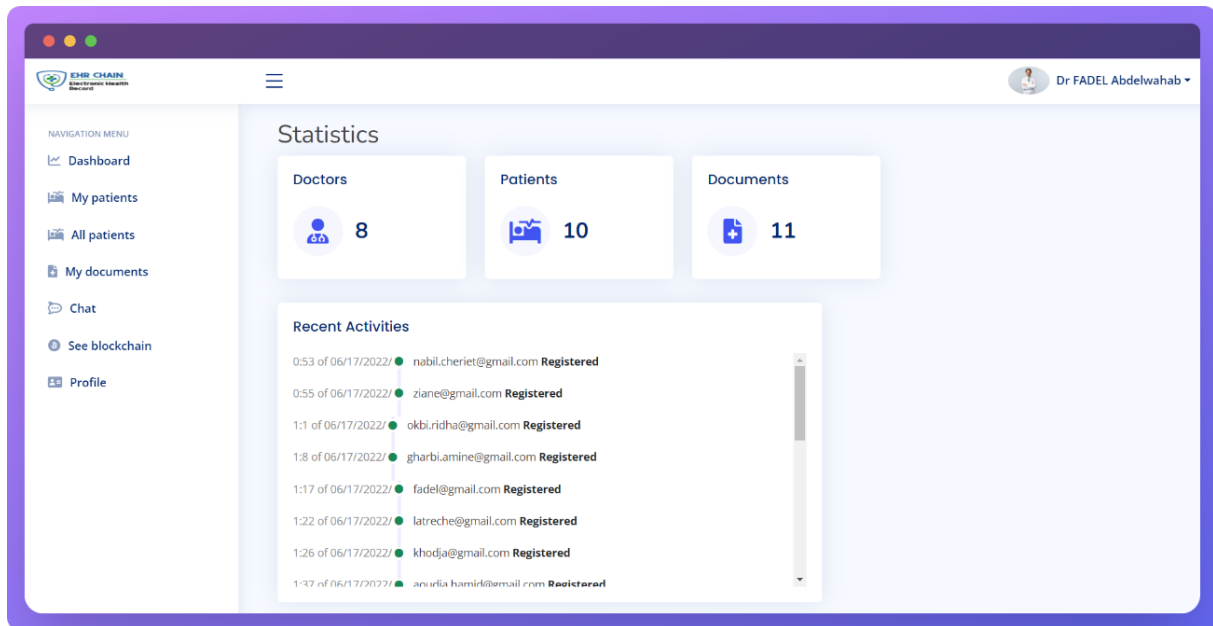


Figure 4.21: Dashboard doctor

- then can you access to the list of all patients, see Figure 4.22. You may add patients to your patient list or remove patients from your list using this list.

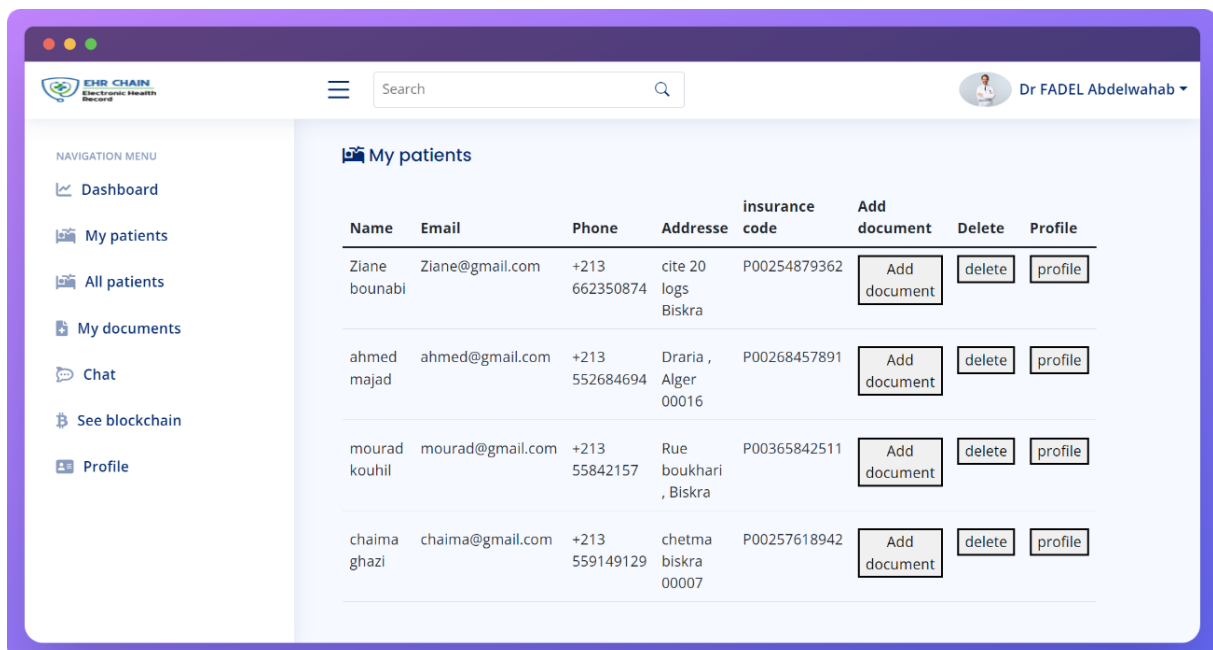


Figure 4.22: List of my patients

- You may also create an EHR for a new patient who doesn't have one by selecting the patient (Add document), then creating a new document(record) by filing the form (Figure 4.23) next press the "Generate Pdf" button to upload the record format Pdf or upload an X-ray, Analysis...etc.

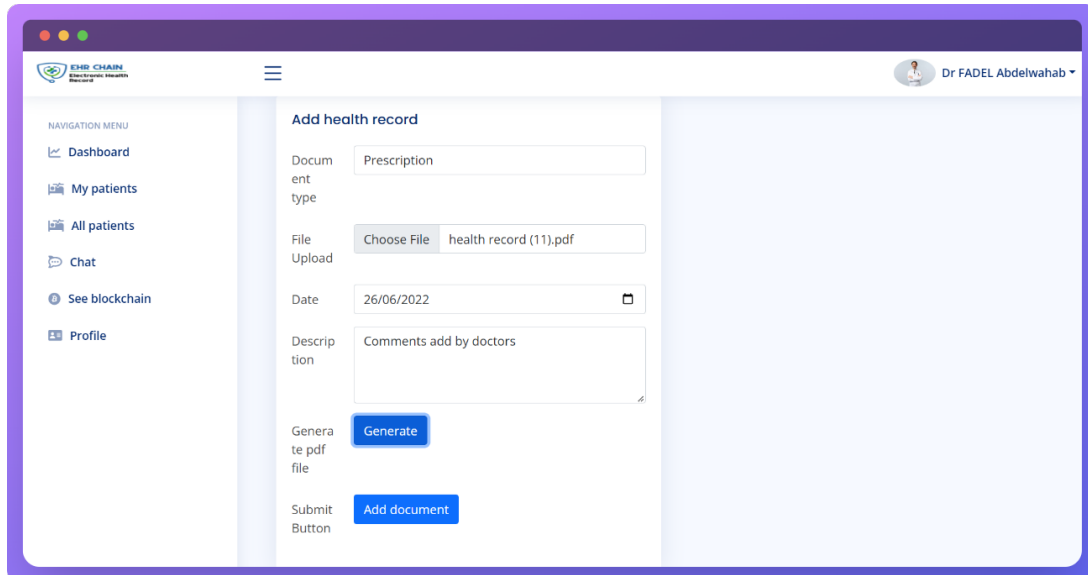


Figure 4.23: Add a new record

- In order to access the EHR of such a patient, you must first access the "My patients list" then press on the "profile" button corresponding to this patient. In this case, you can see the list of his documents also, if you need to display the record press "show file" button (Figure 4.24).

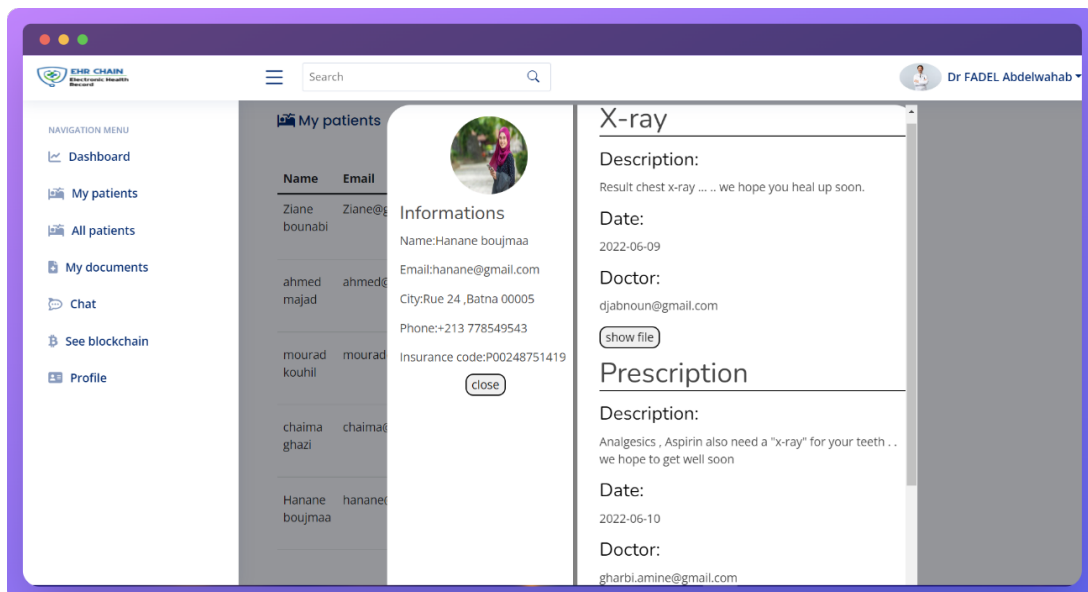


Figure 4.24: List of patient documents

- You may also check the blockchain list for any patient who has a health record in the system (see Figure 4.25).

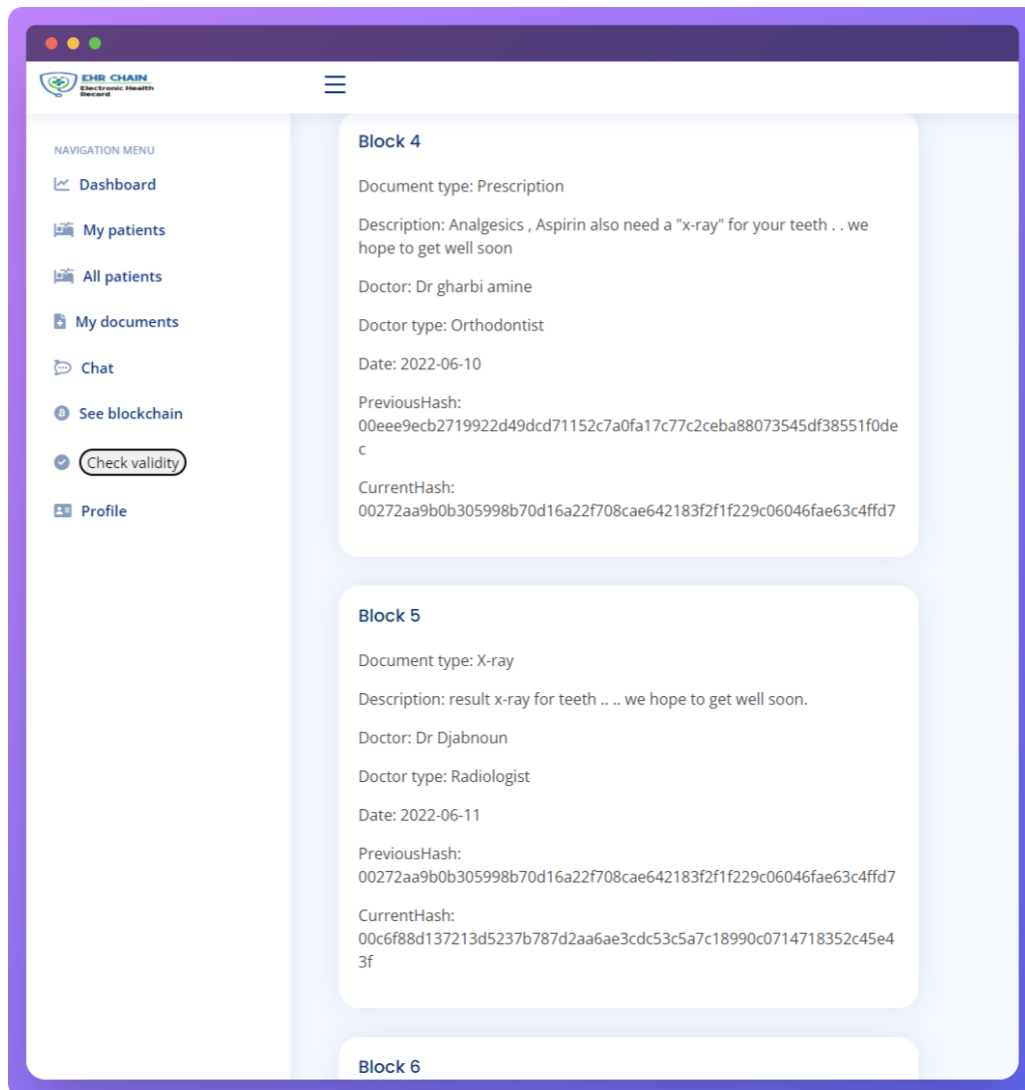


Figure 4.25: Blockchain

4.5.4 Access as an administrator

Finally, as an administrator, you may see your system as follows:

- Have the list of all patients (Figure 4.26), as well as their health records.

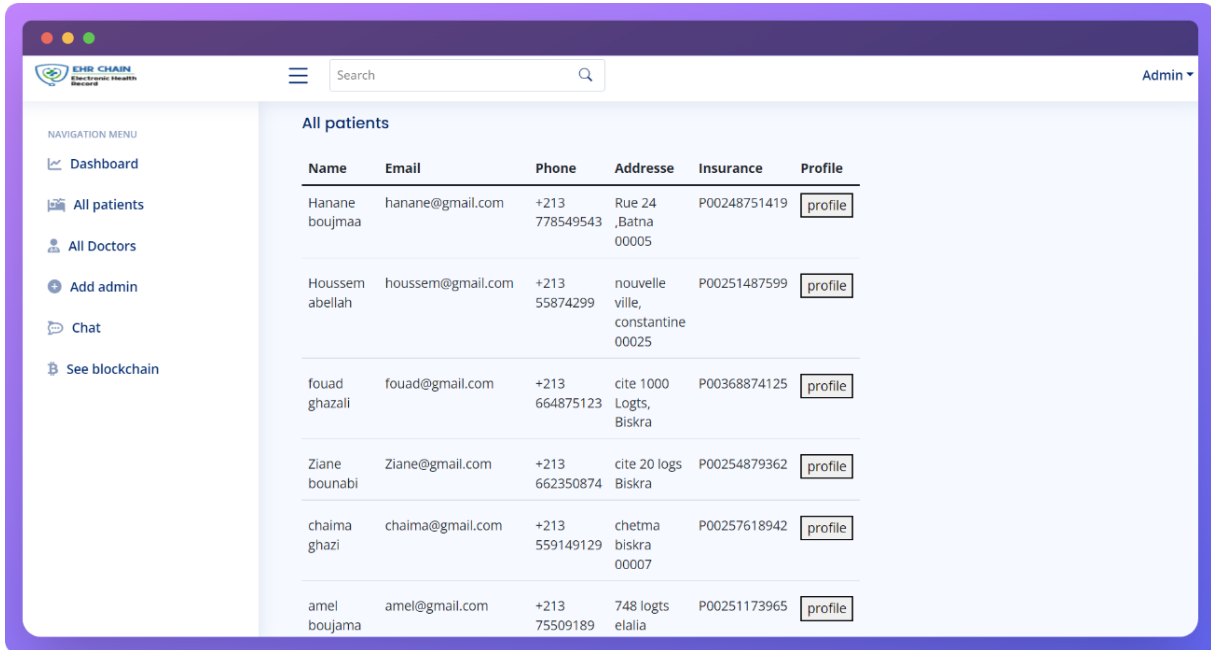


Figure 4.26: List of all patients

- Have access to a list of all doctors (Figure 4.27), which you can delete anyone.

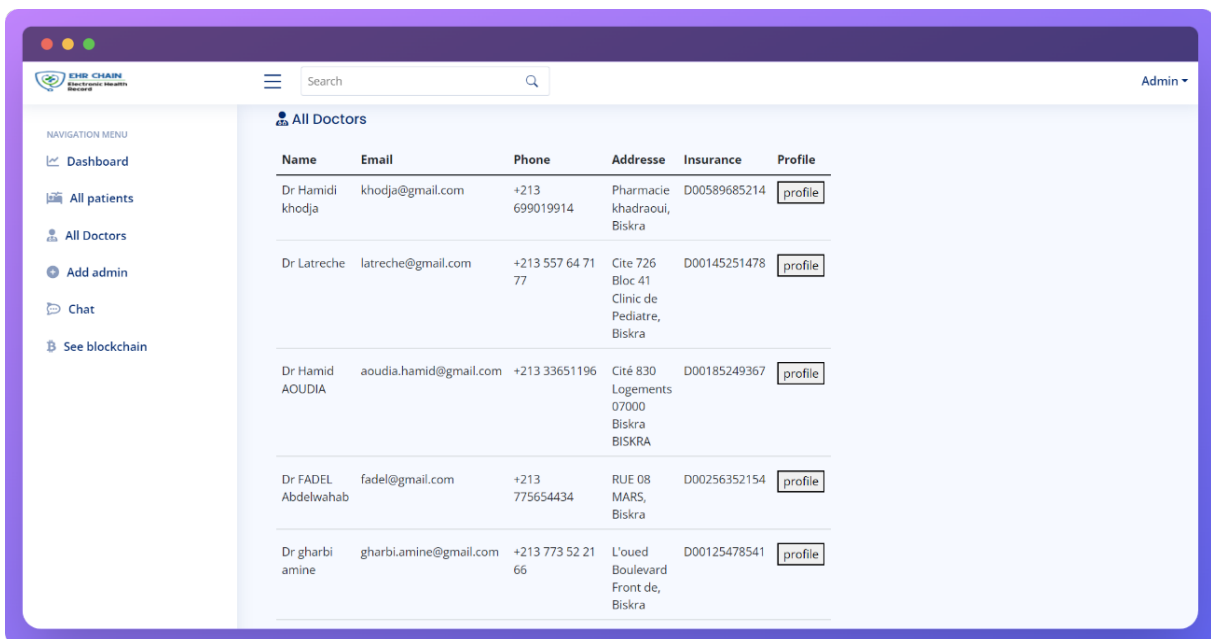


Figure 4.27: List of all doctors

You may also add a new administrator and view or change your information (Figure 4.28).

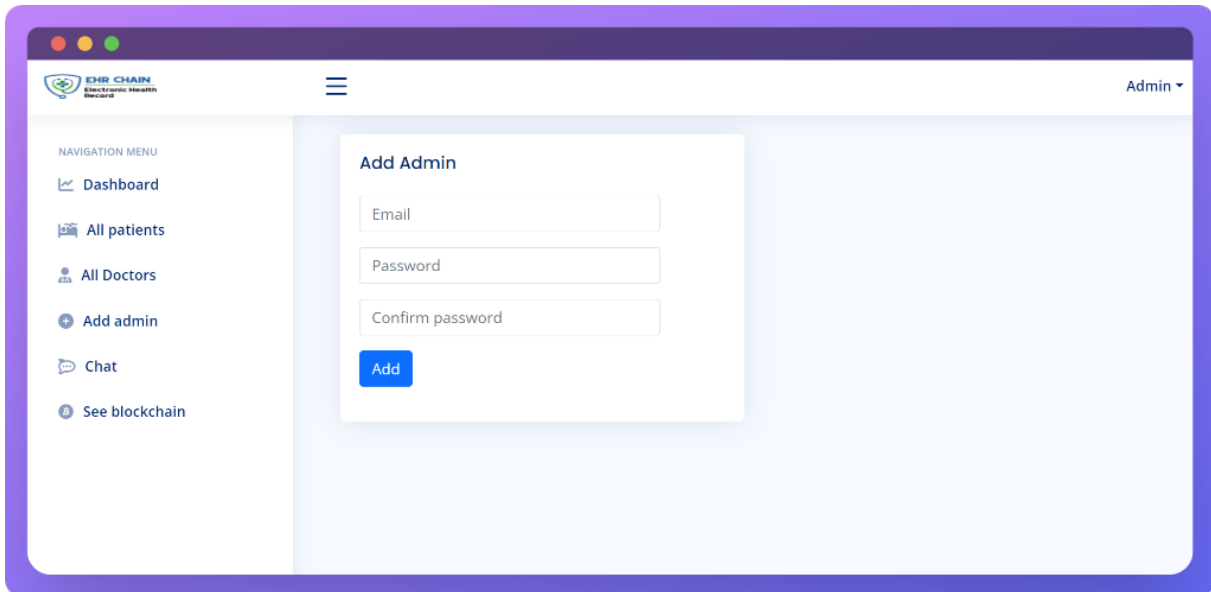


Figure 4.28: Add a new admin

We also added the feature of communication "chat" (ask question, need help ... etc.) between all actors of the system and identified each one in a custom text color, for example: admins with red color, patient with blue color and doctors with black color as shown in (Figure 4.29).

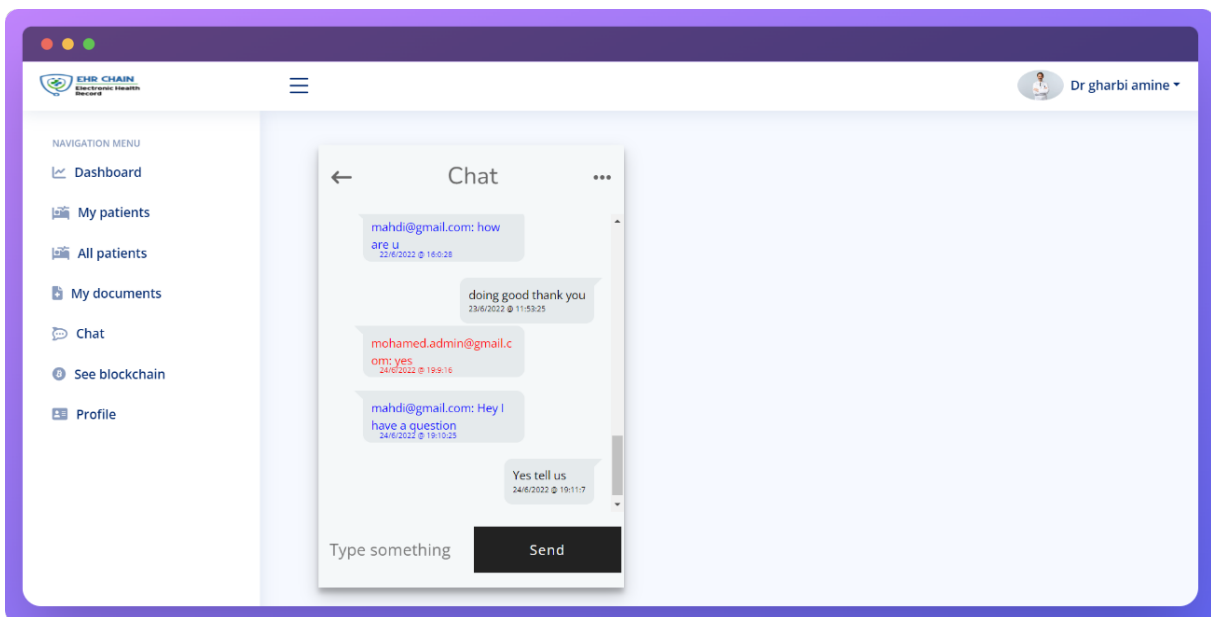


Figure 4.29: Chat page

4.6 Conclusion

The implementation process of our system is the most crucial. We presented the development tools we utilized in this chapter, along with a highly extensive description of the completed system, in which we discussed the major interactions that can occur throughout the EHR system's operation.

General Conclusion

The use of blockchain in healthcare systems plays a critical role in the current healthcare market. It can result in automated data collection and verification processes, correct and aggregated data from various sources which are immutable, tamper resistant and provide secured data, with reduced probability of cyber crime.

Blockchain technology has potential applications to some challenges faced by the healthcare industry. The strongest potential of blockchain technology in the healthcare arena is its heavily researched applications, namely: security, integrity, decentralized nature, availability, and authentication principles due to the general ledger and block related infrastructure.

In this thesis, we presented the design of our system allowing the secure sharing of health data which, in fact, was a difficult subject for a long time because it lacked trust and therefore security. In fact, most of the data are stored in different medical institutions, which leads to their dispersion. And this makes it difficult for patients to acquire all their medical records from the various medical institutions they have visited. For this reason, the storage, sharing and application of medical data is essential in cases where security and confidentiality are guaranteed.

As a result, we've proposed our EHR system, which is built on the Blockchain, for managing health data by storing, and sharing electronic health records securely. It also allows doctors to get health information from other health professionals, for example, by creating a health record for each patient. Also, we can even cite one of the strong aspects of the EHR system :

For a patient, this means that he can securely access his health information at any time and from any location, with no risk of lost or misplaced X-rays, scans, analysis, prescription...etc. The doctor will have access to all the patient's documents and health record.

For the healthcare professional, can easily and quickly access his patient's electronic health record (EHR) at any time and from anywhere. It can also discover all of a patient's medical history. The EHR system makes it possible to avoid prescribing tests or treatments already requested, in addition to avoiding drug interactions.

Future Work

Current work has primarily aims to manage medical data using electronic health record. We tried to suggest a potential solution using blockchain technology as a distributed network and a cloud database. There are several parts of this work that may be added or improved for future work, as listed below:

- We plan to implement the payment module in the existing solution. For this we need to have certain considerations as we need to decide how much a patient would pay for consultation by the doctor on this decentralized system functioning on the blockchain. We would also need to define certain policies and rules that comply with the principles of the healthcare sector.
- Set up a medical Blockchain network linking as many establishments of medical and healthcare as possible.
- Implemented our application on other platforms that can be replaced with some changes, including Ethereum, Hyperledger and Corda. Creating the same application over other platforms allows us to compare the efficiency of these platforms.
- Coupling of this project with the Big Data model.

These additional topics require further research.

Bibliography

- [1] Tiana Laurence. *Introduction to blockchain technology*. Van Haren, 2019.
- [2] N. REIFF. *Introduction a la blockchain explained*. <https://www.investopedia.com/terms/b/blockchain.asp>. ,Accessed:Feb 25, 2022).
- [3] J Michael, ALAN Cohn, and Jared R Butcher. “Blockchain technology”. In: *The Journal* 1.7 (2018).
- [4] Arshdeep Bahga and Vijay K Madiseti. “Blockchain platform for industrial internet of things”. In: *Journal of Software Engineering and Applications* 9.10 (2016), pp. 533–546.
- [5] Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid. “Using blockchain for electronic health records”. In: *IEEE Access* 7 (2019), pp. 147782–147795.
- [6] *history of blockchain*. <https://www.javatpoint.com/history-of-blockchain>. Accessed: 2021-12-10.
- [7] *history of blockchain*. <https://academy.binance.com/en/articles/history-of-blockchain>. Published Dec 6, 2018 ,Accessed: 2021-12-10.
- [8] Marion PIGNEL and Denis STOKKINK. *LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale?* 2019.
- [9] *Peer to peer network*. <https://www.vocal.com/video/p2p-network/>. Accessed: 2021-12-11.
- [10] Claire Fénéron Plisson. “La blockchain, un bouleversement économique, juridique voire sociétal”. In: *I2D Information, donnees documents* 54.3 (2017), pp. 20–22.
- [11] K Hemalatha, K Hema, and V Deepika. “Utilization of blockchain technology to overthrow the challenges in healthcare industry”. In: *Emerging Research in Data Engineering Systems and Computer Communications*. Springer, 2020, pp. 199–208.

- [12] Joao Sousa, Alysson Bessani, and Marko Vukolic. “A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform”. In: *2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN)*. IEEE. 2018, pp. 51–58.
- [13] Xiwei Xu, Ingo Weber, and Mark Staples. *Architecture for blockchain applications*. Springer, 2019.
- [14] Binance academy. *What Is a Blockchain Consensus Algorithm?* <https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm/>. ,Accessed:Mar 25, 2022).
- [15] IAB ThCH LAB. *Overview of 9 blockchain consensus algorithms*. <https://iabtechlab.com/wp-content/uploads/2018/07/Blockchain-Technology-Primer.pdf>. Published july, 2018 ,Accessed: 2021-12-15.
- [16] Sirine HAMLAOUI. “Blockchain for The Drug Supply Chain Management”. In: (2020).
- [17] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: *Decentralized Business Review* (2008), p. 21260.
- [18] Pranav Kumar Singh et al. “Managing smart home appliances with proof of authority and blockchain”. In: *International conference on innovations for community services*. Springer. 2019, pp. 221–232.
- [19] Jerome Kehrli. “Blockchain explained”. In: *Netguardians [en lnia].[Data de consulta: 25 de juny de 2017]; https://www.netguardians.ch/news/2016/11/17/blockchain-explained-part-1* (2016).
- [20] Dylan Yaga et al. “Blockchain technology overview”. In: *arXiv preprint arXiv:1906.11078* (2019).
- [21] Anastasios Kalogeropoulos. “A Reference Architecture for Blockchain-based Resource-intensive Computations managed by Smart Contracts”. PhD thesis. Technische Universität München Munich, Germany, 2018.
- [22] N.Szabo. *Smart contracts: Building blocks for digital markets*. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. ,Accessed:Feb 10, 2022).
- [23] Maher Alharby and Aad Van Moorsel. “Blockchain-based smart contracts: A systematic mapping study”. In: *arXiv preprint arXiv:1710.06372* (2017).
- [24] Vincenzo Morabito. “Smart contracts and licensing”. In: *Business Innovation Through Blockchain*. Springer, 2017, pp. 101–124.

- [25] DATAFLAIR TEAM. *Blockchain Cryptography – History — Cryptosystem*. <https://data-flair.training/blogs/blockchain-cryptography/>. ,Accessed:Mar 8, 2022).
- [26] Nikita Storublevtcev. “Cryptography in blockchain”. In: *International Conference on Computational Science and Its Applications*. Springer. 2019, pp. 495–508.
- [27] DATAFLAIR TEAM. *Type of blockchains - decide which one is better for your investment needs*. <https://data-flair.training/blogs/types-of-blockchain/>. ,Accessed:Feb 15, 2022).
- [28] M Niranjnamurthy, BN Nithya, and SJCC Jagannatha. “Analysis of Blockchain technology: pros, cons and SWOT”. In: *Cluster Computing* 22.6 (2019), pp. 14743–14757.
- [29] DATAFLAIR TEAM. *Advantages and Disadvantages Of Blockchain Technology*. <https://data-flair.training/blogs/advantages-and-disadvantages-of-blockchain/>. ,Accessed:Mar 6, 2022).
- [30] Julija Golosova and Andrejs Romanovs. “The advantages and disadvantages of the blockchain technology”. In: *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*. IEEE. 2018, pp. 1–6.
- [31] Blockchaintechnology. *Advantages Disadvantages of Blockchain Technology” 2016*. Available. <https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/>. ,Accessed:Mar 5, 2022).
- [32] e-book. *Blockchain*. <https://www.blockchainexpert.uk/book/blockchain-book.pdf>. ,Accessed:Feb 29, 2022).
- [33] Cointelegraph. *West Virginia Secretary of State Reports Successful Blockchain Voting in 2018 Midterm Elections*. <https://cointelegraph.com/news/west-virginia-secretary-of-state-reports-successful-blockchain-voting-in-2018-midterm-elections>. ,Accessed:Feb 28, 2022).
- [34] Monia Milutinović et al. “Cryptocurrency”. In: - 1 (2018), pp. 105–122.
- [35] T Todorov. “Bitcoin—an innovative payment method with A new type of independent currency”. In: *Trakia Journal of Sciences* 15.1 (2017), pp. 163–166.
- [36] Hyperledge. *Advancing business blockchain adoption through global open source collaboration*. <https://www.hyperledger.org/>. ,Accessed:Mar 02, 2022).
- [37] Christian Cachin et al. “Architecture of the hyperledger blockchain fabric”. In: *Workshop on distributed cryptocurrencies and consensus ledgers*. Vol. 310. 4. Chicago, IL. 2016, pp. 1–4.

- [38] Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.
- [39] Maria Prokofieva, Shah J Miah, et al. “Blockchain in healthcare”. In: *Australasian Journal of Information Systems* 23 (2019).
- [40] Asad Ali Siyal et al. “Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives”. In: *Cryptography* 3.1 (2019), p. 3.
- [41] V Rawal et al. “White paper: blockchain for healthcare an opportunity to address many complex challenges in healthcare”. In: *CitiusTech: Princeton, NJ, USA* (2017).
- [42] Kevin A Clauson et al. “Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An exploration of challenges and opportunities in the health supply chain”. In: *Blockchain in healthcare today* (2018).
- [43] R Mauri. *Blockchain for Fraud Prevention: Industry Use Cases*. <https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/>. July 2017, Accessed: Mar 28, 2022).
- [44] Thomas McGhin et al. “Blockchain in healthcare applications: Research challenges and opportunities”. In: *Journal of Network and Computer Applications* 135 (2019), pp. 62–75.
- [45] Liam Bell et al. “Applications of blockchain within healthcare”. In: *Blockchain in healthcare today* (2018).
- [46] Mohsen Attaran. “Blockchain technology in healthcare: Challenges and opportunities”. In: *International Journal of Healthcare Management* (2020), pp. 1–14.
- [47] *Blockchain and healthcare—drug traceability and data management*. <https://medium.com/@juraprotocol/blockchain-healthcare-drug-traceability-data-management-traceability-259dd7c79c24>. , Accessed: Mar 11, 2022).
- [48] Sudeep Tanwar, Karan Parekh, and Richard Evans. “Blockchain-based electronic healthcare record system for healthcare 4.0 applications”. In: *Journal of Information Security and Applications* 50 (2020), p. 102407.
- [49] Ibrar Yaqoob et al. “Blockchain for healthcare data management: opportunities, challenges, and future recommendations”. In: *Neural Computing and Applications* (2021), pp. 1–16.
- [50] Vincent Renotte. *La Blockchain s’empare de votre dossier médical*. <https://medium.com/@vincent.renotte/la-blockchain-sempare-de-votre-dossier-medical-e8ed834fd338>. , Accessed: Mar 10, 2022).
- [51] S Daley. *Examples of How Blockchain is Reviving Healthcare*. 2019.

- [52] Marr B. *35 Amazing real-world examples of how Blockchain is changing your world. Forbes. 2018 Sep 25.* <https://bernardmarr.com/default.asp?contentID=1302>. ,Accessed:Mar 15, 2022).
- [53] David R Matos et al. “Securing electronic health records in the cloud”. In: *Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems*. 2018, pp. 1–6.
- [54] Alevtina Dubovitskaya et al. “ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care”. In: *Journal of medical Internet research* 22.8 (2020), e13598.
- [55] soni technology. *BLOCKCHAIN DECISION TREE — HOW TO DECIDE WHEN TO USE BLOCKCHAIN*. <http://www.sonitechnology.com/2018/06/blockchain-decision-tree-how-to-decide.html>. ,Accessed:Mar 18, 2022).
- [56] *Documentation for Visual Studio Code*. <https://code.visualstudio.com/docs>. ,Accessed:may 2, 2022).
- [57] *Documentation for Bootstrap*. <https://getbootstrap.com/docs/5.1/getting-started/introduction/>. ,Accessed:May 2, 2022).
- [58] *Documentation for JQuery*. <https://api.jquery.com/>. ,Accessed:May 3, 2022).
- [59] *Documentation for Firebase*. <https://firebase.google.com/>. ,Accessed:May 3, 2022).
- [60] *Documentation for Firebase*. <https://docs.flutter.dev/development/data-and-backend/firebase>. ,Accessed:May 3, 2022).