الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة د.مولاي الطاهر

كلية التكنولوجيا

قسم: الإعلام الآلي

Master's thesis

Specialty: ***Sécurité Informatique et Cryptographie***

Theme

Securing Medical Records using Blockchain Technology

Presented by :

Belhadj Mohamed Ali

Bergui Rachida

Led by :

Mr. Ahmed Chaouki Lokbani

Class of 2022-2023

Dédicaces Belhadj Mohammed Ali

Thank God for giving me the strength and patience to overcome the challenges faced during this journey.

To my whole family,

This project is dedicated to my loving family, whose unwavering support has been my source of inspiration.

To my mentors and teachers, thank you for your guidance and wisdom.

To my friends,

your camaraderie has made this experience memorable. And to all those who believe in the power of education

Dédicace Bergui Rachida

To my dear parents,

I can't possibly describe how much I adore and appreciate you in these few words. However, I really appreciate your unwavering support and significant sacrifices, which have enabled me to successfully navigate all challenges throughout my years of study.

To my dear sisters and brothers,

Thank you for staying with me and your sincere encouragement to me throughout my studies and during difficult times when I needed you most. Thank you for staying by my side.

To my whole family,
For their continued support, great confidence in my abilities, love and great appreciation for me, I present them this work and I hope to repay them one day.

To all my friends, and to all my relatives,
For their help and moral support during the development of my graduation project.

To Mohamed Ali,
Because you are a hardworking and persevering colleague, as well as to everyone else whose names I have forgotten.

Thanks

It gives me tremendous pleasure to communicate in these few lines my sincere appreciation and affection to everyone I know, both close by and far, as well as to everyone who has helped me succeed.

First of all,I would like to express my sincere gratitude to **Mr. Ahmed Chaouki Lokbani** for his guidance, support, seriousness, and compassion, especially for his crucial help during the creation of this work. No student will ever forget what they learned from him, and he will always be imprinted in our memories, in my opinion. He was a superb and respected educator.

Additionally, I would like to acknowledge the honor that the jury members have bestowed upon me by accepting to evaluate my work.

Last but not least, I am happy to fulfill my obligation to express my gratitude and thanks to all of my instructors for the quality instruction they provided me during my studies in order to give me an effective education. I also want to express my gratitude to **Saida University** , especially since it served as a second home for me there for five years, where I made many wonderful memories that I will never forget no matter how much time passes.

Abstract

Electronic health records (EHRs) include crucial and extremely confidential health information that has to be constantly exchanged across peers. Blockchain is a decentralized database that fosters interpersonal trust without the involvement of a third party. To develop dependable and transparent applications, it offers a shared, immutable, and transparent history of all transactions. This presents an exceptional opportunity to create a secure and trustworthy data sharing and management system (DSE) utilizing blockchain. The goal of this project is to suggest a straightforward blockchain-based system for managing medical data.

Keywords : Blockchain, Electronic health record EHR, Healthcare, Smart contracts

Résumé

Les dossiers de santé électroniques (DSE) sont des informations médicales privées critiques et hautement sensibles qui doivent être partagées fréquemment entre pairs.La blockchain est une base de données partagée qui crée la confiance entre les individus sans l'intervention d'un tiers. Elle fournit un historique partagé, immuable et transparent de toutes les transactions pour créer des applications fiables, responsables et transparentes. Cela offre une opportunité unique de développer un système de gestion et de partage de données sécurisé et fiable à l'aide de la blockchain, appelé DSE.L'objectif de ce projet est de proposer un système simple basé sur la blockchain pour la gestion des données médicales.

Mots clés : Blockchain, Dossier de santé électronique (DSE) , Santé, Contrats intelligents

ملخص

تعد سجلات الصحة الإلكترونية ***(EHR)*** حاسمة وحساسة للغاية وتحتاج إلى مشاركة متكررة بين الأقران. البلوكشين هو قاعدة بيانات مشتركة تخلق الثقة بين الأفراد بدون طرف ثالث

يوفر تاريخًا مشتركًا غير قابل للتغيير وشفاف لجميع المعاملات لإنشاء تطبيقات موثوقة وقابلة للمساءلة وشفافة. وهذا يوفر فرصة فريدة لتطوير نظام آمن وموثوق لإدارة ومشاركة البيانات باستخدام التكنولوجيا المبنية على البلوكشين. هدف هذا المشروع هو اقتراح نظام بسيط يعتمد على التكنولوجيا المبنية على البلوكشين لإدارة البيانات الطبية.

كلمات مفتاحية : البلوكشين ، سجل صحي إلكتروني (EHR) ، الرعاية الصحية ، العقود الذكي

Table of Contents

Generale Introduction

Blockchain is a distributed ledger that provides safe and open record-keeping.It was first introduced as the foundational technology for cryptocurrencies like Bitcoin. Each node on the network,which is decentralized, keeps a copy of the full blockchain and this allows it to function. Data immutability, transparency,and resistance to manipulation are all guaranteed by the decentralized structure of the system and cryptographic methods.

There are various advantages to using blockchain technology with electronic medical records.The first benefit is that it offers a distributed and decentralized storage solution,doing away with the requirement for a centralized authority that may be exposed to hacker assaults or data breaches. Additionally,it gives patients and healthcare professionals secure access to and sharing of medical records while preserving their privacy.Last but not least,preset rules and agreements may be automatically and securely carried out thanks to the usage of smart contracts on the blockchain.

In our capstone project,we want to investigate blockchain technology by creating a state-of-the-art on the subject and showing a practical application.We have created a health application that is a prime illustration for this situation.blockchain applications outside of ecurrencies.The memory is structured as follows:

- The first chapter presents in detail the fundamental concepts of the blockchain technology.
- The second chapter presents the applications of blockchain in healthcare and significant research work of systems that use blockchain in the medical field, as well as a summary of the key points cited in each work treated.
- The suggested system's design is presented in the third chapter.
- while its realization and execution are covered in the fourth.

We conclude our thesis with a broad statement.

CHAPTER 1

Technology of Blockchain

Contents

1.1. Introduction

A decentralized and distributed digital ledger called blockchain technology is employed to keep track of transactions among several computers. A blockchain is a collection of computers (referred to as nodes) that each store an exact replica of the ledger. The chain's data blocks are linked together by a cryptographic hash of the preceding block, preventing tampering without being seen. The blockchain is protected by a consensus mechanism that enables everyone to concur on the ledger's current state. When a block of transactions is added to the blockchain, it becomes immutable and cannot be changed. Transactions are verified by a network of nodes.[22]

Numerous sectors, including finance, healthcare, supply chain management, and voting systems, could be completely transformed by blockchain technology. Benefits include improved transaction efficiency, security, and transparency. Additionally, it does away with the need for middlemen, cutting costs and enhancing mutual trust.

Although the technology is still in its infancy, it has already attracted considerable interest from investors, governments, and corporations, and its potential impact on the future is enormous.

1.2. Definition of Blockchain

A blockchain, at its foundation, is a database that stores information across a network of computers. Each block in the chain has a timestamp as well as a unique cryptographic hash that connects it to the preceding block, resulting in a secure and tamper-resistant chain of transactions. Once added to the chain, a block cannot be changed or removed, giving it a secure and transparent record of all transactions.

Blockchain technology, in addition to being immutable and secure, is also decentralized, which means it does not rely on a single point of control or authority. Instead, the blockchain's network of computers collaborates to authenticate and verify transactions, guaranteeing that they are accurate and trustworthy.[19]

1.3. Difference between Blockchain and a Database

1. **Database :**

   Generally a database is a data structure which is used for storing information. It is a organised collection or storage of data which is able to store a new data or access a existing data. The data stored in a database can be organized using a database management system. The database administrator can modify the data stored in the database. A database is implemented using the client-server network architecture.

2. **Blockchain :**

   A blockchain is a growing set of documents called blocks that are connected together via encryption. Each block contains the preceding block's cryptographic hash, a timestamp, and transaction data. By design, data change is not permitted here. It enables decentralized control and reduces the possibility of data tampering by third parties with appropriate system access. Key differences between Blockchain and a Database are:[15]

Database	*Blockchain*
Database uses centralized storage of data.	*Blockchain uses decentralized storage of data.*
Database needs a Database admin or Database administrator to manage the stored data.	*There is no administrator in Blockchain.*
Modifying data requires permission from database admin.	*Modifying data does not require permission. Users have a copy of data and by modifying the copies does not affect the master copy of the data as Blockchain is irresistible to modification of data.*
Centralized databases keep information that is up-to-date at a particular moment.	*Blockchain keeps the present information as well as the past information that has been stored before.*
Centralized databases are used as databases for a really long time and have a good performance record, but are slow for ertain functionalities.	*Blockchain is ideal for transaction platform but it slows down when used as databases specially with large collection of data.*

Figure 1.1: *Difference between Blockchain and a Database [15]*

1.4. History of Blockchain

Since its introduction in 2008 as the underlying technology behind the cryptocurrency Bitcoin, blockchain technology has evolved at a rapid and transformational pace. The following are some significant milestones in the growth of blockchain technology:

In 2008, Satoshi Nakamoto, the anonymous creator of Bitcoin, issued a white paper titled "Bitcoin: A Peer-to-Peer Electronic Currency System."

The first Bitcoin block was mined in 2009, and the first Bitcoin transaction occurred in 2010 between Satoshi Nakamoto and a programmer called Hal Finney.

Alternative cryptocurrencies, or "altcoins," initially appeared in 2011, with Litecoin being the most popular.

Ethereum was created in 2014, allowing the development of decentralized applications (dapps) utilizing smart contracts.

R3, the first enterprise blockchain consortium, was founded in 2015 with the intention of providing blockchain solutions for financial institutions.

In 2017, the price of Bitcoin reached an all-time high of nearly $\$20,000$ drawing widespread attention to cryptocurrencies and blockchain technology.[20]

1.5. Key Features

The key features of blockchain technology include:[23]

1. **Decentralization :** The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework.Instead,a group of nodes maintain network making it decentralized.

2. **Cannot Be Corruption :** Every node on the network has a copy of the digital ledger.To a transaction every node needs to check its validity.If the majority think it's valid,then it's added to the ledger.This promotes transparency and makes it corruption-proof.

3. **Distributed Ledgers :** the ledger on the network is maintained by all other users on the system .This distributed the computational power across the computers to ensure a better outcome .

4. **Enhanced Security :** As it eliminates the needs for central authority ,no one can just simply change any characteristics of the network for their benefit .Also using encryption ensures another layer of security for the system.

5. **Consensus :** Every blockchain thrives because of the consensus algorithms.The architecture is cleverly designed ,and consensus algorithms are at the core of this architecture.Every blockchain has a consensus to help the network make decisions .

6. **Faster Settlement :** Blockchain offers a faster settlement compared to traditional banking systems.This way a user can transfer money relatively faster,which saves a lot of time in the long run.

1.6. Structure of a blockchain

The structure of a blockchain typically consists of the following components:[24]

1.6.1. Node

Nodes are network members whose gadgets enable them to keep track of the distributed ledger and act as communication hubs in a variety of network jobs. When a miner attempts to add a new block of transactions to the blockchain, a block is broadcast to all network nodes.

1.6.2. Transactions

A transaction is a contract or agreement, as well as the transfer of assets between parties. Often, the asset is cash or property. The blockchain network of computers keeps transactional data as a copy, with the storage sometimes referred to as a digital ledger.

1.6.3. Block

A block in a blockchain network is analogous to a link in a chain. Blocks in bitcoin are like records that hold transactions like a record book and are encrypted into a hash tree.

Every day, billions of transactions take place throughout the world. Users must keep track of such transactions, which they accomplish with the use of a block structure. The blockchain's block structure is depicted in the first diagram in this article.

1.6.4. Chain

A chain is a notion in which all blocks in the whole blockchain structure in the globe are connected via a chain. And those blocks are linked using the preceding block hash, indicating a chaining structure.

1.6.5. Miners

Blockchain mining is a procedure that validates each stage of the transaction while all coins are in operation. Miners were people who worked in the mining industry. Blockchain mining is the process of validating each stage of a transaction while using cryptocurrency.

1.6.6. Consensus

A consensus is a fault-tolerant strategy used in computer and blockchain systems to obtain the necessary agreement among distributed processes or

multi-agent systems, such as cryptocurrencies, on a single state of the network. It can be used for record keeping and other purposes.

There are several types of consensus mechanism algorithms, each of which operates on a different set of principles:[24]

1.6.6.1. Proof of Work (PoW)

Markus Jakobsson and Ari Juels created the term "proof of work" in a paper released in 1999. It has something to do with bitcoin. Proof of Work (PoW) is a technique meant to make digital transactions safe without the need to trust a third party. This piece expands on prior puzzle solutions. PoW might be used to validate current and historical transactions. Mining is the process through which the labor that goes into solving a problem creates rewards for whoever solves it. In other words, this is frequently an algorithm meant to validate transactions and add new blocks to the blockchain. With Proof of Work, miners compete to be the first to solve a complicated mathematical challenge that will create this new block, which means they'll be able to receive some new Bitcoins as a reward.

Because it is extremely difficult to accomplish work, PoW minimizes the chance of a 51% assault .

No one miner will be able to dominate the Bitcoin network. Hashcash PoW system is used.

Before proposing a new block, miners must provide confirmation that they have completed some work. At the same time, each solution is simple for the community to validate. This makes it simple to verify the legitimacy of all transactions. PoW also limits the number of new data blocks that may be produced. Miners, for example, can only generate a Bitcoin (BTC) block every 10 minutes.[24]

It is not dependent on a single third-party transactor. This creates a network that is "trustless" and transparent. Monopoly can grow over time.

1.6.6.2. Proof of Stake (PoS)

Proof-of-stake is a consensus process that determines who validates the next block based on how many coins you own, rather than miners solving cryptographic problems using computer power to verify transactions like they do with standard Proof-of-Work. The likelihood of validating a fresh block is governed by a person's stake.[24]

The validator does not get a block reward; instead, they are compensated with network fees.

Peercoin was the first cryptocurrency to use a full-fledged PoS consensus process.

Monopoly and Power Consumption.

1.6.6.3. Difference between (PoW) and (PoS)

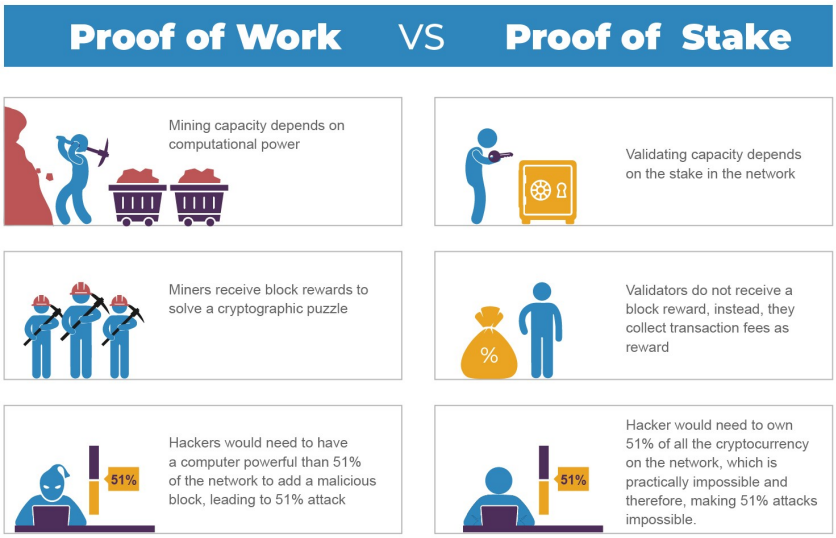

Figure 1.2: *Proof of Work vs Proof of Stake [24]*

1.7. How does Blockchain Work

Blockchain is a digital ledger system that is decentralized and distributed, allowing safe transactions and information sharing between participants without the need for a central authority or intermediary [7].Here's a quick rundown of how it works:

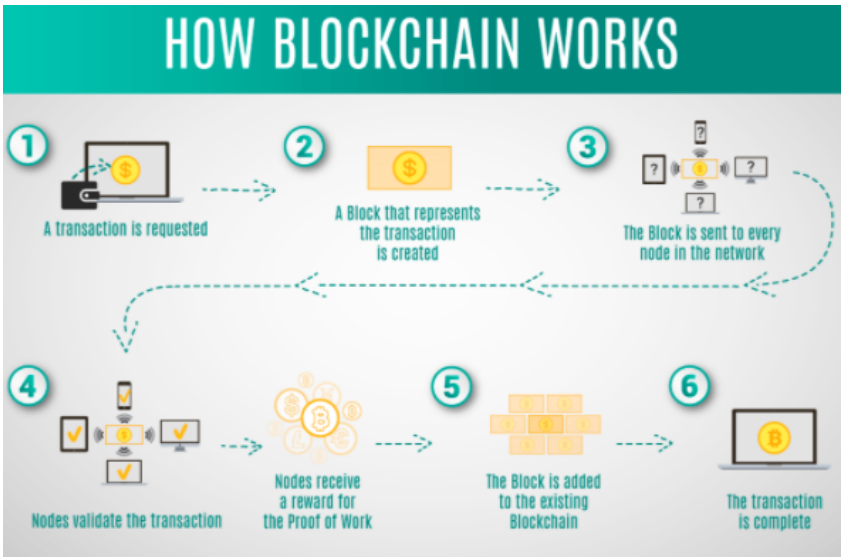

Figure 1.3: *How Blockchain Works [7]*

1.7.1. Transactions

A transaction is started by a user and broadcast to the blockchain's network of nodes (computers).

1.7.2. Verification

Using algorithms and consensus processes, the network of nodes validates the transaction. After validated, the transaction is merged with other transactions to form a block.

1.7.3. Hashing

A block is formed by running transactions through a cryptographic hash function, which creates a unique code known as a hash.

1.7.4. Creating the block

Once the block is formed, it is added to the blockchain, which is a decentralized and distributed public ledger that maintains track of all network transactions.

1.7.5. Validation

The network of nodes validates the new block using consensus processes. Once verified, the block is uploaded to the blockchain and becomes a permanent part of the network.

1.7.6. Security

The decentralized structure of blockchain makes tampering with data on the network exceedingly difficult. Each block contains a reference to the hash of the preceding block, forming a chain.

1.7.7. Decentralization

Because blockchain technology is not centralized, it is more secure and transparent. As a result, it is an excellent choice for applications such as digital money, supply chain management, and voting systems.

1.8. Smart Contracts

1.8.1. Definition

A Smart Contract (or cryptocontract) is a computer software that manages the transfer of digital assets between parties directly and automatically under particular conditions. A smart contract functions similarly to a standard contract while additionally automatically enforcing it. Smart contracts are programs that run precisely how their developers put them up (coded, programmed). Smart contracts are enforceable by code in the same way that regular contracts are[8].

1.8.2. Features

The following are some essential characteristics of a smart contract:

1. **Distributed :** Everyone on the network is guaranteed to have a copy of all the smart contract conditions, and none of the parties can modify them. All nodes linked to the network duplicate and disseminate a smart contract.
2. **Deterministic :** Smart contracts can only perform their intended tasks when the necessary circumstances are satisfied. The end result will be the same regardless of who executes the smart contract.
3. **Immutable :** Once deployed, a smart contract cannot be altered; it can only be withdrawn if the functionality has already been developed.
4. **Trustless :** These are not required by third parties to verify the process's integrity or to ensure that the required criteria are satisfied.
5. **Self-verifying :** These are self-verifying because of automated capabilities.
6. **Self-enforcing :** These are self-enforcing when all of the requirements and regulations are satisfied.

1.8.3. How Do Smart Contracts Work?

A smart contract is just a digital contract with blockchain security code. It has specifics and permissions specified in code that need a particular sequence of events to occur in order to trigger the agreement of the smart contract's conditions. It may also contain time limits, which may result in contract deadlines. Every smart contract has a blockchain address. If the contract has been published on the network, it may be interacted with by using its address[8].

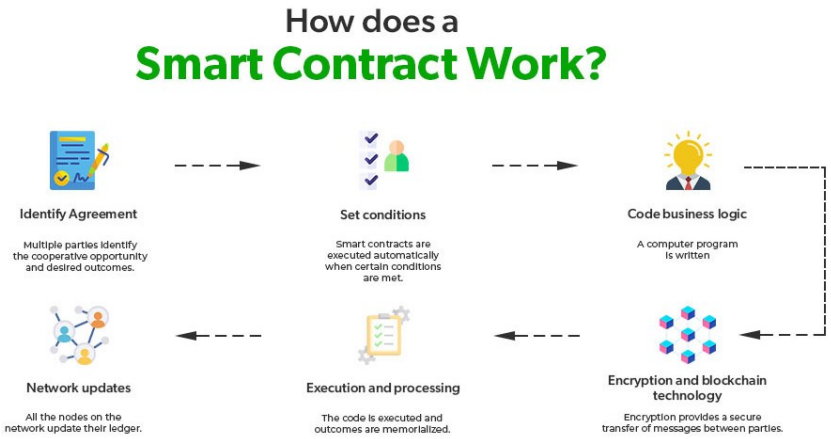

Figure 1.4: *How Smart Contract Works [8]*

- **Agreement Identification :** Multiple parties identify the cooperation potential and intended goals, and agreements may involve business procedures, asset exchanges, and so on.
- **Set conditions :** Smart contracts can be triggered by parties or when particular circumstances are satisfied, such as financial market indices, occurrences such as GPS locations, and so on.

- **Code business logic :** When the conditional parameters are satisfied, a computer program is built that will execute automatically.
- **Blockchain technology and encryption :** Encryption ensures the safe authentication and transport of messages between smart contract participants.
- **Execution and processing :** During blockchain iteration, whenever parties establish agreement on authentication and verification, the code is performed and the results are recorded for compliance and verification.
- **Network updates :** Following the execution of smart contracts, all nodes in the network update their ledger to reflect the new status. Once a record has been posted and validated on the blockchain network, it cannot be changed; it is only in append mode.

1.8.4. Advantages of Smart Contracts

1. **Recordkeeping :** All contract transactions are maintained on the blockchain in chronological order and may be viewed together with the full audit trail. However, the parties engaged can be encrypted for complete secrecy[8].
2. **Autonomy :** Direct transactions occur between parties. Smart contracts eliminate the need for intermediaries and enable transparent, direct interactions with clients.
3. **Reduce fraud :** Detection and reduction of fraudulent behavior. The blockchain is where smart contracts are kept. Forcefully changing the blockchain is extremely difficult due to its computational complexity. A breach of the smart contract can also be detected by network nodes, and such a violation attempt is considered invalid and is not kept in the blockchain.

4. **Fault-tolerance :** Because no one person or entity controls the digital assets, one-party dominance and the circumstance of one part backing out do not occur because the platform is decentralized, and the contract stays intact even if one node detaches itself from the network.

1.8.5. Challenges of Smart Contracts

- **No regulations :** There are no worldwide rules concentrating on blockchain technology (and associated technology such as smart contracts, mining, and use cases such as cryptocurrency), making these technologies difficult to monitor[8].
- **Difficult to implement :** Because smart contracts are still a relatively new idea, study is currently being conducted to properly understand the smart contract and its ramifications.
- **Immutable :** They are basically unchangeable. When a modification must be included into the contract, a new contract must be created and implemented in the blockchain.
- **Alignment :** Smart contracts can accelerate the execution of processes involving numerous parties, regardless of whether the smart contracts are in alignment with all of the parties' intentions and understanding.

1.9. TYPES OF CRYPTOGRAPHY IN BLOCKCHAIN

Cryptography is a technique for protecting data from unwanted access. Cryptography is used in blockchain to safeguard transactions between two nodes in a blockchain network. As previously stated, the two essential ideas in a blockchain are cryptography and hashing. In a P2P network, cryptography is used to encrypt communications, while hashing is used to protect block information and link blocks in a blockchain. The primary goal of cryptography is to ensure the security of participants, transactions, and protections against double-spending. It aids in the security of various transactions on the blockchain network. It assures that only the personnel who are supposed to receive, read, and process the transaction data may do so.[9]

1.9.1. SYMMETRIC-KEY CRYPTOGRAPHY

In this encryption approach, we use a single key. This same key is utilized in both the encryption and decryption processes. Employing a single common key raises the issue of securely passing the key between the sender and the recipient. It's also known as Secret-Key Cryptography. Block ciphers, on the other hand, encrypt one block of information at a time, as the name implies. In this situation, however, the same plaintext block will be repeatedly encrypted to the same ciphertext.[9]

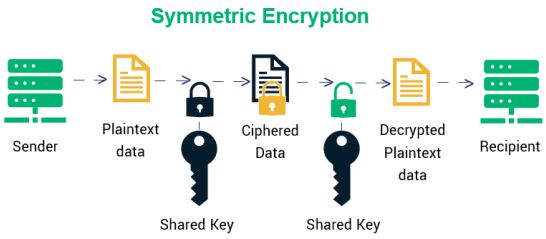

Figure 1.5: *Symmetric-Key Cryptography [9]*

1.9.2. Asymmetric-Key Cryptography

This cryptographic approach employs separate keys for encryption and decryption. This encryption method employs both public and private key techniques. This public key mechanism allows entirely unknown individuals to communicate information such as email addresses. The private key aids in the decryption of communications as well as the verification of digital signatures. The private key cannot be deduced from the public key, but the public key may be derived from the private key, according to the mathematical relationship between the keys. ECC, DSS, and so on are examples.[9]

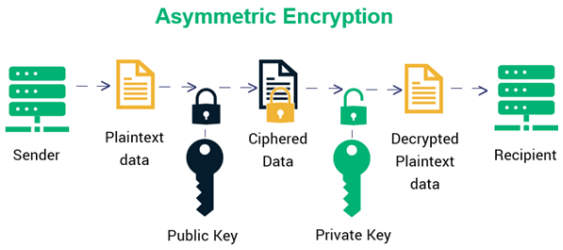

Figure 1.6: *Asymmetric-Key Cryptography [9]*

1.9.3. Hash Functions

Cryptographic hashing is a well-known application of cryptography. Immutability in the blockchain is enabled through hashing. Keys are not used in the encryption of cryptographic hashing. After a transaction is validated, the hash algorithm adds the hash to the block and creates a new unique hash from the original transaction. While hashing continues to combine or create new hashes, the original footprint remains available. The root hash is the single combined hash. The hash function aids in the linking of blocks as well as the integrity of data inside blocks; any changes to the block contents result in a break in the blockchain. MD5 and SHA-1 are two regularly used hashing functions.[11]

1.9.3.1. SHA-256

One of the original and most well-known hashing algorithms is SHA-256, which is utilized in blockchains including Bitcoin, Bitcoin Cash, and Bitcoin SV. In a blockchain, SHA-256 is employed at many stages, most notably:[11]

- **Consensus mechanism:** Miners adjust the nonce value in a bitcoin block until they achieve the hash below the threshold. They then use SHA-256 to determine the hash of new blocks that will be generated. The block can then be approved for entry into the ledger.
- **Block chains:** Each block in the ledger has a SHA-256 hash referencing the block before it in the chain.
- **Digital signatures:** Transactions use digital signatures to maintain integrity, the information used in the transaction is hashed using SHA-256, and then it is encrypted with the sender's private key to generate a signature. The miner then verifies this signature to validate the transaction.

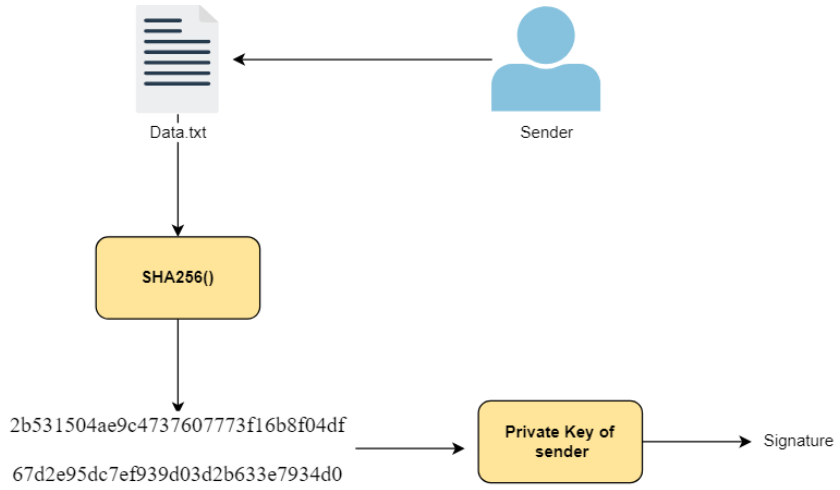

Figure 1.7: *The process of signature generation [11]*

1.10. Evolution of Blockchain Technology

1.10.1. Bitcoin

The first decentralized cryptocurrency's peer-to-peer network eliminates the need for middlemen. In 2008, a person or group of people known as Satoshi Nakamoto established the Bitcoin cryptocurrency. Bitcoin transactions are recorded on the blockchain, a public ledger. There are currently more than 18, as opposed to the existing limit of 21 million Bitcoin tokens in circulation.[10]

1.10.2. Litecoin

Litecoin was created in 2011 by Charlie Lee, a former Google employee. He contributed advancements to Bitcoin technology such as faster transaction speeds, lower fees, and a concentration of miners.

1.10.3. Ethereum

In July 2015, Vitalik Buterin launched Ethereum. Ethereum is now the second-largest cryptocurrency by market capitalization, after only Bitcoin. Ethereum includes its own programming language, Solidity, as well as its own digital money, Ether. (ETH).

1.10.4. Ripple

Ripple: Similar to Litecoin and Bitcoin, Ripple is a cryptocurrency that operates on an open-source, peer-to-peer, decentralized network that allows for simple money transactions in any format. Ripple, a blockchain-based digital payment network and protocol, has its own currency known as XRP.

1.10.5. NEO

Developed in China, NEO, originally known as Antshares, is actively attempting to surpass other prominent cryptocurrency competitors on the worldwide scene. It focuses on smart contracts, also known as digital contracts, which allow users to design and execute contracts without the involvement of a mediator.

1.10.6. IOTA

IOTA is an Internet of Things (IoT) application that was invented in 2016. By 2020, billions of devices would be connected to the internet. In this Internet of Things ecosystem, smart gadgets may transmit data and payment information with a variety of different devices throughout the day. IOTA aspires to become the standard means of conducting transactions on smart devices.

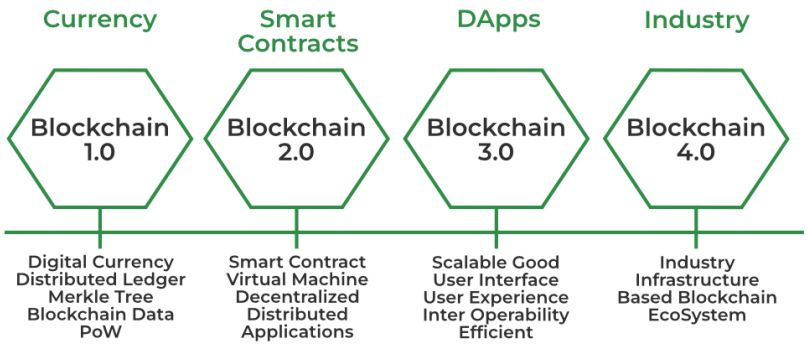

Figure 1.8: *Phases of Evolution of Blockchain [10]*

1.11. Types of blockchain

1.11.1. Public Blockchain

A public blockchain is a decentralized network in which anybody may join and view the blockchain's transactions. There is no centralized authority managing the network, and anybody may host a node and validate transactions. For cryptocurrencies and other decentralized applications that need transparency and open participation, public blockchains are frequently employed.

1.11.2. Private Blockchain

A private blockchain is a network that only authorized users may use to validate transactions and view the blockchain's contents. Participants are frequently identifiable entities, such as corporations or persons, and the network is not open to the public. Businesses routinely use private blockchains to improve the efficiency, security, and transparency of their internal processes.

1.11.3. Blockchain Consortium

A consortium blockchain is a cross between public and private blockchains. It is a permissioned network in which various organizations or entities collaborate to keep the network running. Consortium blockchains are commonly used in areas where numerous parties must securely collaborate and exchange data, such as supply chain management or banking. The consortium members govern the network, and authorized participants have access to the network and data.[21]

1.12. Advantages and disadvantages of Blockchain

1.12.1. Advantages of Blockchain

- **Verifiable :** Blockchain technology is used to store information in a decentralized fashion so that everyone may verify the accuracy of the information by utilizing zero-knowledge proof, in which one party verifies the accuracy of data to another party without revealing anything about the data.
- **Immutability :** Because blockchain technology is decentralized, any modification will be mirrored in all nodes, making it impossible to commit fraud; hence, transactions can be claimed to be tamper-proof.
- **Transparency :** It makes transaction histories visible since every node in the network has a copy of the transaction. Any updates to the transaction are accessible to the other nodes.
- **Efficiency :** Blockchain eliminates third-party interaction between transactions and eliminates errors, making the system more efficient and speedier. Settlement is made simpler and more efficient.[12]

1.12.2. Disadvantages of Blockchain

- **Modification of data :** Blockchain technology does not allow for easy change of data after it has been recorded, and rewriting the codes in all of the blocks is time-consuming and costly. The disadvantage of this feature is that it is difficult to repair errors or make required modifications.

  One solution does not meet all needs, and blockchain technology is no exception. There is a lot of talk in the business about blockchain and Web3, and many organizations want to transition from Web 2.0 to Web3, but this is not a simple "lift-and-shift" solution. Companies should do due diligence and a deep dive study to determine whether blockchain technology is a good fit for their purposes, and then plan their development or migration to Web3 appropriately.

- **Speed and performance :** Blockchain is considerably slower than the traditional database because blockchain technology carries out more operations. First, it performs signature verification, which involves signing transactions cryptographically. Blockchain also relies on a consensus mechanism to validate transactions. Some consensus mechanisms, such as proof of work, have a low transaction throughput. Finally, there is redundancy, where the network requires each node to play a crucial role in verifying and storing each transaction.

- **High implementation cost :** Blockchain is costlier compared to a traditional database. Additionally, businesses need proper planning and execution to integrate blockchain into their process[12].

1.13. Future of Blockchain

- **Emerging Trends :** Blockchain is a fast changing technology, and numerous emergent themes are expected to define its future. They include the expansion of decentralized finance (DeFi), the creation of new consensus mechanisms, the integration of artificial intelligence (AI) with blockchain, and the introduction of new blockchain-based business models.

- **Potential Disruptions :** Blockchain has the potential to disrupt several industries, including banking, healthcare, supply chain management, and others. Blockchain can enhance efficiency, minimize fraud, and boost confidence by providing secure, transparent, and decentralized systems.

- **Adoption in Different Industries :** Blockchain technology is already being used in a variety of areas, including banking, logistics, healthcare, and others. As more businesses grasp the potential benefits of blockchain, adoption is projected to increase. Blockchain can enable quicker, cheaper, and more secure transactions in finance, while it can enhance patient outcomes and lower costs in healthcare.

  Blockchain can enable more transparent and efficient monitoring of items in logistics and supply chain management, as well as lower the risk of fraud. [12]

1.14. Conclusion

By enabling safe and transparent peer-to-peer transactions without the need for middlemen, blockchain technology has the potential to revolutionise numerous sectors. While there are still difficulties and constraints to overcome, the future of blockchain is bright, with new trends, possible disruptions, and growing acceptance across sectors.

CHAPTER 2

Application of Blockchain in Health records

Contents

2.1. Introduction

Many issues confront the healthcare business, including data security, interoperability, and privacy concerns. Patient data is frequently segregated in several healthcare systems, making it difficult for doctors to obtain the information they need to offer effective care. The application of blockchain technology in healthcare can assist in addressing these issues by offering a secure, transparent, and efficient method of storing and sharing patient data. Furthermore, blockchain can facilitate the creation of novel healthcare solutions such as smart contracts and decentralized healthcare apps.

2.2. Comparison between the Classic solution and the Blockchain solution

1. **Classic Solution:** A single entity is often centralized and controls everything (e.g. a company,government agency).[15]
    - Data is kept in a centralized database or on a server.
    - The controlling entity's data may be exposed to hackers, fraud, or manipulation.
    - The credibility of the governing entity may have an impact on data privacy and security.
    - Transactions can be time-consuming, expensive, and need the use of middlemen.
2. **Blockchain Technology:**
    - Decentralized and dispersed across a node network.
    - Data is kept in a distributed ledger, which is maintained by network participants by consensus.
    - Cryptographic techniques are used to safeguard data, making it harder to hack, modify, or corrupt.

- Participants have ownership over their own data and may specify who gets access to it.
- Transactions are quick, secure, and low-cost, and they may be completed without the use of middlemen.
- Data sharing and storage transparency.

2.3. Advantages of Using Blockchain technology in Healthcare

Blockchain technology can benefit healthcare businesses in a number of ways at once. First, it has to do with patients' medical records. EHRs may be safely kept in a decentralized system using blockchain that is immune to hacking and manipulation. Secondly, hospitals and other healthcare institutions can decide on patient care more quickly. It is feasible because all patient data is kept in a single, 24/7 system.[16]

Blockchain technology's simple data access speeds up the process of issuing medical credentials to healthcare workers.

2.3.1. Advantages for Patients

What matters most to patients? It's most likely the safety of their private medical information. By granting people control of their medical records, blockchain makes this possible.

In addition, no one is permitted to access patient data without that person's consent. Blockchain offers technologies like consensus processes, and because of these, medical data will only be seen by the patient.

Wearable technology is also covered by blockchain-powered data security. Patients can securely submit the data gathered by these gadgets to their doctors.

Patients will be able to take part in medical research, and blockchain will help them get money from their involvement. Doctors will benefit as well since they will have access to more research data.

2.3.2. Advantages for Pharmaceutics

Speaking of medical research, pharmaceutical firms might entice more participants for new drug clinical trials by utilizing the blockchain.

Additionally, because of the blockchain's immutability, data on medications and associated clinical trials will be accurate and simple to verify. This also makes it simple to identify fake medications, which is an advantage.

2.3.3. Advantages for Insurance

Patients can swiftly acquire insurance confirmation thanks to blockchain technology. Quick data transfer across companies is made possible by this technology.

Smart contracts may also be used to finalize insurance contracts, protecting patient data and providing ease for insurers.

2.4. Applications of Blockchain Technology in Healthcare

2.4.1. Electronic Health Records

EHRs are digitized records of a patient's medical history, including diagnosis, treatments, prescriptions, and test results. Blockchain technology has the potential to create a secure and decentralized platform for storing and distributing EHRs, giving patients more control over their data and guaranteeing that healthcare professionals have access to correct and up-to-date information.[1]

Figure 2.1: *Electronic health records [1]*

2.4.2. Patient Data Management

Patient data management is the most obvious blockchain use case example in the healthcare industry. For instance, if a patient knows blockchain encryption is in place, they may feel considerably more at ease providing information like their social security number and credit card details. In result, breaking a blockchain encryption system will be significantly harder for hackers. Additionally, you're considering secure patient data storage and improved accessibility. When a person needs access to their test results, they may set up their account information and get the information without worrying that someone is eavesdropping on their most private affairs. At the same time, their doctors have easy access to that data without worrying about prying eyes. Through the use of instruments like a patient health information portal, or PHI, the accuracy of a patient's medical records is guaranteed. A specialized blockchain-compatible IoT gadget may be used to collect electronic health records and quickly transfer them to a new doctor. Additionally, processing medical insurance claims is simple.[1]

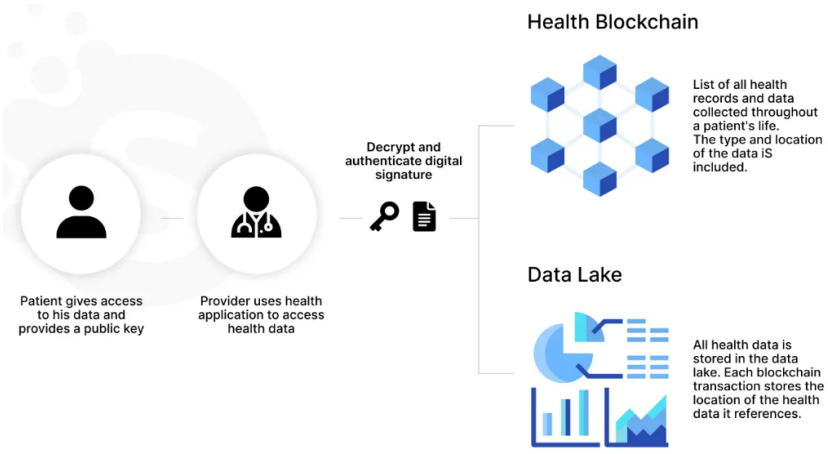

Figure 2.2: *Patient Data Management [1]*

The most secure approach to safeguard is by utilizing blockchain technology along with healthcare APIs, especially when it comes to a patient's identification. With an API in place, patients may choose who, outside their doctor, should have access to their medical information. They are even free to choose whether to grant full or restricted access. While doctors can more quickly diagnose a patient's condition and offer more conclusive and accurate medical care when using transparent data.[1]

2.4.3. High-Security Standards in Data Encryption

There are numerous applications for blockchain technology in healthcare, but it would be difficult to come up with one that is more compelling than preventing data breaches. Users of healthcare networks are more afraid of it than nearly anything else.

They don't simply want their credit card information or social security number to remain private. Additionally, if something concerning them is happening that they would prefer to keep private, they might not want the information about their medications to be disclosed.

When we consider how blockchain can improve healthcare, it becomes clear that a strong security standard is required to prevent this sensitive data from being spread widely across the internet.

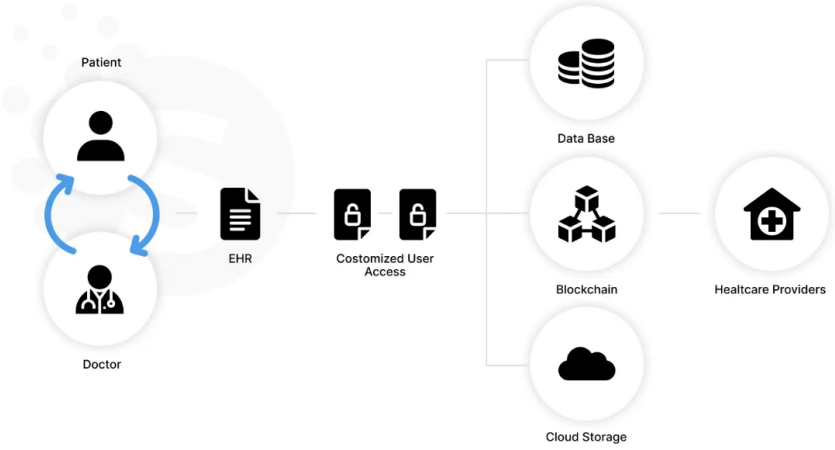

Figure 2.3: *High-Security Standards in Data Encryption [1]*

With the help of methods like capturing and encrypting data and anchoring it to the public blockchain, blockchain offers safe data transport techniques.

Blockchain data encryption is virtually impenetrable to hackers. While using it now, when telemedicine applications are rapidly evolving, is very advantageous, HIPAA mandates the use of secure data transfer and communication channels in the healthcare sector. Both doctors and patients are ecstatic about this new technology.[1]

2.4.4. Healthcare Transactions Control

You would also be right to assume that when blockchain technology is used, people feel more secure about their payment information. To maintain the security of your data, you may use a variety of encryption techniques, such as the transparent database encryption that we've incorporated into the Extobit project's development.

Every day, hundreds or perhaps thousands of patient claims and remittances are processed by hospitals and clinics. Additionally, they send out requests for unpaid patient bills. If fraudsters gain access to such information, they may cause all sorts of trouble. Given the level of expertise some of these hackers develop, identity theft is a serious concern.

The use of blockchain technology can reduce the number of claim denials.

Underpayments may be notified right away, minimizing human error and waiting times.

Many of these processes can be streamlined using blockchain, which also eases payment concerns. Medical institutions can enhance their daily revenue cycles and business processes.[1] '

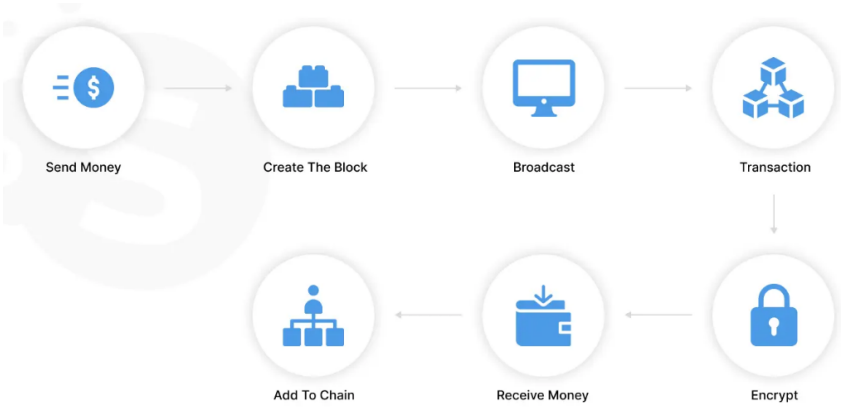

Figure 2.4: *Electronic health records [1]*

2.4.5. Drug Supply Chain Management

Let's start with some numbers. According to the National Crime Prevention Council, around 10% of the medications in the world's supply chain are fake. That's a worrying development, especially if folks who require such treatments aren't receiving the care they require to recover from potentially fatal illnesses. Some estimates place the annual market value of these fake drugs at up to $200 billion. However, all blockchain transactions are timestamped and immutable. It follows that using blockchain will make it simple to spot and halt the sale of fake pharmaceuticals and drug transactions. Another use of blockchain is for drug traceability, since it allows for the management of inventories and the tracking of medication life cycles.[1]

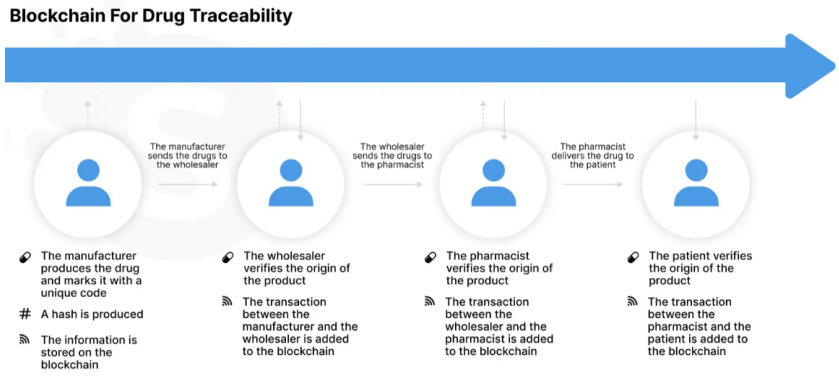

Figure 2.5: *Electronic health records [1]*

2.4.6. Clinical Trials and Healthcare Research Improvement

When it comes to clinical trials, which are used to examine the efficacy of new treatments, researchers gather and record enormous volumes of data. Test results, quality reports, and important data may be among them. Blockchain enables easy access to all of that while maintaining security and transparency in the knowledge that no unauthorized individuals are viewing it.

Blockchain also enhances organized processes and guarantees that trial participants gave their informed permission. The use of timestamps and smart contracts makes this possible.

Since the trial design must be followed and there is no chance of changing the test parameters in the middle of the trial, researchers are kept on their toes. Additionally, blockchain can link data from studies that appear to be incompatible. By using blockchain technology, connections that could have gone unnoticed can be instantly located. All of this leads to more reliable findings from medical research.[1]

2.4.7. Medical Paperwork Management

Another area where blockchain technology is useful is the handling of medical documents.

The amount of paperwork that hospitals and other healthcare facilities' patients and physicians must fill out might be decreased. Every time a digital system can take the place of a paper-based one, it benefits storage, lowers expenses and time spent on repetitive chores, and even avoids medical fatigue.

Additionally, it becomes simpler to track insurance transactions so that nothing is lost. Everyone concerned enjoys not having to go through the effort of giving additional copies of transactions to insurance carriers. [1]

2.4.8. Integration with Wearable IoT Devices

The ability of blockchain developments to work with wearable internet of things devices is now one of their most impressive features. It enables both patients and physicians to more effectively monitor medical records.

Blockchain can offer a simple authentication process and safe platform for integrating data from wearables like activity, health, or fitness trackers. Both the physicians and the patients have access to this safeguarded, often updated data, making it easier to follow changes or patients' progress.[1]

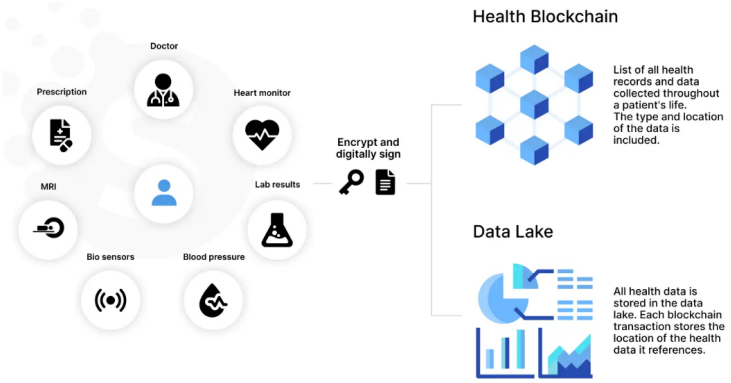

Figure 2.6: *Integration with Wearable IoT Devices [1]*

2.4.9. Tracking Medical Credentials

Every patient wants to have faith in the medical professional who will be treating them. What training does the specialist have, where has he worked before, and what are his credentials?

One of the applications of blockchain in healthcare is the verification of medical qualifications. With the help of this technology, all provider data may be kept in a single database. The blockchain will also assist in confirming the legitimacy of these credentials.

Since the employer can quickly review all the information about the candidates without a lot of red tape, it can also aid in the hiring of medical personnel. Furthermore, all medical credentials are protected by advanced blockchain security standards.[1]

2.4.10. Smart Contracts for Insurance

Smart contracts for insurance are another common application of blockchain in healthcare. This technology enables insurance service providers to automate insurance issuing and move their activities to a digital setting.

There won't be any disagreements about the conditions of the insurance because each smart contract will be easily available and registered on the blockchain. You may check online for information on health insurance coverage and medicine reimbursement.

Additionally, smart contracts enable insurers to employ cutting-edge analytics, which enables providers of such services to optimize insurance plans for their clients.[1]

2.5. Blockchain-based Health Record Keeping

2.5.1. How Blockchain Works in Health Record Keeping

- **Distributed Ledger Technology :** Blockchain employs distributed ledger technology (DLT), in which information is kept in several locations. This helps to avoid data manipulation since any modifications to the ledger are instantaneously logged across all network nodes.
- **Cryptography :** Blockchain employs complicated cryptographic methods to maintain the security and privacy of data stored on the network. This helps to safeguard sensitive data, such as patient health records.
- **Smart contracts :** are self-executing contracts in which the contents of the buyer-seller agreement are directly put into lines of code. Smart contracts may be used to automate the process of storing, updating, and retrieving health information, improving efficiency and transparency.[17]

2.5.2. Key Features of Blockchain in Health Record Keeping

- **Decentralized :** Blockchain is a decentralized system, which means that data is held across numerous network nodes rather than in a single database. This guarantees that the data cannot be manipulated by a single entity and that the system is transparent and trustworthy.
- **Immutable :** Data saved on the blockchain cannot be changed or destroyed. This ensures the integrity and validity of health records maintained on the blockchain.
- **Secure :** Blockchain employs powerful encryption to maintain the security and privacy of data stored on the network. As a result, it is an excellent choice for keeping sensitive patient health information.

- **Transparent :** The decentralized nature of the blockchain makes it transparent, allowing patients to have greater control over their health records and providing a clear audit trail of all changes made to the records.[17]

2.5.3. Advantages of Blockchain-based Health Record Keeping:

- **Improved Data Privacy:** Blockchain-based health record keeping systems can provide patients more control over their data, ensuring that only authorized parties have access to it. This can aid in the protection of sensitive health information from data breaches and cyber assaults.
- **Increased Data Security:** Blockchain technology is very secure, protecting data from alteration and illegal access. As a result, it is an excellent choice for keeping sensitive patient health information.
- **Enhanced Data Accessibility :** Patients may access their health records at any time and from any location in the world, without the requirement for a central authority or mediator. This can assist to increase healthcare system efficiency and cut administrative expenses.
- **Improved Interoperability :** Blockchain can assist to enhance interoperability between different healthcare providers and systems, enabling for seamless sharing of health data and improved care coordination.
- **Greater Efficiency :** By automating the process of storing and accessing health records, blockchain-based solutions can assist to cut administrative expenses and enhance the efficiency of the healthcare system. This can lead to better patient outcomes and higher levels of care.[17]

2.6. Challenges and Limitations of Blockchain Technology in Healthcare

- **Regulatory Frameworks :** The absence of clear legislative frameworks is one of the most significant barriers to the implementation of blockchain technology in healthcare. Blockchain-based solutions may not cleanly fit into existing regulatory frameworks, and clear guidelines are required to guarantee that blockchain-based solutions comply with existing legislation and standards.

- **Interoperability :** nteroperability is another barrier to blockchain technology adoption in healthcare. Healthcare data is frequently held in silos, making it difficult to communicate information between systems and companies. Blockchain-based solutions can provide a safe and decentralized platform for data exchange, but standards and interoperability frameworks are required to ensure that diverse systems can efficiently communicate and share data.

- **Integration with Existing Systems :** Combining blockchain-based solutions with current healthcare systems and infrastructure might potentially be difficult. Healthcare companies have invested considerably in current systems, and blockchain-based solutions must interact smoothly with these systems to guarantee that they can be adopted and used efficiently.

- **Data Privacy :** Another barrier to blockchain technology adoption in healthcare is data privacy. While blockchain can provide a safe and transparent platform for storing and exchanging data, patient data must be secured and patient privacy must be respected.

  Blockchain-based solutions must adhere to existing data privacy legislation and standards, and patient data must be accessible only by authorized parties.[17]

2.7. Future of Blockchain Technology in Healthcare

- **Emerging Trends :** Emerging trends in blockchain technology adoption in healthcare include the use of blockchain-based solutions for patient-generated health data, the integration of blockchain with other emerging technologies such as artificial intelligence and the Internet of Things, and the development of new blockchain-based business models for healthcare.[18]
- **Potential Disruptions :** By offering a more secure and efficient platform for storing and exchanging healthcare data, blockchain technology has the potential to revolutionize the healthcare business. It may also allow new healthcare business models that stress patient-centered treatment and bring better openness and accountability.
- **Adoption in Different Healthcare Sectors :** Blockchain technology has the potential to be used in a variety of healthcare industries, including medicines, medical equipment, insurance, and supply chain management. Blockchain-based solutions can help enhance efficiency, boost transparency, and safeguard the security and privacy of patient data in each of these industries.[18]

2.8. Conclusion

Finally, blockchain technology has the potential to revolutionize the healthcare business by offering a more secure, transparent, and efficient platform for storing and distributing healthcare data. While there are still obstacles to overcome, like as legal frameworks and interoperability, the future of blockchain technology in healthcare is bright. We should expect tremendous gains in patient outcomes, healthcare operations, and overall quality of care as the healthcare industry continues to implement blockchain-based solutions.

CHAPTER 3

Conception

Contents

3.1. Introduction

In this chapter, we attempted to create a blockchain-based system for medical data management that would provide patients complete control over their medical data while also protecting their privacy. So, we'll go through the overall architecture of our system, as well as the various diagrams, such as the use case diagrams and the sequence diagram....etc. The application will then be realized, and we will conclude with a conclusion.

3.2. Problem

Electronic health records (EHRs) are digital databases that contain health information. Demographics, medical history, drug and allergy information, vaccination status, laboratory test results, radiological pictures, vital signs, personal statistics, and billing information are all possible in EHRs. EHR is crucial in supporting doctors and healthcare facilities in assessing a patient's profile and offering appropriate therapy. breaches, frauds, and data thefts restrict healthcare providers from providing excellent medical care, possible data loss, and security attacks such as ransomware attacks.

3.3. Objective

The objective of this research is to create a blockchain-based system that aids in the administration and protection of patient data. This system creates a decentralized, iterative, safe, and open healthcare ecosystem using blockchain technology and smart contracts. With full control over their medical data privacy, people will be able to freely and securely exchange their medical records with physicians, hospitals, research institutes, and other organizations. Additionally, this research considers the usage of blockchain technology in a range of quickly expanding applications.

3.4. Overall operation

I will represent the design of my application, define the modeling language i will be using (UML" Unified Modeling language") is a standardized modeling language enabling developers to specify, visualize, construct and document artifacts of a software system. UML makes these artifacts scalable, secure and robust in execution. UML is an important aspect involved in object-oriented software development. It uses graphic notation to create visual models of software systems.[28]

There are two types of UML diagrams:

- **Structure diagrams :**
    1. Class diagram
    2. Composite Structure diagram
    3. Component diagram
- **Behaviour Diagrams:**
    1. Activity diagram
    2. Use Case diagram
    3. Sequence diagram

3.4.1. Use case diagram

A use case diagram depicts the interactions between actors and use cases as well as the functional needs of the system.

Actor	***Role***
Admin	• Login • Create Doctor • Create Patient • View List of patients
Doctor	• Login • View My Personal Information • View Personal information & Medical Record of Patient • Edit Medical Record
Patient	• Login • View My Personal Information • View My Medical Record • Approve Doctor + • Disapprove Doctor - • Approve Company + • Disapprove Company -
Insurance company	• Login • View Company info • View Personal information & Medical Record of Patient

Figure 3.1: *Actors and Rols of The EHR System*

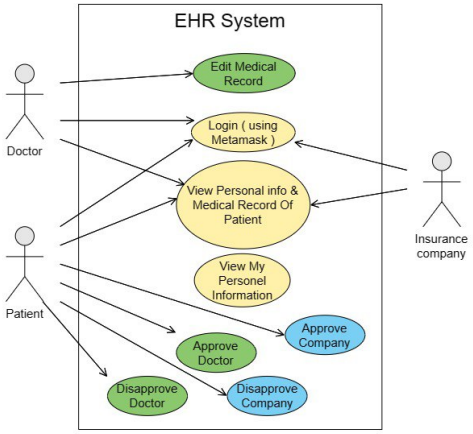

Figure 3.2: *Use Case Diagram of THE EHR System*

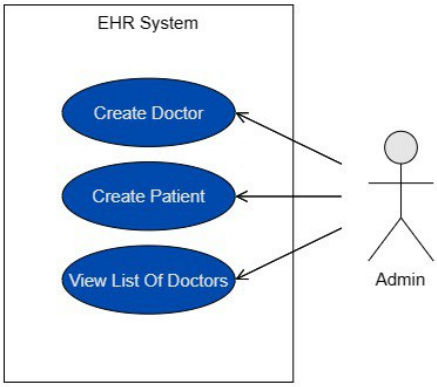

Figure 3.3: *Use Case Diagram of Administrator*

3.4.2. Sequence Diagram

A sequence diagram is used in this chapter to depict how items interact with one another over time. For a blockchain-based secure data management solution for electronic medical records.

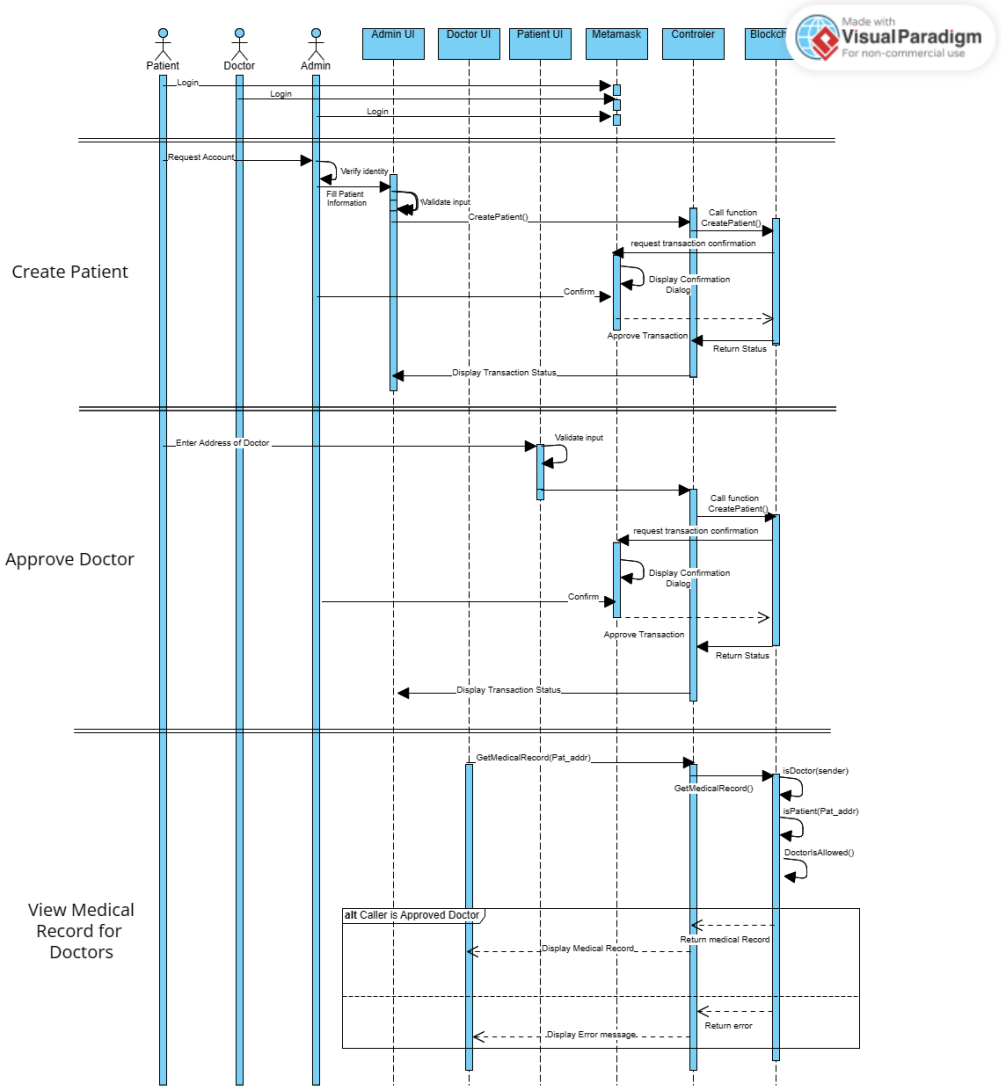

Figure 3.4: *Sequence Diagram of the EHR system*

3.5. Detailed Architecture

1. **Blockchain Network :** The patient is the only one with access to their private key. A request from the patient is required if a doctor wants to view a patient's medical records.

   A patient can provide access by inputting their private key when they get a waitlist request on their mobile app or on their website. The blockchain network will be updated after the operation is finished.

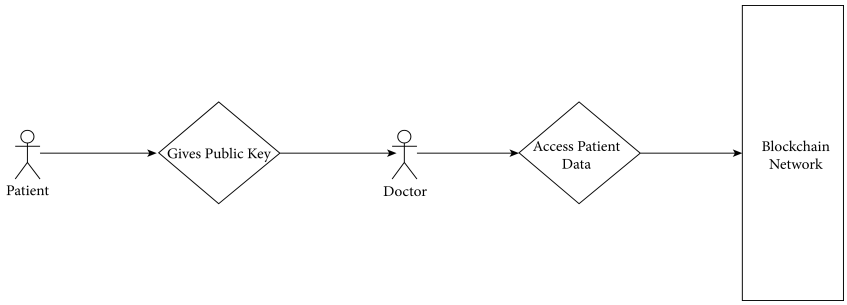

Figure 3.5: *Authentication of public key and blockchain network*

2. **Administrator :** When a patient or doctor wants to register in the system, they will need to provide the administrator with proof of their identity and doctor's certificates. Once the administrator verifies their documents and ensures their authenticity, a patient or doctor profile will be created for them from the administrator's dashboard.

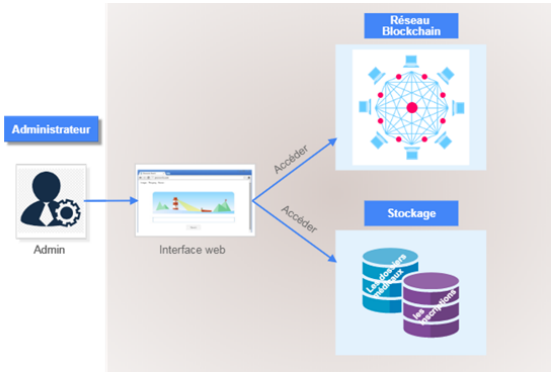

Figure 3.6: *"Admin" node architecture [3]*

Additionally, patients and doctors are required to provide their wallet address to the administrator.

3. **The Doctor :** If the patient grants permission, the doctor has the ability to access the patient's personal information and review or make edits to their medical record.

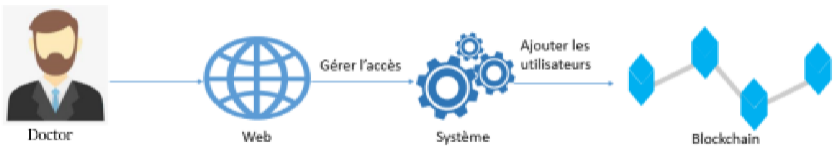

Figure 3.7: *"Doctor" node architecture [3]*

4. **The patient :** The patient is the owner of their information. No one can see their personal information or medical records unless the patient allows them to do so. The patient can only access and read their own information and medical records. They also have the ability to grant/revoke permission to a doctor to view and modify their medical records, as well as grant/revoke permission to an insurance company to access their medical records.

Figure 3.8: *"Patient" node architecture [3]*

5. **Insurance company :** If the patient grants permission, the insurance company can access the patient's personal information and medical record.

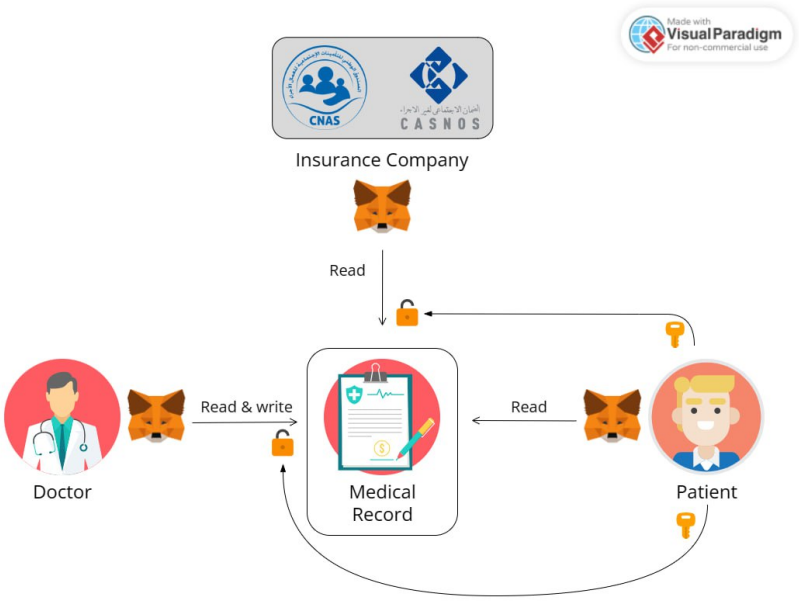

Figure 3.9: *Insurance company*

3.6. Conclusion

We have proposed a modeling of our system using UML through sequence diagrams and use case diagrams. We have presented the development of our system. The next chapter will focus on the implementation and realization of our system.

CHAPTER 4

Implementation and Result

Contents

4.1. Introduction

In this chapter, we will begin with an overview of the tools used to achieve our system Development tools and some screenshots on the app Implemented.

4.2. Fundamental Framework

4.2.1. Ethereum

A decentralized network based on blockchain technology, Ethereum. It was initially put into use on the well-known cryptocurrency Blockchain. The purpose of Ethereum was to provide an open-source platform for smart contracts with blockchain capabilities. Peer-to-peer networking is another method this technology employs to spread itself. This network also utilizes Ethers, a coin of its own. Additionally, Ethereum provides programmers with the Solidity language, which lets them to create their own blockchains. It was developed for Ethereum's last feature, smart contracts.[14]

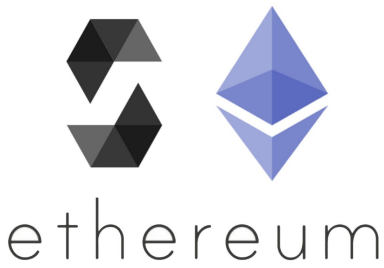

Figure 4.1: *Ethereum [14]*

4.2.2. Information Transaction

The way that outside parties communicate with Ethereum is through transactions. On the Ethereum blockchain network, it may be used by outside users to modify the status of a file or collection of data. An Ethereum transaction contains following elements[13]:

- **From:** the message's 20-byte address's sender.
- **To:** the receiver of the message, who likewise has a 20-byte address.
- **Value:**the sum of money (wei) that was sent from one party to another.
- **Data (optional) :** provides the receiver with the message that is being sent.
- **Gas:** The sender must pay a fee known as "Gas" for every transaction made on the Ethereum blockchain in order to complete it.
  - **Gas Price:** Each transaction includes the gas cap and gas price.
  - **Gas Limit:** the charge for which the transaction sender is prepared to pay.

4.2.3. The Smart Contract

A set of instructions known as a smart contract may be used to complete any transaction on the blockchain. This piece of code is executed when users send transactions. They function directly on the blockchain, making them resistant to manipulation and alteration. Any type of blockchain activity may be programmed using smart contracts, which use the Solidity programming language. The necessary operations can be compiled by the programmers once they have been programmed. They may then be assembled, executed, and deployed on the Ethereum blockchain. The smart contract code is written using JavaScript, which implements Ethereum's Solidity language.[25]

4.2.4. Ethereum Virtual Machine(EVM)

One of the Ethereum platform's main advantages is its programmable blockchain. It gives users the option to develop custom applications that work with Ethereum. Distributed Applications (DApps) are the name given to the applications created on this platform. They include a variety of protocols that are bundled up to make a DApp platform. These DApps include smart contracts with user-defined code that carry out specific application task definitions. The Ethereum Virtual Machine (EVM) is used to deploy and run that code [13],[14]. As a result, the smart contract-based apps are really being operated on EVM.

4.3. Software Required

4.3.1. Node.js

Node.js is an open-source, server-side runtime environment for JavaScript that enables programmers to create scalable and quick network applications. It handles concurrent requests quickly and effectively because it has an event-driven, non-blocking I/O approach. [29]

Figure 4.2: *Node.js [29]*

4.3.2. Ganache

It is a neighborhood Ethereum blockchain enabling the quick development of decentralized applications. Throughout the development cycle, Ganache may be used to deploy, develop, and test in a controlled and secure environment. Both the desktop application and the command-line tool (Ethereum) are functional.[25]

Figure 4.3: *Ganache [25]*

4.3.3. MetaMask

An Ethereum wallet is a software application that allows you to store, manage, and interact with your Ethereum (ETH) cryptocurrency. Ethereum wallets provide a secure way to hold your ETH tokens and other digital assets built on the Ethereum blockchain, such as ERC-20 tokens. Ethereum wallets come in various forms, including:[26]

- **Hardware Wallets:** These are physical devices specifically designed to store cryptocurrencies securely. They keep your private keys offline, protecting them from potential online threats. Popular hardware wallets for Ethereum include Ledger Nano S and Trezor.

- **Web Wallets:** These wallets operate online and can be accessed through a web browser. They offer convenience but may have lower security compared to software or hardware wallets since your private keys are stored on a remote server. Examples include MyEtherWallet (MEW), MetaMask (also available as a browser extension), and Coinbase Wallet.
- **Software Wallets:** These are applications that you install on your computer or mobile device. They offer greater control and security since you have direct access to your private keys. Examples include MetaMask, MyEtherWallet, and Trust Wallet.

Figure 4.4: *MetaMask [26]*

It's important to note that whichever wallet you choose, you should always prioritize security. This includes using strong passwords, enabling two-factor authentication (2FA), and keeping your private keys or recovery phrases safe and confidential.

4.3.4. Web3

In order to communicate with the chain's modules, transactions in the chain need be verified. A member in the network of another offline framework must transmit a transaction to the peer-to-peer (p2p) link, which is a real network, in order to produce and validate it. In order to facilitate communication between Ether-eum nodes and in-chain components, it also offers a library collection. It is used by Node.js on the server side.

Web3 connects to the Ethereum network by means of an Ethereum node using the Hypertext Transfer Protocol (HTTP) connection. This may be a node for local system ETH wallets. With the help of the in-browser plugin MetaMask, you may access your Ethereum accounts and utilize the platform on the website. The Ethereum wallet MetaMask is a browser-based application that links the browser to a Web3 provider class.[25] A data structure known as a Web3 provider

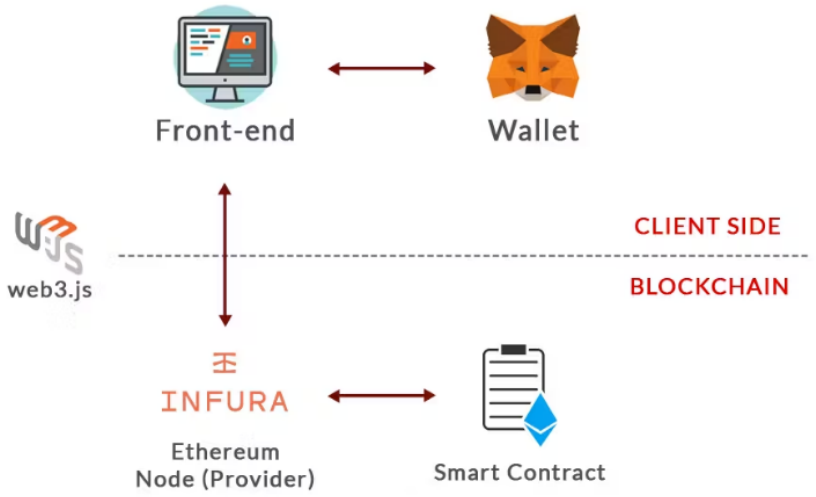

Figure 4.5: *Web3 App Architecture [25]*

offers a connection to publicly accessible Ethereum nodes. With the help of MetaMask, a user may use, save, and manage public and private keys that are specific to their account. Back-to-front communication is made possible by the combination of Ethereum, MetaMask, and web3.js, as well as a web interface.

4.3.5. Truffle

It has a robust environment for developing the Ethereum Virtual Machine that makes use of blockchains, as well as an asset pipeline and testing framework. It has several functionality, including binary dependency management and the computation, implementation, and maintenance of smart contracts. Additionally, it offers a scriptable deployment and migration architecture and a fully automated environment for testing smart contracts. Direct connection with the contract as well as a pipeline with close integration may be created. Programs are executed in the Truffle environment.[25]

Figure 4.6: *Truffle [25]*

4.3.6. WEBSTORM

An integrated development environment (IDE) for JavaScript and associated technologies is called WebStorm. Like previous JetBrains IDEs, it improves your development experience by automating tedious processes and assisting you in mastering challenging ones[12].

Figure 4.7: *webstorm [12]*

4.4. HARDWARE ENVIRONMENT

- **Processor:** Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz 2.80 GHz
- **Installed RAM:** 4.00 GB
- **System type :** 64-bit operating system, x64-based processor

4.5. LANGUAGES

Utilizing HTML (Hypertext Markup Language), JavaScript , React.js, the front-end design of our website was constructed. Using Node.js and the Solidity programming language, the website's server and back end are managed. The system is built using two tools: Truffle and Ganache, which generate local Ethereum blockchains. The system is accessed or utilized by the Ethereum virtual interface, MetaMask (as a wallet), Truffle (as an IDE), Yarn (a command-line interface), Ganache (account creation), and Local Web3 (a web interface).[25]

4.5.1. ReactJs

An open-source JavaScript library for creating user interfaces is called React. React, which was created by Facebook, enables programmers to design reusable UI components that can be combined to create intricate and dynamic online apps. It adopts a component-based approach, where each component has its own rendering and logic, making it simple to construct and manage complex applications. [30]

Figure 4.8: *React [30]*

4.5.2. Solidity

Solidity is a high-level programming language that is used to write smart contracts on the Ethereum blockchain. It was designed to be a contract-oriented language, with syntax and features that make it easy to write secure and efficient smart contracts.

Figure 4.9: *Solidity [27]*

Because Solidity is a statically typed language, each variable's type is specified directly at build time. It enables the creation of modular and extendable smart contract designs by supporting inheritance, interfaces, and abstract contracts.[27]

4.6. Protocol Layout

When a patient decides to examine their medical data using MetaMask or the healthcare system's centralized website, Figure 4.8 shows how the system is organized. The user logs in immediately by obtaining the private key from the Ethereum wallet. A cold storage wallet is the Ethereum wallet. As a consequence, the risk of compromise is rather minimal when compared to other hot wallets. Additionally, if the device is lost, the patients may simply receive a replacement without suffering consequences for losing their medical information. The wallet may be used in the same way to verify information or sign any document. You can use this wallet to carry out multiparty patient verification.[5]

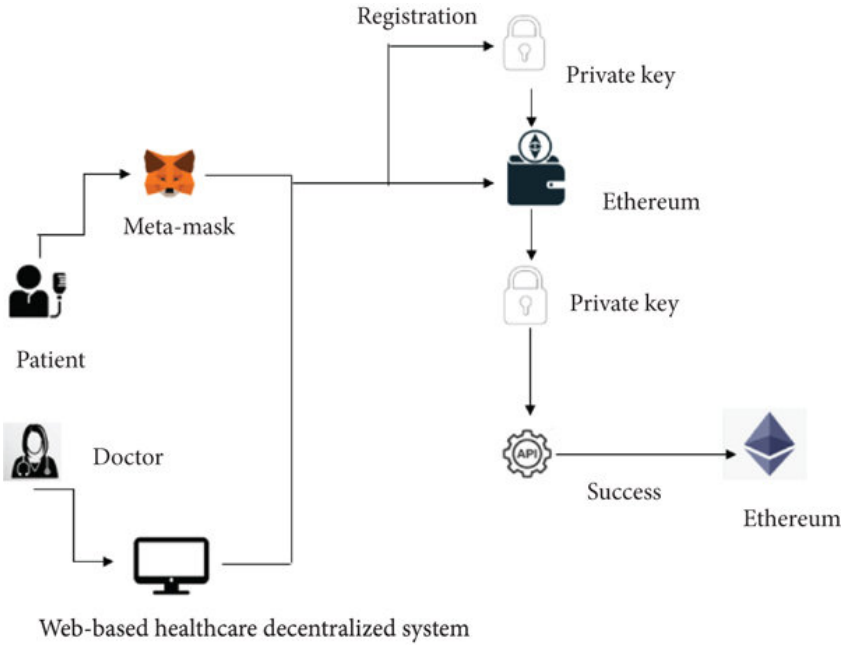

Figure 4.10: *The protocol layout of the EHR system [5]*

It may be used to create distributed property identification systems based on blockchains and role-based access control for records. A similar multiple-party authorization process can be used to provide access to the patient's records in the case of a medical emergency.

4.7. Process to Get Access to the Proposed System (Back End Part)

4.7.1. Transaction Deployment Using the Ethereum Blockchain

Use the Ethereum Blockchain to post transactions. The Ganache-represented Ethereum blockchain is seen in Figure 4.11. It was utilized for system deployment and testing. Ganache provides a few virtual accounts with 100 ETH for local testing and development. When implemented on the Ethereum mainnet, it offers a feature comparable to Ganache. The first step is to download and install Ganache Ethereum from the Truffle Suite in the background. After completing the Ganache installation, you must create a new workspace with the name EHR-project.

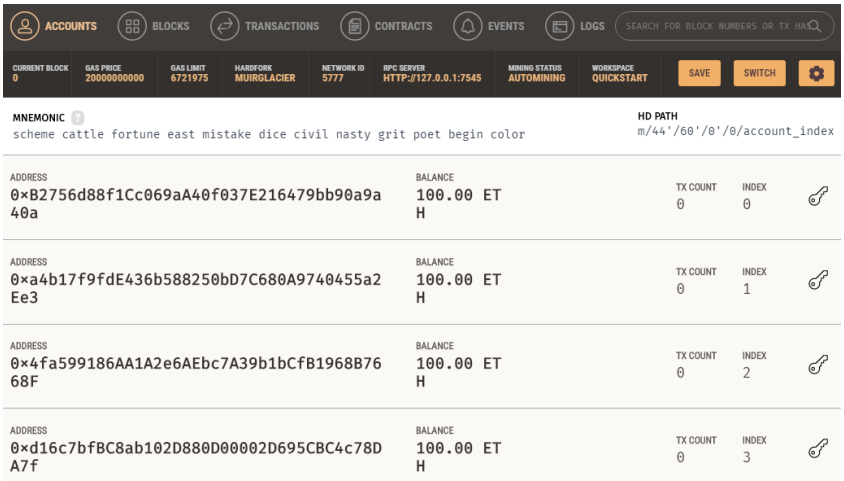

Figure 4.11: *Ganache home page*

4.7.2. Account creation using a smart contract

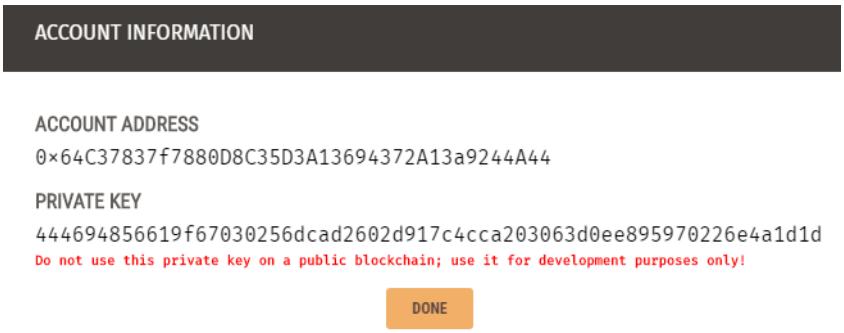

Figure 4.12: *Ganache Ethereum (account address)*

Figure 4.12 depicts the step-by-step account creation procedure and account data from Ganache Ethereum, which enables users to access a decentralized system using a browser without needing a complete node of the blockchain.

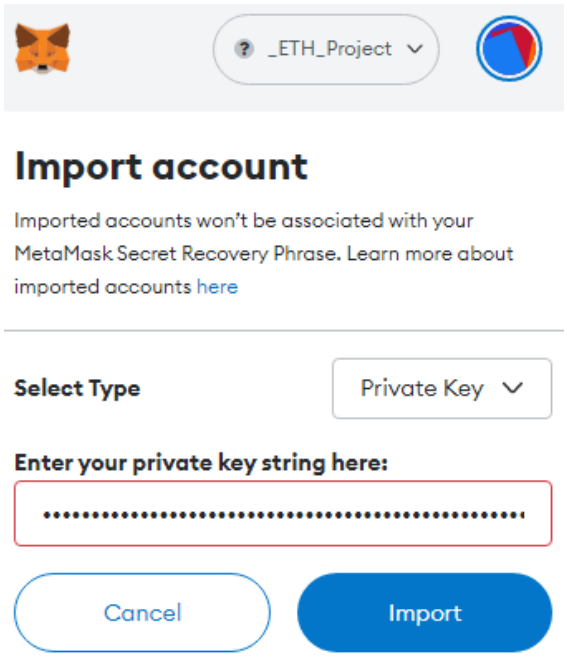

Figure 4.13: *add private key, and create account*

4.7.3. Truffle Migration and smart contract execution

Truffle Migration and Contract Execution. A snapshot of the migration and deployment process for a Truffle is shown in Figure 24.Truffle migrations enable you to upload smart contracts to the Ethereum blockchain (local) on a blockchain with a smart contract and build up the necessary processes for fusing transactions with other transactions and giving contracts with initial data.

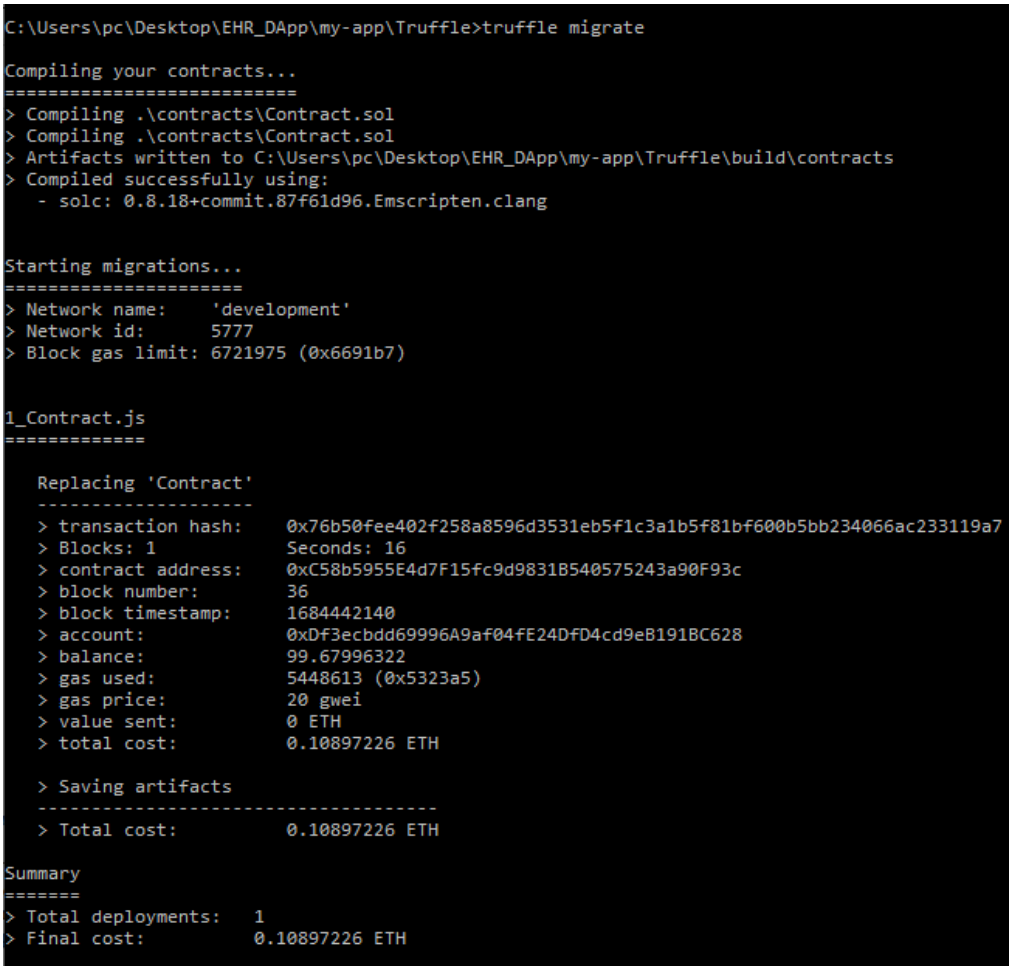

Figure 4.14: *Truffle Migration and smart contract execution*

4.8. Process of the System (Front-End Part)

4.8.1. Homepage

The main page of a software System is seen in Figure 4.15. The user must register for an account in order to view this home page. the system may then be accessed by users by Homepage. This homepage features four portals. The Patient, Assurance Company, and Doctor are the other users, with the System Administrator being the first.

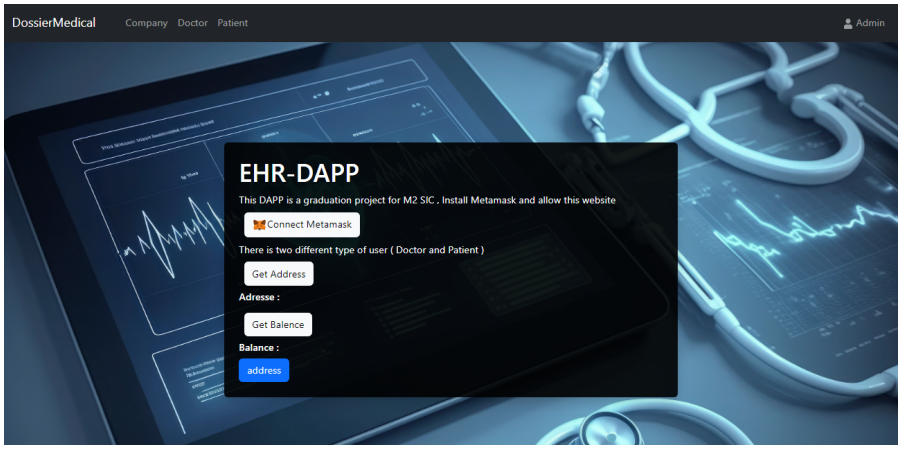

Figure 4.15: *Homepage of the proposed system*

4.8.2. Admin Panel

This system's admin interface is seen in Figure 4.16. Admins can add doctors and patients to the system.

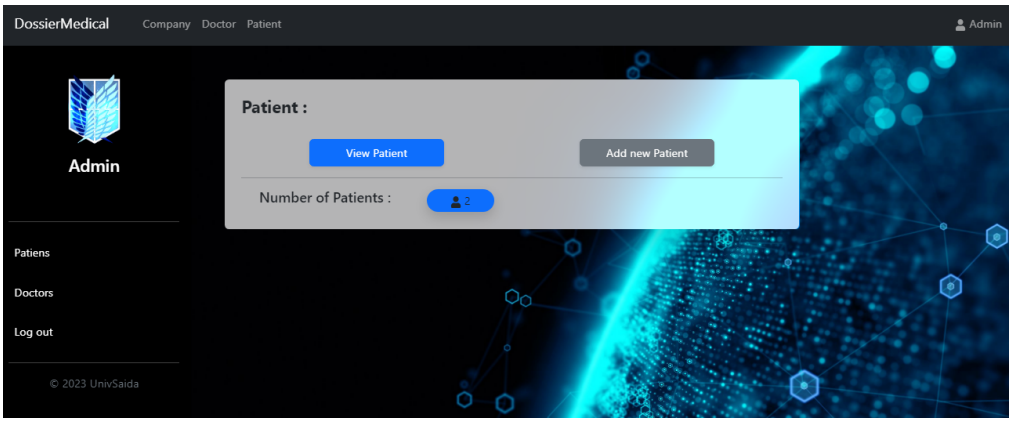

Figure 4.16: *Admin panel*

1. **Add doctor:** The method of adding a doctor is shown in Figure 4.17. depicts the doctor registration module where you must enter a doctor's information, including name, date of birth, email address, mobile number, and doctor ID, which is an identification number. account information for Ganache City,

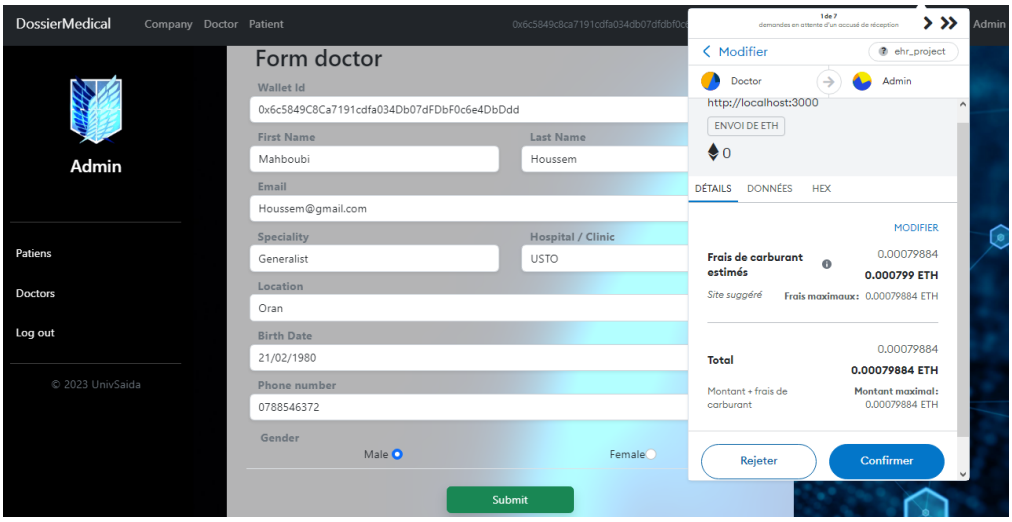

Figure 4.17: *Add doctor*

State, Specialty: Ethereum. The MetaMask confirmation message, which serves as a smart contract, All of the doctor's information will be saved using MetaMask, and the system will get an authentication confirmation message. However, the system will display an access forbidden notice if a user enters incorrect information or the same account address. Last but not least, this smart contract guarantees the privacy of the patient's data.

2. **Add Patient:** The module for patient registration is shown in Figure 4.18. which asks for patient data including names, email addresses, phone numbers, and patient IDs—which is a Ganache Ethereum account address—to be supplied. The user must click the "Submit" button after completing all of the fields with the necessary data in order to store the information and continue to the subsequent step.

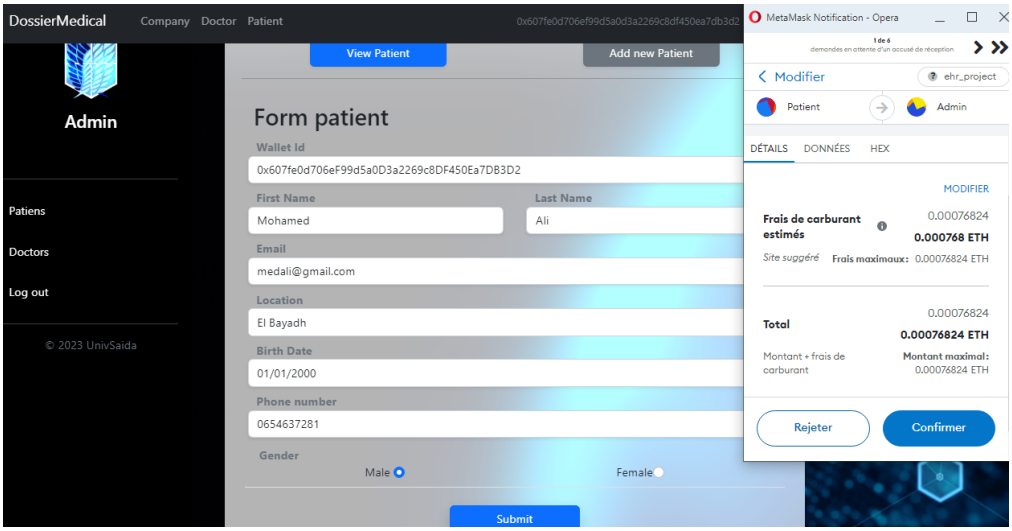

Figure 4.18: *Add Patient*

4.8.3. Doctor's Panel

In Doctor panel, the doctor can view and modify files Information.

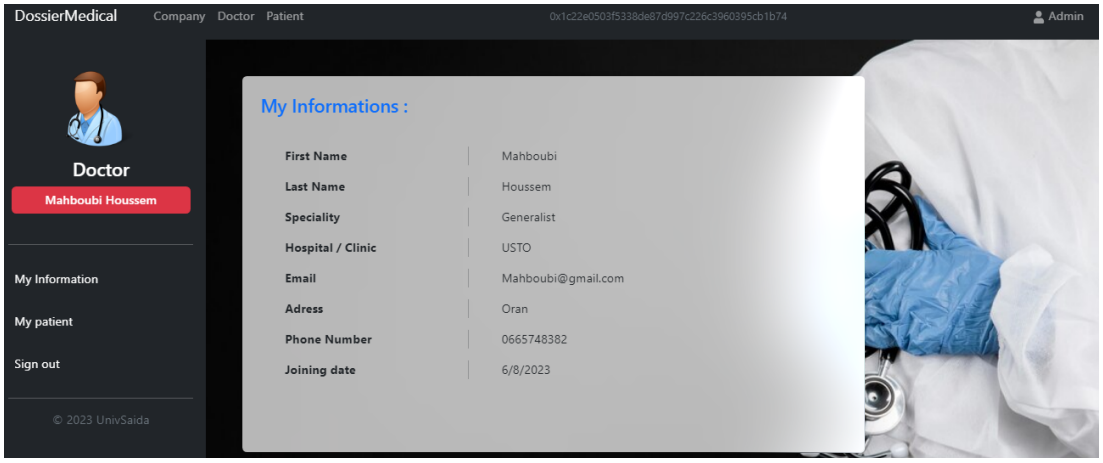

Figure 4.19: *Doctor information*

- The doctor can view personal information of patient and edit medical record.

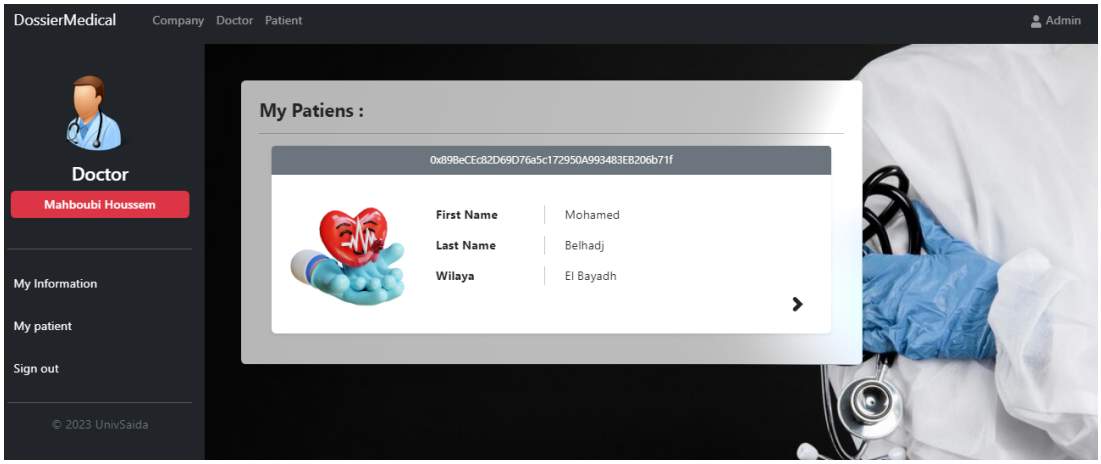

Figure 4.20: *View and Edit EHR of patient*

4.8.4. Patient's Panel

Figure 4.21 depicts the plate of a patient. The patient's personal information is displayed on the patient plate. Now that medical records have been created by doctors, patients may view them.

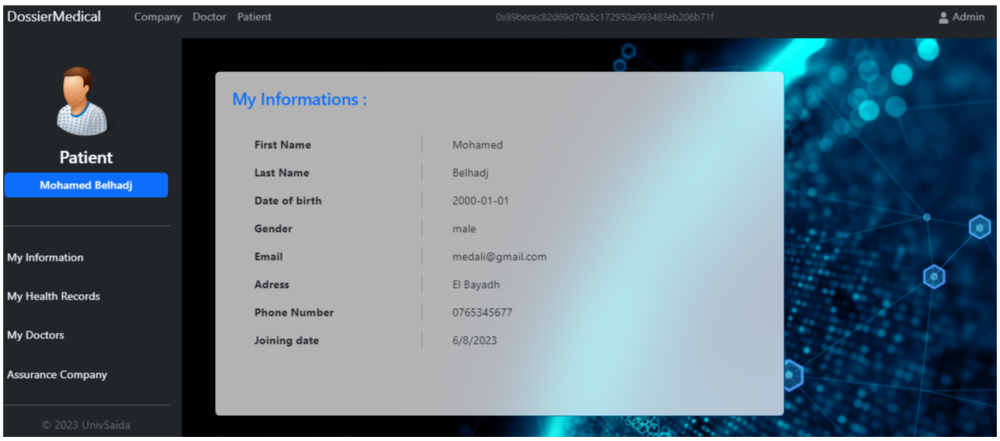

Figure 4.21: *Patient's information*

4.8.4.1. View the patient medical record

File is shown in Figure 4.22. the patient can log in and view their own medical records. This provides them with convenient access to their health information, including diagnoses, treatments, medications, and test results.

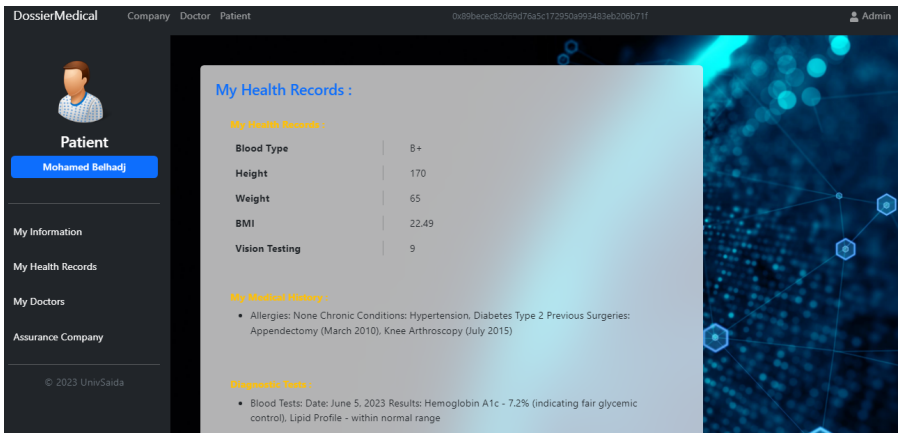

Figure 4.22: *View of the patient medical records*

4.8.4.2. Approve and Add Doctor's

Patients who want access to their medical information may have the option to accept or disapprove the doctors who request it. Patients now have discretion over who may access their private medical information.

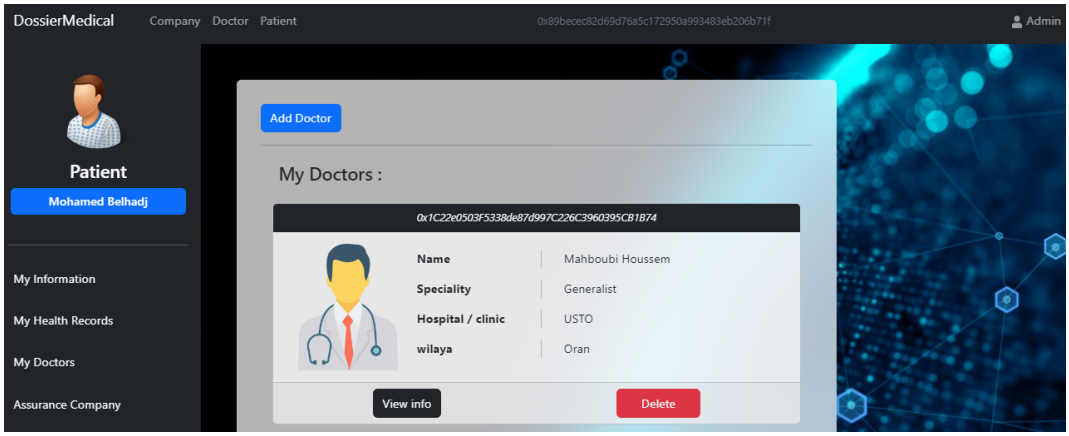

Figure 4.23: *Approve and Add Doctor's*

4.8.4.3. Approve Issurance Company

A request for access to certain medical records may be made to the patient by the insurance provider. The patient has the option to study the request and determine whether or not to permit access to their medical data for the purposes of determining insurance coverage or processing claims.

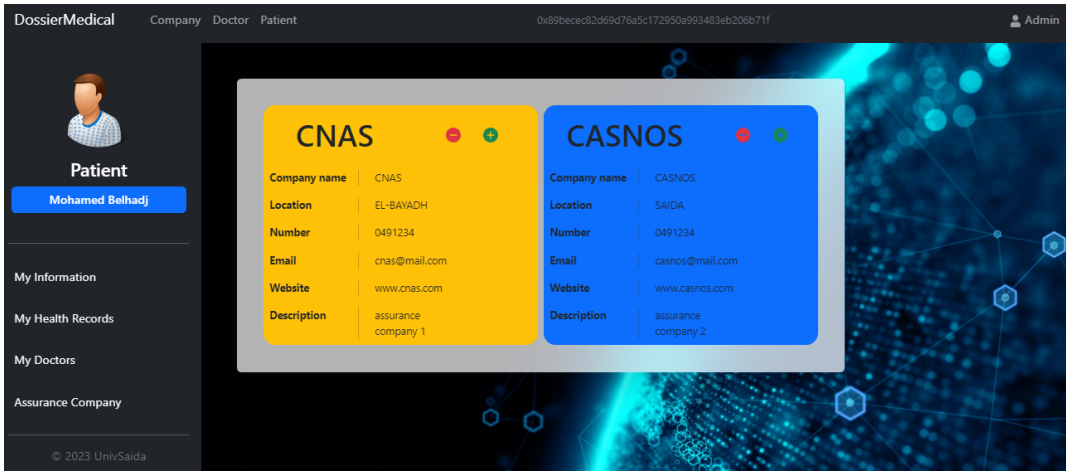

Figure 4.24: *View Issurance Company*

4.8.5. Issurance Company Panel

Figure 4.25 depicts the plate of Issurance Company.the Issurance Company normally does not have direct access to or read patient-specific personal information and medical data. The main goal is to make sure that the system as a whole complies with the relevant privacy and security requirements to safeguard patient data.

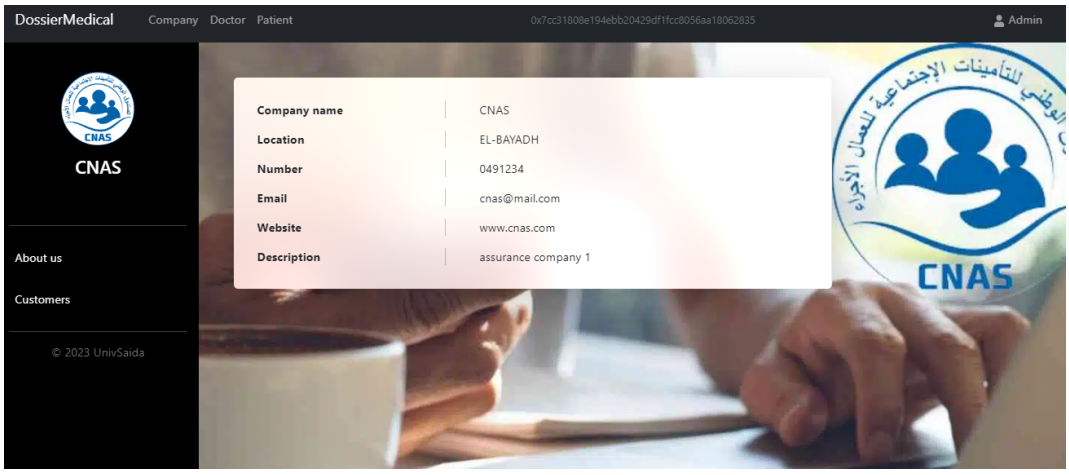

Figure 4.25: *Issurance Company Panel*

4.9. Conclusion

In this chapter, we realized a blockchain system using the development mentioned above. This allowed us to obtain a patient monitoring system and offers the ability to make a patient's lifestyle collection and make a connection between health professionals and patients.

Conclusion générale

A potential answer to the problems the healthcare sector is facing is the implementation of blockchain technology for safe data management of electronic medical records. Blockchain's decentralized and open nature offers a solid framework for safeguarding the privacy, availability, and integrity of patient data. By using a blockchain-based system, healthcare providers may enhance data security and privacy while reducing the likelihood of unauthorized access, data breaches, and manipulation. The immutability and openness of the blockchain, which ensures the integrity of medical records, have produced a trustworthy and auditable source of truth.

Additionally, blockchain technology enables the efficient and safe data sharing of authorized parties, such as patients, doctors, and healthcare institutions. Smart contracts enable automated implementation of predetermined rules and agreements, which also simplifies processes and improves interoperability.

This article's recommended architecture offers a conceptual framework and practical guidance for implementing secure data management of electronic medical records using blockchain technology. The technical requirements, design ideas, and system requirements necessary to create a scalable, dependable, and user-friendly solution are all described. Adopting cutting-edge technologies like blockchain will enable safe data management for electronic medical records and pave the path for a healthcare ecosystem that is more patient-focused and secure.

Abbreviation list

2FA Two-Factor Authentication

ECC Elliptic Curve Cryptography

DSS Digital Signature Service

EHRs Electronic health records

MD5 Message Digest

SHA-1 Secure Hash Algorithm

AI Artificial Intelligence

IOTA Internet Of Things Application

API Application Programming Interface

DLT Distributed Ledger Technology

UML Unified Modeling Language

EVM Ethereum Virtual Machine

MEW MyEtherWallet

HTTP Hypertext Transfer Protocol

IDE Integrated Development Environment

BTC Bitcoin

ETH Ether

POS Proof of Stake

PoW Proof of Work

P2P Peer to Peer

Bibliography

[1] Vaniukov, S.(2022, September 30). Top 9 Blockchain Use Cases in Healthcare Benefits You Should Know. Retrieved from softermii.com: https://www.softermii.com/blog/blockchain-in-healthcare-practical-use-cases-benefits-you-should-know/

[2] arghac14(2022, May 11). Difference between Blockchain and a Database.Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/difference-between-blockchain-and-a-database/

[3] Blockchain pour gestion des données médicales(2021).Retrieved from archives.univ-biskra.dz:http://archives.univ-biskra.dz/bitstream/123456789/18900/1/ZOUAOUI-RANIA.pdf.

[4] Beldjoudi,C,Yaic,M Bazizi,S.2020).Conception et réalisation d'une blockchain, cas d'étude: gestion du dossier de santé Electronique (Doctoral dissertation, université Abderrahmane Mira-Bejaia).

[5] Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., Saini, D. K. (2022). Electronic healthcare data record security using blockchain and smart contract. Journal of Sensors, 2022, 1-22.

[6] Azbeg, K., Ouchetto, O., Andaloussi, S. J., Fetjah, L. (2022). A taxonomic review of the use of IoT and blockchain in healthcare applications. Irbm, 43(5), 511-519.

[7] AnubhavUjjawal.(2023, Feb 17). How Does the Blockchain Work? Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/how-does-the-blockchain-work/

[8] Hooda, P.(2022, Sep 30). Smart Contracts in Blockchain. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

[9] guptavivek0503. (2022, Sep 20). Cryptography in Blockchain. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/cryptography-in-blockchain/

[10] swapnilkalyani96. (2022, Nov 26). Phases of Evolution of Blockchain. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/phases-of-evolution-of-blockchain/

[11] ritesh-nehru.(2022, Oct 13).Blockchain Hash Function. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/blockchain-hash-function/

[12] lastbitcoder. (2022, May 11). Advantages and Disadvantages of Blockchain. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-blockchain/

[13] G. Wood, "Ethereum: A Secure Decentralised generalised transaction ledger. EIP-150 revision," Tech. Rep., Aug. 2017, p. 33.

[14] I. Grishchenko, M. Maffei, and C. Schneidewind, "A semantic framework for the security analysis of ethereum smart contracts," in Principles of Security and Trust. 2018, pp. 243–269.

[15] Raj, R.(2023, May 10). What is Blockchain Database and Blockchain vs Database. Retrieved from https://intellipaat.com: https://intellipaat.com/blog/tutorial/blockchain-tutorial/blockchain-database/?US

[16] Nadejda Alkhaldi,Innovation Analyst.(2022, March 23).Top 7 blockchain use cases in healthcare. Retrieved from https://itrexgroup.com: https://itrexgroup.com/blog/blockchain-use-cases-in-healthcare-advantages-challenges/

[17] Fang, H. S. (2020, October 17). Blockchain Personal Health Records: Systematic Review. Retrieved from jmir.org: https://www.jmir.org/2021/4/e25094/

[18] The Future of Blockchain in Healthcare. (2023, 02 27). Retrieved from technology.com: https://isi-technology.com/blog/the-future-of-blockchain-healthcare/

[19] HAYES, A. (2023, April 23). Blockchain Facts: What Is It, How It Works, and How It Can Be Used. Retrieved from investopedia: https://www.investopedia.com/terms/b/blockchain.asp

[20] javatpoint.com. (n.d.). Retrieved from History of Blockchain: https://www.javatpoint.com/history-of-blockchain

[21] What is Blockchain?(2023).Retrieved from oracle.com: https://www.oracle.com/middleeast/blockchain/what-is-blockchain/

[22] AmishGupta.(2023, Apr 19).Introduction to Blockchain technology.Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/blockchain-technology-introduction/

[23] Key Features of blockchain.(n.d.).Retrieved from chat.openai.com: https://chat.openai.com/c/53f08d8d-6ad4-4d75-8358-337b8cf1f019

[24] m0hitkirange.(2022,Nov 16).Blockchain Structure. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/blockchain-structure/

[25] Farjana Khanam Nish,Mohammad Monirujjaman Khan.(2022).Electronic Healthcare Data Record Security Using Blockchain and Smart Contract.Retrieved from hindawi.com: https://www.hindawi.com/journals/js/2022/7299185/

[26] Matt Hussey ,Daniel Phillips.(2022, May 3).What is MetaMask? How to Use the Top Ethereum Wallet. Retrieved from https://decrypt.co: https://decrypt.co/resources/metamask

[27] Raj,R.(2023, May 10).What is Blockchain Database and Blockchain vs Database.Retrieved from https://intellipaat.com: https://intellipaat.com/blog/tutorial/blockchain-tutorial/blockchain-database/?US

[28] UML(informatique).(2017,décembre).Retrieved from wikipedia.org: https://fr.wikipedia.org/wiki/UML-(informatique)

[29] Desai, J. (2023). What Makes NodeJS Considerable for Software Development. Retrieved from positiwise.com: https://positiwise.com/blog/nodejs-for-software-development

[30] Walke, J. (2013). Your custom development solution with React JS. Retrieved from https://ubidreams.fr/: https://ubidreams.fr/en/expertises/development/react-js

List of Figures