ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Ανάπτυξη ηλεκτρονικού συστήματος ασφαλούς διαχείρισης αρχείων υγείας με χρήση της τεχνολογίας Blockchain

Φοιτήτρια: Σοφία Σπυροπούλου
Αριθμός Μητρώου: 50106710

Επιβλέπων Καθηγητής

Δρ. Γρηγόριος Κουλούρας
Αναπληρωτής Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΜΑΡΤΙΟΣ 2022

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

Development of an electronic system for the safe management of health records using Blockchain technology

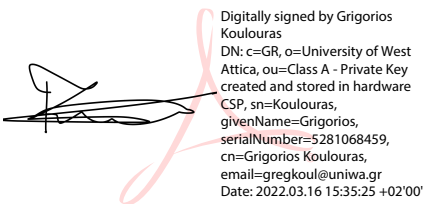
Student: Sofia Spyropoulou
Registration Number: 50106710

Supervisor

Dr. Grigorios Koulouras
Associate Professor

ATHENS-EGALEO, MARCH 2022

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Γρηγόριος Κουλούρας, Αναπληρωτής Καθηγητής	Δημήτριος Καλύβας, Καθηγητής	Ξενοφών-Διονύσιος Κανδρής, Καθηγητής
 (Υπογραφή)	Dimitrios Kalyvas Digitally signed by Dimitrios Kalyvas Date: 2022.03.16 15:30:38 +02'00' (Υπογραφή)	Dionisis Kandris Digitally signed by Dionisis Kandris Date: 2022.03.16 14:42:45 +02'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Σοφία Σπυροπούλου του Δημητρίου, με αριθμό μητρώου 50106710 φοιτήτρια του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.»

Η Δηλούσα
Σοφία Σπυροπούλου

Sofia Spyropoulou
Digitally signed by Sofia Spyropoulou
Date: 2022.03.16 14:29:51 +02'00'

(Υπογραφή)

I would like to thank my supervising professor Mr. Gregory Koulouras for the opportunity he gave me to do my thesis with him, and especially my family and friends for their support.

11/03/2022
Sofia Spyropoulou

Περίληψη

Τα τελευταία χρόνια έχει εισαχθεί με μεγάλη επιτυχία η τεχνολογία Blockchain και έχει κεντρίσει το ενδιαφέρον του κόσμου σε πολύ μεγάλο βαθμό. Στη σημερινή εποχή ένα μεγάλο ζήτημα που απασχολεί την κοινωνία αλλά και τους επιστήμονες είναι οι καινοτομίες που πρέπει να αναπτυχθούν στο χώρο της υγείας και της ιατρικής περίθαλψης. Σκοπός της συγκεκριμένης διπλωματικής εργασίας είναι να γίνει αρχικά μια διεξοδική ανάλυση των τεχνολογιών που σχετίζονται με την τεχνολογία Blockchain, προκειμένου να γίνει πλήρως κατανοητή η αξία της. Έπειτα, πολύ αξιόλογο κομμάτι αποτελεί η ανάλυση των προνομίων και των ελαττωμάτων που μπορεί να επιφέρει μια τέτοια τεχνολογία στον ιατρικό τομέα, μιας και θέτονται καίρια κοινωνικά, ηθικά και άλλα ζητήματα.

Θα γίνει αναφορά σε μερικές από τις εφαρμογές οι οποίες έχουν υλοποιηθεί από διάφορους οργανισμούς και εταιρείες παγκοσμίως και έχουν αρκετό ενδιαφέρον να παρουσιαστούν εκτενέστερα.

Τέλος θα υλοποιηθεί ένας προσωπικός φάκελος υγείας για τον ασθενή όπου θα αποθηκεύονται όλες οι πληροφορίες. Ο χρήστης θα μπορεί να αποδέχεται ή να απορρίπτει αιτήματα τρίτων που ζητούν πρόσβαση, αλλά θα μπορεί επιπλέον να έχει πρόσβαση ανά πάσα στιγμή για να παρακολουθεί την κατάσταση των δεδομένων του αλλά και τις απαντήσεις που λαμβάνει από τους γιατρούς στα αιτήματα του. Πιο συγκεκριμένα, θα εφαρμοστεί ιδιωτική αλυσίδα κόμβων με τη χρήση κατάλληλου λογισμικού ώστε να υπάρχει επικοινωνία μέσω της διαδικτυακής πλατφόρμας που θα αναπτυχθεί αλλά και της ιδιωτικής αλυσίδας, προκειμένου να είναι φιλική προς τον χρήστη και εύκολα προσβάσιμη.

Λέξεις – κλειδιά

Τεχνολογία Blockchain, Περιοχή Υγείας, Γιατρός, Ασθενής, Αιτήματα, Ιατρικά Δεδομένα, Ιατρικό αρχείο, εφαρμογή Ιστού, MetaMask, Ethereum Blockchain, Web3, P2P

Abstract

In recent years, Blockchain technology has been introduced with great success and has aroused the interest of the people to a great extent. Nowadays a big issue that concerns the society but also the scientists are the innovations that must be developed in the field of health and medical care. The purpose of this thesis is to first make a detailed analysis of technologies related to Blockchain technology, in order to fully understand its value. Then a very important part is the analysis of the benefits and weaknesses that such technology can bring to the medical field, since significant social, ethical, and other issues are raised.

Reference will be made to some of the applications that have been implemented by various organizations and companies worldwide and are of considerable interest to be studied.

Finally, a personal health file for the patient will be implemented where all the information will be stored. The user will be able to accept or reject requests from third parties requesting access but will also be able to access at any time to monitor the state of his data but also the answers he receives from doctors to his requests. More specifically, a private chain of nodes will be implemented with the use of appropriate software so that there is communication through the internet platform that will be developed and the private chain, in order to be user-friendly and easily accessible.

Keywords

Blockchain technology, Health Area, Doctor, Patient, Requets, Medical Data, Medical Record, Web app, MetaMask, Ethereum Blockchain, Web3, P2P

Index

List of Tables

List of Figures

List of Equations

Alphabetical Directory

AI: Artificial Intelligent

API: Application Programming Interface

ASIC: Application-Specific Integrated Circuit

CD: Compact Disk

CPU: Central Processing Unit

CRUD: Create, read, update and delete

CSS: Cascading Style Sheets

CyberTech Ltd: CyberTech Limited

DHT: Distributed Hash Table

ECMAScript: European Computer Manufacturers Association Script

ECDSA: Elliptic Curve Digital Signature Algorithm

EVM: Ethereum Virtual Machine

EOA: Externally Owned Accounts

Geth: Go Ethereum

GNU: GNU's Not Unix!

HTML: HyperText Markup Language

HTTP: Hypertext Transfer Protocol

ICO: initial coin offering or initial currency offering

Id: identity document

IDE: Integrated Development Environment

I/O: input/output

IPC: Interprocess communication

IT: Information Technology

MIT: Massachusetts Institute of Technology

MOH: Medical Officer of Health

NPM: Node Package Manager

P2P: Peer-to-Peer

PoA: Proof of Authority

PoW: Proof of work

RSA: Rivest–Shamir–Adleman

Src: source

SQL: Structured Query Language

URL: Uniform Resource Locator

USB: Universal Serial Bus

Introduction

In recent years due to the pandemic, the medical sector has been hit hard. Doctors and nurses are the ones who play the most important role in our society and fight daily for every patient's life. The lives lost due to the pandemic and Covid-19 are many, and the medical staff is the one who lived it to the fullest. Nevertheless, everyone did their best and managed, through research, to create medicines to shield our health. However, all this would be much easier if there was a system for recording medical data for each patient, in order to have easy access to his medical health history for the most appropriate treatment. Nowadays there is a need for an innovative idea in the medical field. Blockchain technology could revolutionize the way patients' medical data is stored and recorded. This will enable physicians to have faster and more complete access to medical information of the patient in critical situations. In a Blockchain application the entire medical history of a patient could be stored in it and be immediately accessible by doctors at any time, which is why the use of Blockchain technology in the medical field offers a great benefit.

In the present thesis, we will create an application of a Blockchain system that will offer patients a complete and easily accessible electronic record of their medical data.

Aims and objectives

The main objective of this current thesis is to learn how to build a Blockchain system step by step. Throughout this process a considerable amount of time was spent to learn a widely known programming language that is called JavaScript and consequently Node.js which is a software development platform built on a JavaScript environment. The abstract goal of this project more is the making of a patient's medical file, using the Blockchain technology, since once you upload your request into the system no one could make changes to it neither remove it.

Implementation

The methodology of this thesis was relatively like the most Blockchain applications. First thing was to find what programming language will be used to code and the best choice was JavaScript since that is the language most of the developers use. Next step was to find out the integrated development environment (IDE) to compose the code, which was easy since Visual Studio gives you the power to run your program. After that comes choosing between sqlyog or navicat for the database. Navicat is a series of database management and development software developed by CyberTech Ltd. for MySQL. Since Ethereum Blockchain used for this project the software cryptocurrency wallet used was MetaMask to interact with the Blockchain. Really important part of this thesis is learning how to

implement your own smart contract and for this the programming language called Solidity was used. After choosing all the programming tools, the next step was to find what programming libraries will be used and therefore are necessary to build such a program. Furthermore, Xampp used because it includes the MySQL database. Xampp is an open-source software package. A small online search easily led to what is needed for this project. Since all the desirable research has been done and after the necessary material and knowledge for the implementation have been gathered, the project began. The project was built locally since the creation of the application has no commercial purpose but mainly educational.

Innovation

Blockchain technology is relatively new to the world and especially in the medical field. There are some applications in the health industry that are based in the Blockchain, but they are not widely used in the field. As a result of this dissertation and its objectives, a code structure has been implemented and an application was created which not only in Greece but also worldwide can be used. The electronic medical file which offers the possibility to the patient to have all his medical records registered regardless of the hospital or the doctor who has performed the respective examination, operation, prescription, etc. can make the work of the doctors easier, but also in periods of crisis when time is precious mistakes can be avoided.

Structure

In the first chapter, it can be described as one of the main chapters of this thesis since it describes the Blockchain technology as briefly as possible. It contains the history of the technology and explains what exactly this technology is. After that, Web3 is presented, which is the most modern development of the internet and the one that makes the existence of decentralized applications possible today. Following up with the peer-to-peer network which is a key component of the technology. Also, there will be a discussion about the elliptic curve cryptography in which the Ethereum is used for the security of the network. Finally, in this chapter a detailed presentation of Ethereum Blockchain and the smart contracts is made, as there are the basic technologies used for the implementation of this thesis.

Following up with the Blockchain technology in the healthcare industry, there will be a presentation of the advantages of the technology and the disadvantages in the field since we can compare according to the respective data, the way hospitals operate, the medical records of the patients but also how the data management can be done much easier. Also, there will be a discussion about the companies that

have already created this kind of applications with the Blockchain technology in the healthcare industry in order to provide them with security of their data and to accelerate the care process, improve health outcomes etc. After that, it is time to talk more precisely about the application that we are about to create. So, in chapter 3 we begin with the tools and the technologies that was used in order to create the app. More specifically, Ethereum Blockchain technologies are mentioned, the Node Package Manage, the Node.js and the MySQL since it is the database. Afterwards, in chapter 4 it is going to be examined the design and the implementation of the project and more specifically the smart contract that it was implemented, and the front-end and the back-end development of the application. In Chapter 5, after all the above are explained and fully understood, it is the right time to present the application and the way it can be used by each user individually. To finish this thesis, in the end there is a small chapter about all the things implemented and some future goals for this project.

1 Theoretical Background

1.1 Introduction

In recent years, many papers and books have studied the Blockchain technology and its use in today's society. Starting off with this thesis, finding useful resources was the main goal of building up this research. This chapter sets out the theoretical background of the technology of the Blockchain. The initial goal is to emphasize the importance of the technology and the innovations that have come about thanks to it. Then reference is made to the evolution of the world wide web to the present day. After that, the technology of peer-to-peer networks is described below, as it is one of the key elements of Blockchain. Finally, there is an extensive presentation of Ethereum Blockchain and the smart contracts that are one of the most important parts of this thesis.

1.2 Blockchain

Blockchain technology first appeared in 1991 by W. Scott Stornetta and Stuart Haber, who wanted to build a specific system in which data could not be changed. After them, Satoshi Nakamoto in 2008 created the cryptocurrency called Bitcoin, which is a P2P (peer-to-peer) network. Bitcoin mainly provides the possibility of financial transactions verified by network nodes through cryptography and it is recorded into the Blockchain. Cryptocurrency is secured by cryptography, and it is a digital currency. Most of the cryptocurrencies that exist today are based on Blockchain technology. Bitcoin is the most popular cryptocurrency in today's world [1].

Furthermore, Satoshi Nakamoto improved the existing idea and created a system for recording all the transactions of the network. Then many different Blockchain applications came to the world, with the most famous of all being Ethereum.

The technology of the Blockchain is based on a data structure invariant that manages a computer cluster which is not part of any single entity. Each of the blocks depends on other blocks and is secured by cryptographic principles. This technology is a simple and smart way to transfer information from one user to another in a simple secure and automated way. To create each block, you need to do the following, firstly a large volume of computers across the network validates this block. Then, this block is being added to the chain, and then stored across the network, creating a unique and specific file. It is almost impossible to attempt to falsify the chain data, as this presupposes that the user attempting to do so has access to the entire network of the Blockchain.

Figure 1 - Bitcoin[1]

1.3 Web3 – Decentralized web

In this part it will be analyzed the evolution of the web. The web that is now used is completely different to the one that it was used (Web 1.0), and with the decentralized internet everything is going to change once again. Web 1.0 approximately lasted from 1991 to 2004 and it was the first edition of the web and it mainly had static pages with "read-only" options. But on 2004 Web 2.0 appeared, which added to the modern lives of the people the social network and also the online shopping. In this web you do not have to be a developer in order to contribute to the content of the site. Web 2.0 is that simple that even more and more people are trying to become designers. The main think about it, is that basically in every application there is a central entity which can manage the operation of the whole application. This mode of management is based on the assumption that users have confidence and trust in the managers. Talking about a manager, refers to an organization, a company, or a government agency. Even in the Peer-to-Peer (P2P) applications there is someone who is doing the manager job.

[1] https://pixabay.com/images/id-2007769/ (last accessed 25/02/2022)

The Blockchain technology, is the technology that is needed to avoid the above problems as it seems to be the main guide to the new generation network, the Decentralized Web (Web 3.0)[2].The Blockchain gives the opportunity of the P2P transactions without having intermediate parties. The use of decentralized applications is becoming more and more popular due to the fact that developers try to reduce the use of central servers. With this new model it is believed that today will address the client-server problem, which have to do with the data of the customers, their security, interception, and abuse by organizations but also their loss due to the only point of failure (Single Point of Failure) etc. The Blockchain is a fundamental element of the Web3 [2]. Nowadays the technology has evolved so much that it has reached the point where there is the possibility of developing and operating a decentralized application (Dapp).

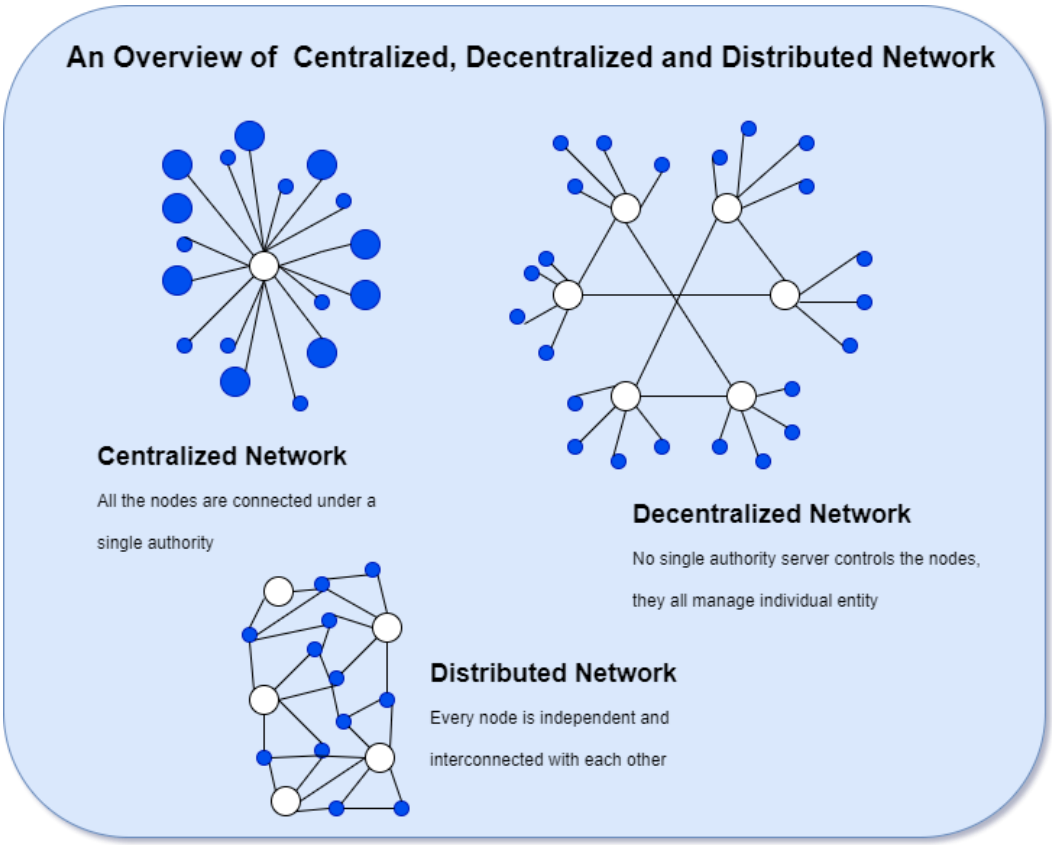


Figure 2 - Centralized, Decentralized and Distributed Network

[2] https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained (latest accessed 25/02/2022)

1.4 Peer-to-peer architecture

The dominant models of the web applications are the client-server model and the peer-to-peer model. The main difference between those two is that on the first one there is always a computer in use, the server, and he serves requests for services from the clients. On the other hand, on P2P model there is little or no support in data centers [3]. In the peer-to-peer architecture there is a straight communication between the computers. The computers are managed by users that all have same abilities, privilege, and the same part in the network. Consequently, they have a portion of their resources running the network, and this results in no need for a host. Peer nodes act as clients and as servers.

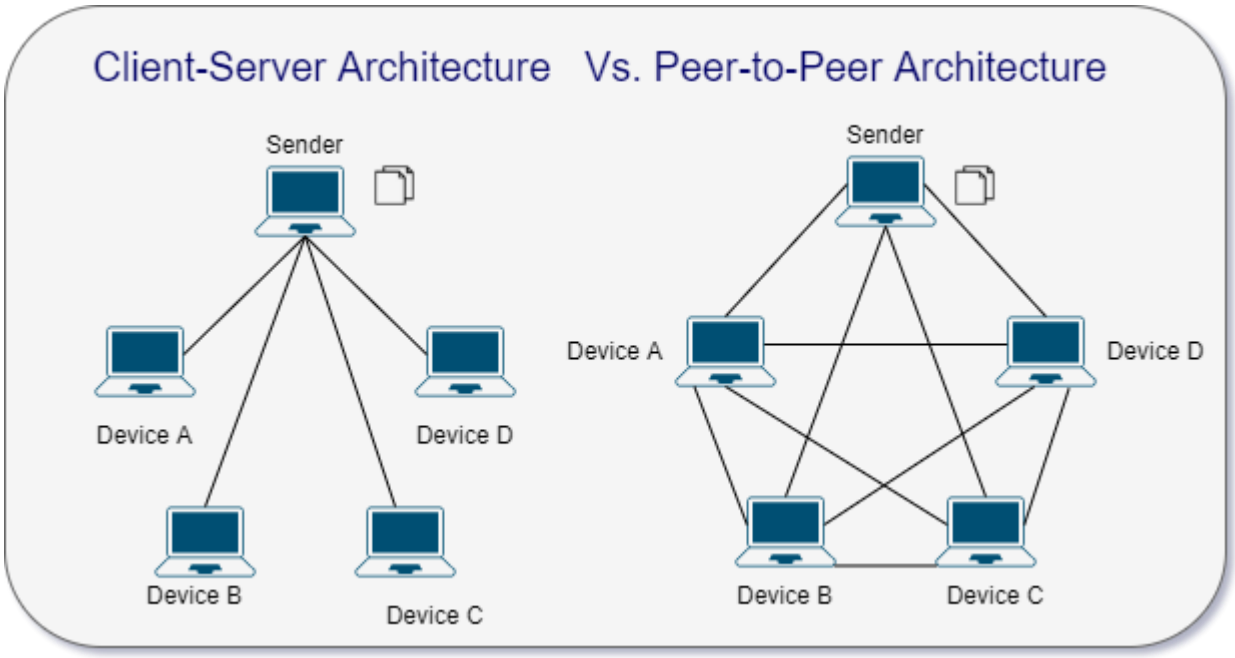


Figure 3 - P2P

The Blockchain technology is also a technology based on the peer-to peer architecture.

There are categories for the P2P network. Firstly, there are the structured P2P networks where the higher level of the network is organized in such a way as to have a specific network topology based on a protocol. This is to ensure that it has a better search for every data within the nodes. The most widely known structured P2P network, is the Distributed Hash Table (DHT). It looks up data based on key-value pairs. Every single node is responsible for a specific set of keys and their linked values. Data values have a key that is a unique identifier, and it is created when you run a hashing function. Any form of values can be a data value.

On the other side, there is also the unstructured P2P network where the upper level of the network does not have a desired form, but the nodes are connected completely randomly with each other. Such networks are easy to be made and that is one of their biggest advantages. If a peer wants to find a specific data in the network, the query will look for it in order to locate the most peers that share the exact data. The main disadvantage is that the queries may not often be resolved. In several peers you can find a popular content and if any peer is looking for it, it is likely to find the same, but if he is looking of a data that is not as popular shared by a few peers, then it is usual this kind of search not to be successful. They are causing flooding to the P2P network.

So, in order to have a smooth routing of data, it is required for all the nodes of the network to adhere to neighbor lists with specific standards. This makes the network more vulnerable in the event of a large increase and departure of nodes (churn).

1.4.1 Some of the advantages of peer-to-peer network are the followings:

- Cost: If you want to build a P2P network, the complete cost is inexpensive. Because there is no central configuration, the cost of the setup has been reduced and there is no need for payment for all the users for the windows server.

- Self-scalability: The performance of the network will remain the same, as many extra clients added. At the same time the available resources of the system increase, due to the dual nature of every single peer node.

- Administration: All the users can manage their own system and choose which files they would like to share. That is why there is no need for a specialized network administrator.

- Server Requirement: There is no dedicated server because each computer is a workstation and a server at the same time.

- Reliability: All the computer users of the network can function independently with each other. If a part of the peer-to-peer network has a failure, that does not mean that the other parts will have a problem.

- Implementation: It needs specialized software, but in general, it is easy to setup a peer-to-peer network considering that all the computers can control themselves.

- Resource Sharing: Everything is shared to all the users similarly. At the same time, they can consume and provide resources.

1.4.2 Some of the disadvantages of a peer-to-peer network

- Security: The peer-to-peer applications can create problems due to their open and distributed nature.
- Performance: P2P network does not work that well when the number of the devices connecting increases.
- Remote access: Sometimes, some users are accessing into some files with no permission.
- Backup Recovery: Since the network is decentralized, backup is saved in multiple systems. That means, backup is done on every computer separately.
- Virus attack: If a computer gets infected to a malware and virus attack, it can spread the virus easily to the other computers since they are on the same network, even if the computers are protected.

1.5 Elliptic Curve Cryptography

Elliptic Curve Cryptography is a new science that helps create global security. This theory firstly appeared in 1985 by Victor Miller and Neal Koblitz as a pioneering mechanism for executing public keys. It is based on discrete logarithms, which makes it even harder to break compared to other public key algorithms such as the Rivest–Shamir–Adleman algorithm (RSA) [4].

Nowadays, the Elliptic Curve Digital Signature Algorithm (ECDSA) is used in Ethereum for cryptography, and it is not easy to be violated by any attack.

1.6 Ethereum Blockchain

Ethereum platform has been created in order to develop smart contracts. It is a very flexible platform. Ethereum was developed after Bitcoin, and it can be used to develop decentralized applications that perform in complete security.

Figure 4 - Ethereum [3]

The most crucial difference of Ethereum compared to Bitcoin, is that the former is a much more flexible and customizable platform. In Ethereum there is the possibility of creating and secure operation of decentralized applications, compare to Bitcoin in which pretty much financial transactions are made using the cryptocurrency.[4]

Ethereum is a Turing complete computing architecture in which every single node of the network performs some transactions which are then classified into blocks and in the end added to the chain. Each block contains the proof of work (PoW). Every single time, only one block is added to the Blockchain and the network nodes that create these blocks are called miners [5].

1.6.1 Ethereum Virtual Machine

Ethereum Virtual Machine can execute code of any algorithmic complexity and could be used to solve any computational problem. Furthermore, the Ethereum virtual machine or EVM is completely isolated, which means that the code running inside the EVM does not have access to any network. Therefore, the code is completely safe.

In the center of Ethereum we have the "EVM" (Ethereum Virtual Machine), which have the ability to execute code of arbitrary algorithmic complexity. The Ethereum is Turing complete as it was mentioned above. Turing completeness is quite important for smart contracts because we can

[3] https://pixabay.com/images/id-6293700/ (last accessed 25/02/2022)

[4] https://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html (last accessed 25/02/2022)

implement complicated logic. Ethereum contains the peer-to-peer network protocol, which has the power to coordinate connected nodes and to guarantee the smooth operation of the network. This gives Ethereum very high error resistance, unbreakable operation and guarantees that the data of the system will not be changed.

1.6.2 The way Ethereum Blockchain works

Ethereum is very similar to Bitcoin but introduces many different modifications and innovations in the way it works. So, while in Bitcoin for each block there is a list of very specific transactions, the basic idea of Ethereum is the exchange of data between multiple accounts. So, every single block checks the status of each account and all changes that are being made to Ethereum involve the transfer of cryptocurrencies and information between accounts.

There are two types of accounts. Firstly, the Externally Owned Accounts (EOA), which are being controlled by private keys. Secondly, the Contract Accounts, which are being controlled by their internal code and can be activated by only one EOA.

The basic difference between those two is that the Externally Owned Accounts are being controlled by the users that they own and check their private keys, and on the other hand the Contract Accounts are being controlled by their internal code as it was mentioned above.

Smart Contracts refers to code that exists within a Contract Account and is executed when a transaction is sent to that specific account. With Elliptic Curve Cryptography the users have the ability to send transactions to the network and signing the transactions with their own private key. A transaction can be valid only when it is signed by the sender, so that the network can be completely sure that the sender is the one who says it is and not someone else.

Moreover, users must pay small network charges (gas) in each transaction, and this happens to protect Blockchain Ethereum from malicious users and hacker attacks. This fee is paid on the cryptocurrency of Ethereum that is called ether. The miners collect the fees and validate the network. The network nodes, the miners, validate, transmit, receive, and execute transactions. Some of the transactions are arranged in a block, and the miners compete with each other in order to enter them in the Blockchain. And every single time the miner introduces a new block he is being rewarded with an amount of ether. Therefore, the nodes are rewarded with ether for each single block they validate.

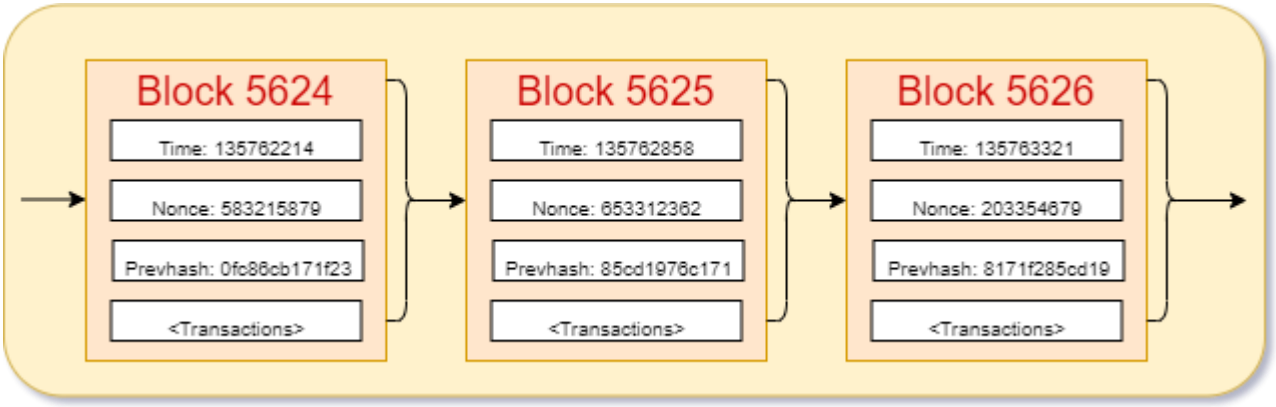


Figure 5 - Ethereum Blocks

The algorithm used to authenticate the new blocks that they added to the Blockchain, called Proof-of-Work. This is a difficult mathematical problem to be solved. This problem needs a huge amount of memory, so to do mining in Ethereum, memory is required from the system but also CPU, while in Bitcoin only a graphics card is needed. To conclude, in the case of Ethereum there is a decentralized network and PoW is more resistant to ASIC's. Consequently, there is greater security (many and small miners, rather than few and strong).

As mentioned above ether is the name of the cryptocurrency that is used in the Blockchain of Ethereum. Ether consists of eighteen decimal places. The smallest unit of measurement of ether is called Wei (Ethereum Homestead, 2018). Finally, below is a list of ether subdivisions and their value based on Wei[5].

[5] https://www.investopedia.com/terms/w/wei.asp (last accessed 26/02/2022)

Unit	wei value	wei	ether value
wei	1 wei	1	10^-18 ETH
kwei	10^3 wei	1,000	10^-15 ETH
mwei	10^6 wei	1,000,000	10^-12 ETH
gwei	10^9 wei	1,000,000,000	10^-9 ETH
microether	10^12 wei	1,000,000,000,000	10^-6 ETH
milliether	10^15 wei	1,000,000,000,000,000	10^-3 ETH
ether	10^18 wei	1,000,000,000,000,000,000	1 ETH

Table 1 - Sub-units of Ether

1.7 How the blocks are produced

In the Ethereum Blockchain there is not a regular size for the blocks, neither the blocks are being produced at specific times. However, they have the gas limit which limits the computing power that each block will need in order to be created as well as its size. The gas limit can change from time to time and does not have a specific value. It refers to the maximum quantity of gas you can spend on a certain transaction. A higher gas limits demands that it will need more computational power in order to execute the smart contract.

The time gap between two consecutive blocks is not fixed and it depends on the network. So, to calculate the block time, the following functions are being used.

$$blockTime = currentBlockTimestamp - parentBlockTimestamp$$

Equation 1 – Blocktime

$$currentBlockDifficulty = parentBlockDifficulty + \frac{parentBlockDifficulty}{2048} \times max\left[\left(1 - \frac{blockTime}{10}\right), -99\right] + floor\left(\frac{currentBlockNumber}{100000}\right) - 2$$

Equation 2 – currentBlockDifficulty

At this point it must be noted that the divisions are integers, and the floor size is defined as the largest integer that is less than the number contained [6] .

1.8 Smart Contracts

The term "smart contract" was first appeared in 1997 and it was used by Nick Szabo, longtime before the Bitcoin. He is a law scholar, a computer scientist, and a cryptographer and what he wanted to do was to use a distributed ledger to store the contracts. The smart contracts are somehow like the contracts that we use in real life, except the fact that they are entirely digital. Basically, a smart contract is a small computer program stored inside a Blockchain. They are immutable and by that it means that once the smart contract is created, it can never be changed from nobody. Moreover, they are also distributed and by that it means that the output of the contract is validated by every user on the network.

Ethereum was created and designed in order to support smart contracts, and they can be programmed in a programming language that is called Solidity.

Smart Contracts help you exchange money, music, real estate, videos, shares, or anything of value in a transparent way without differences, while avoiding the services of an intermediary [7].

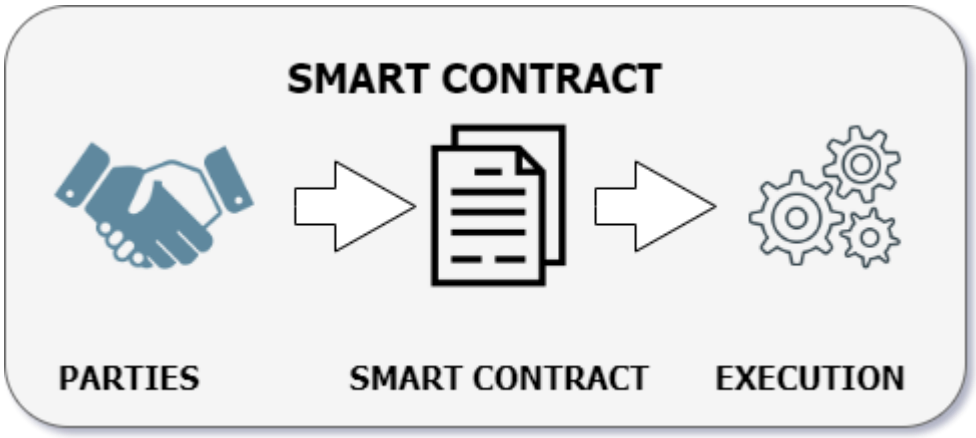


Figure 6 - Smart Contracts

1.9 Conclusion

Concluding this chapter, the general literature review of this research was analyzed and explained. Through the research carried out, the technology is now fully understood. The importance of the technology was emphasized, with references to the evolution of the World Wide Web and how it relates to the Blockchain technology. Furthermore, Ethereum Blockchain presented and all the technologies that are important in order to understand everything about the distributed network. In the end, a small presentation about how the Blockchain works was made in order to understand briefly everything and connect them with the chapters after this one.

2 The Blockchain technology in healthcare

2.1 Introduction

This chapter will cover health technology. What will be the benefits of introducing an application based on the Blockchain technology in the medical field. And of course, the difficulties and disadvantages it can bring to the sector are not overlooked. Finally, some applications that have been developed by various companies will be presented in order to facilitate the health industry.

2.2 Advantages of the technology in the field

A lot of opportunities in the health care system have been presented, and huge challenges for the doctors,the providers and also the patients and regulators of the healthcare, because of the AI (artificial intelligent) and the big amount of data that there are nowadays available. The growth of the technologies can make really big changes to the medical field, since they can convert the data of every person into data sources for prediction in the health care system. More specifically, most of the patients do not really know the meaning behind their medical files and they do not have control over the privileges of access to their data since these data can be really useful. That is why the Blockchain technology provides a lot of solutions and has a lot of advantages.

One of the most important benefit of the technology is the interoperability. The network can connect with multiple other systems with no restrictions, and it has the power to exchange various kind of information, data and use them according to their own needs. The electronic health records that we have nowadays are not interoperability and the cost of use is really high compare to what it can be done with the new technologies. In cases of huge emergency, that the patient maybe needs to get to the surgery most of the doctors do not have full access to important files, and there are cases of patients taking medicines that according to their records must not take. Even the costs of hospital systems are higher when there is no interoperability, since a lot of daily cases of unnecessary medication trials are recorded in several patients [8].

A health care system that uses the Blockchain technology in order to have a medical file for every single patient, with access to the doctors in case of emergency could be a big step in the medical field for a better health care system. The file could provide medical data from the beginning of their life until the end with all examinations, medications, vaccines, any surgeries or prescription and anything else that has happened to the health of the patient throughout his entire life.

The exchange of medical data is quite important but, the healthcare systems of today usually require patients to obtain and share their own medical history and records in other forms, either by physical paper copies or by electronic copies of some type of CD or USB stick. This process is inefficient and has some disadvantages. It must be mentioned that most of the times, is not safe to save your data this way because there is a big risk to lose them. Also, the process takes time, it is slow, and some data sometimes maybe missing.

Since the process is slow, a Blockchain technology application can be fast and flexible. This means that it can manage and monitor related health events in large populations of patients from any location in the world. For instance, let's say that a patient visits a doctor in another country for his own purposes, and simply due to the Blockchain healthcare application the doctor at this country can have his medical history despite the fact he is from another place on earth.

The fact that information could be available at all times makes the Blockchain a potentially autonomous approach to improving the health system and coordinating with doctors, pharmacists, insurance companies, etc., because previously they would communicate by telephone, email or in some cases with fax which takes quite long time.

So, the data are collected, validated and then the doctor can have quick and easy access via Blockchain to monitor and improve the health of the patient. Through the electronic health record management, the data of the patient and history are easily verified, and the doctor can really quickly decide the appropriate treatment that is needed in order to improve his health. These are achieved immediately, and from anywhere in the world, if there is access to the Blockchain network. Such a big change to the medical industry could bring better results especially reducing the time of emergency in the care centers.

When it comes to terms of research, Blockchain can have a key impact to the next generations clinical trials because it will be much easier for the researchers to collect specific data as a result of the technology and the way data been allocated. Nowadays, surgical and medical research burdened by the difficulty of generating large quantities of data for a significant number of patients. Blockchain technology could improve the overall exploration process at the implementation of the experimental work, and also by the modification stage [9].

Another important benefit of the Blockchain as an electronic health recording system is that it can be customized to be compatible with Big Data technology, as it is defined by the ability of saving and

analyzing massive and complicated information. Just take into consideration the amount of medical test, surgeries etc. someone has done throughout all these years of his life. Efforts are already being made by various organizations to create an electronic global health system, which can provide analyzing this massive amount of information. The use of this kind of technology can offer the discovery of new clinical models and the finding of the connection between various diseases and conditions. All this is possible as there is the ability of processing a really big amount of data of any kind. Furthermore, it must be taken into consideration, the fact that Big Data could also be very useful in assessing the overall health of a group of people or a population. Nowadays it usually runs in distributed databases, which are mostly superior to those of Blockchain as they have high-level of performance, lower latency, and higher capacity. Nevertheless, Blockchain databases have been created, which are compatible with Big Data analysis [10].

Another area that could benefit from the introduction of technology in the healthcare sector is the pharmaceutical sector. A very important problem that it has been observed, is the imitation of drugs. As it is already known, the transactions in a Blockchain system are recorded and unchanged, it is much easier to detect illegal dealers and drug suppliers. In order to avoid this, Blockchain healthcare secure private system in order to ensure the authenticity of the products. This will coordinate the private chains by a central authority, so if a particular distributor or producer has access to and distributes the drug, this will be proof that the product is genuine. When the drug is produced and a portion of it is sent for retail distribution, the data will be stored in the Blockchain. This will result to an easy verification of the course of the drug.

Perhaps the most important advantage of the technology is the security but also the transparency of the data. Blockchain technology, in addition to delivering comprehensive healthcare information, also maintains traceable records of distributed data and work. It is reasonable to note that the chances of data leakage without the authorization of the patient are nearly eliminated. Establishing unchangeable blocks where they will be informed of any changes to their healthcare records will eliminate the possibility of abuse.

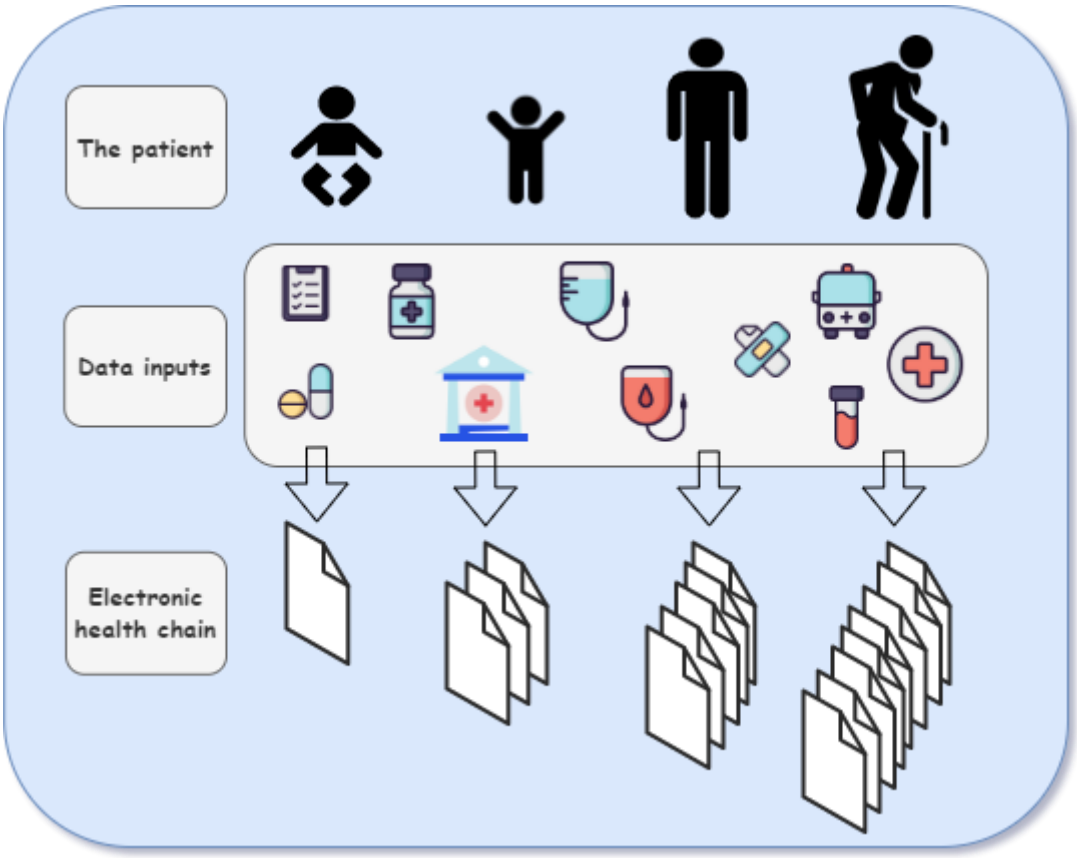


Figure 7 - Blockchain technology in health care

The above diagram saws how starting from birth, patients accumulate data from clinical encounters, pharmaceutical treatments etc. These data can be vaccination histories, pathology reports, etc. and each upload adds a new block to their electronic health chain.

2.3 Disadvantages of the technology in the field

One of the main and important benefits of the technology is that the main owner of the data, namely the patient can decide with whom he will share his files, so in theory there is respect for privacy and data. So, the trust that it must be created between individuals is the key motivator for them in order to participate in some clinical trials. The distrust that exists in today's society between the institutions, regarding the rights to information and respect for the privacy of the people, is very essential for the proper and organized method of consensus and certification of a Blockchain network. The moral perspective from person to person, is really different. Ethical tolerances differ, as there are many who want to have complete control and be responsible for their digital privacy and the transactions they have made in the past. As a result, they do not trust any doctor, pharmacist, hospital, etc. who will share their information with, fearing for what will happen next, since the levels of corruption in today's world are massive [11].

One of the most important features of Blockchain technology is that its network is unchangeable. This happens because as the database is being updated, no changes can be made to its data, there is no deletion or modification. The user can only add more data in the form of additional blocks to the existing chain. In contrast to a traditional database, that has the capacity to perform four basic functions in terms of its data: Create, Read, Update and Delete (CRUD). So, it can be easily understood that in cases of a human error correction is completely impossible, so all procedures must be done very carefully, so that there are no false and incorrect data of the patient.

In addition, it should be noted that such a project in order to be properly implemented in a country, it needs a lot of time, and also involves a fairly large cost. A Blockchain network should have an online platform for transactions to be done (Web Wallet), there is also a need for cryptography development and ICO (initial coin offering or initial currency offering). In an ICO, a big quantity of cryptocurrencies is sold in the form of "coins" to multiple investors, in exchange for legal money or other cryptocurrencies.

Taking into consideration what is mentioned above, specialized staff have to be hired who will know how to create such a system and manage it. Furthermore, a corresponding platform should be created, which will support all the devices. All of this has a fairly high cost, which most of the countries cannot easily cover.

Likewise, in a Blockchain system the necessary data storage space is significantly related to the cost. This has to do with the fact that each complete node must store more and more data at infinity, which is expensive. To conclude the storage part is a very important obstacle in the implementation of such an applications.

It should also be pointed out that there were some notable Blockchain security issues in 2021. In 2018, three cryptocurrency platforms, ZenCash, Verge and Ethereum Classic, experienced measure issues from 51% attacks[6]. Another impressive addition to Blockchain security problem refers to the vulnerability of the Blockchain endpoints. That refers to the fact that the blocks are safe against the hackers, but the wallet accounts are not always. There are also some third-party retailers that have significant impact for facilitating Blockchain transactions. But such types can increase vulnerability to hacking because they include Blockchain payment platforms, smart contracts, and payment

[6] https://news.bitcoin.com/bitcoin-in-brief-monday-zencash-targeted-in-51-attack-ticketfly-hijacked-for-ransom/ (last accessed 26/02/2022)

processors without having powerful security system. They are often noted fishing attacks. Sometimes hackers send emails to people who have wallet key, by posing as an authoritative source. These emails contain phony hyperlinks in order to steal the credentials of the user. When it comes to routing attacks, if they do not detect the attack really quick, considerable cost could be enforced. The last significant worry for security refers to transaction privacy leakage and by that it means that users when they want to make any kind of transaction, they must assign a private key. The researchers have found that over 66% of sampled transactions do not have any chaff coins or mixins, and these can restrict the ability of the hacker to define the coins spent in the transaction that these users want to make.

2.4 Applications in Healthcare

When it comes to healthcare there is a wide range of applications that some companies have created around the world. Some of them manage the medicine supply chain, other the secure transfer of the records of the patients, and others help researchers unlock genetic code. Some of them are the above[7]:

- **Akiri** is a Big Data company with a Blockchain application that operates a network-as-a-service, in order to safeguard the health records of their patients when they transfer them. They do not store the data, the system does the whole thing in real time, from adjusting policies and configuring data layers, to verifying the source of each data and also the final destinations.

- **BurstIQ** is a Big Data, Cybersecurity, Software company, which has a platform that helps healthcare companies in order to manage secure and safely vast amounts of the data of their patients. They use the Blockchain technology to upgrade the way healthcare documents and data is used and shared.

- **Factom** is an IT, Enterprise Software industry how helps the healthcare companies by creating products who store digital records on a platform that is based to the Blockchain technology. This platform is quite easy to use by hospitals and healthcare administrators. They also have security chips for every patient, which can hold information and store the data privately.

[7] https://builtin.com/blockchain/blockchain-healthcare-applications-companies (last accessed 26/02/2022)

- **Medicalchain** is Electronic Health Record, Medical industry that uses Blockchain to maintain the integrity of healthcare data while at the same time establishing a single point of truth. The system protects their personal information and id from hackers.

- **Guardtime** is a Cybersecurity, Blockchain industry who is helping governments and companies by applying the Blockchain technology into their cybersecurity methods. This company had a huge impact in the Estonia's healthcare system. By that, it should be mentioned the fact that Estonia uses the Blockchain technology since 2012, in order to secure medical data and process transactions.

- **ProCredEx (Professional Credentials Exchange)** is a Big Data company has created due to the Blockchain technology a ledger of medical credentials database that allows the data to be processed to meet uniquely shared requirements and organized by making the data eternally traceable and unchanged.

- **Avaneer** is a Big data company that is using the Blockchain technology to improve the healthcare system applying a public directory to support better claims processing, secure healthcare data exchange, and keeping and updating directories.

- **Coral Health** is a Healthcare, IT company that uses the Blockchain technology in order to automate administrative processes and to see better health results and speed up the care process. The company very quickly brings the doctors in direct contact with the technicians of the laboratories but also with the public health managers by entering the medical data of the patients in the distributed record technology. They also implement smart contracts between patients and doctors to ensure the accuracy of the data and treatments.

- **Robomed** is a Blockchain, Medicine company that uses Artificial Intelligent and Blockchain to offer to them a single point of care. They have developed wearable diagnostic devices, chatbots and telemedicine sessions to collect easily and fast patient's data in order to share them with his doctors. Robomeds Panacea platform want to lead their patients into a healthier everyday life be engaging them into specific smart contracts that give them multiple purposes.

- **Patientory** is a Blockchain, Cybersecurity, Healthcare, IT company that shares its data of the patient securely and efficiently by using end-to-end encryption. Their platform uses the Blockchain technology to transfer all information and give access to healthcare providers, patients and clinicians.

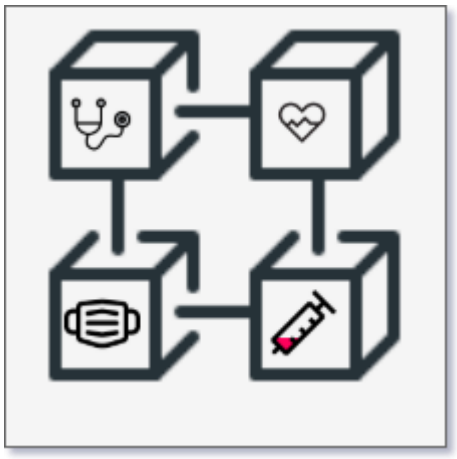


Figure 8 - Health industry and Blockchain

2.5 Comparison of the facts

The following features are considered to be essential elements of the technology in order for the network to function properly. One of the most basic is the common cryptography platform which ensures speed and flexibility with user login, using the private or public key. So, there is easier medical care. But it also has its drawbacks. Common platform means that any modification to the nodes by malicious attacks on the system will result in modification. Such attacks can target transactions of drug content or even payment with the immediate result of the loss of encrypted currencies. The network has the ability to record all data, which in terms of health research is equivalent to a huge amount of information and therefore easier grouping of information for faster results. The huge volume of data enables the application of Big Data technology. However, the storage space required is still huge. It then referred to the ability of the network to remain unchanged with the immediate advantage of data transparency. But the immediate negative effect of immutability is that in the event of an error due to a human factor, there are no correction options. A very important result of these smart contracts and system procedures is the security it provides. The authentication approval is done by each node and as a result another level of security is ensured to the system users. Equally important is the traceability of counterfeit and illicit drug trafficking. However, it is difficult for the competent authorities to have the right to use the keys to control the drugs.

2.6 Conclusion

Closing this chapter, it is fully understood that there will always be risks that must be taken in order to implement innovative ideas in each area. As far as the healthcare industry is concerned, since the advantages that technology can offer are numerous, it has been observed that there are many companies that have made great strides in the field and have developed such applications to provide

to the world a better health care system. So, the conclusion after the analysis of technology in the field of health is that the number of advantages is sufficient to overcome the difficulties that will arise in the implementation of such an application in the field of health and medical care. For this reason, below, in the following chapters, it will be a small implementation of a Blockchain application in the medical field, in order to show in practice how useful it is.

3 Tools and Technologies

3.1 Introduction

Starting off with this chapter, the most important tools and the technologies that had been used for the development of this web application will be presented. More specifically, some of the tools that Ethereum provides in order to implement the application will be presented for better understanding of the application. First, there is Geth, Ethereumjs, Web3, Solidity, NPM and MetaMask. After that, there is Node.js that is being used to communicate with the data base MySQL. Finally, a brief reference will be made to some of the key programs used.

3.2 Web Application

The basic idea is to implement a web application, which is software that runs on a web server. Access will be through the web browser. Such an application is programmed using a client-server model structure. A web server is a computer that stores, for example, HTML, CSS, JavaScript, and images. The Web API is an API (Application Programming Interface) for a web server or web browser.

3.2.1 JavaScript (JS)

JavaScript (JS) complies with ECMAScript (general purpose programming language) requirements. It is a high-level language, interpreted and based on multi-paradigm scripts. At this point it should be noted that along with HTML and CSS, it is one of the key technologies of the World Wide Web, as it provides the ability to build interactive web pages and is an essential part of web applications.

3.2.2 HTML

HTML, or HyperText Markup Language, is a markup language that defines the form of a web page. The basic building blocks of a website are its components which «connect» different parts of the content so that they act or appear in a very specific way.

3.2.3 CSS

CSS, or Cascading Style Sheets, is a style sheet language with which we can selectively format HTML elements in order to improve the appearance of the website and make it more beautiful and therefore easier to read by every visitor of the page.

3.3 Ethereum Blockchain

3.3.1 Geth

Geth is a command line interface, uses the programming language that is called Go for the implementation of the Ethereum node. It offers the possibility to anyone to mine ether, transfer ether between addresses, discover the Ethereum Blockchain, create a private Blockchain in it and also allows all the user to create smart contracts and send various and multiple transactions and much more [12].

3.3.2 Ethereumjs

Ethereumjs is a team whose main goal is to help developers create their applications and interact with the Ethereum network. They achieve that by building JavaScript tools implementing Ethereum APIs, protocols and technologies. They provide a lot of modules that really helps for the execution of Ethereum apps.[8]

3.3.3 Web3.js

It is a collection of libraries and the most important npm packages used for the implementation of each application. It is an interface that allows JavaScript to communicate with Ethereum. Libraries also enable the Ethereum Blockchain to interact with a local or remote node using an IPC, WebSocket or HTTP connection. It is one of the most well-known ways of referring JavaScript programming language to objects that exist within the Blockchain, such as solidity smart contracts, their functions, addresses and account balances, their data, etc [13].

3.3.4 Solidity

Solidity is a programming language that is used in order to implement smart contracts for the Ethereum Blockchain, and it is object-oriented. It must be mentioned the fact that is performed in Ethereum Virtual Machine (EVM). Its syntax is quite reminiscent of JavaScript that is why is easier to use from most of the people. By using Solidity, you can create contracts for users like crowdfunding, voting and multi-signature wallets, etc [14].

[8] https://ethereumjs.readthedocs.io/en/latest/introduction.html (last accessed 24/2/2022)

3.3.5 Remix

Remix is a Solidity IDE that interacts with the Ethereum Blockchain. It is accessible through a browser and is a complete environment used to develop smart contracts, compile them, and then build and execute them in the Blockchain.

3.3.6 MetaMask

MetaMask is a plugin accessible from browsers, like Mozilla Firefox, Brave, Google Chrome, and Opera. [15] It is a software cryptocurrency wallet that is used to interact with the Ethereum Blockchain. It gives the opportunity to users to interrelate with decentralized applications by having access to their online wallet through browser extension or a mobile application. At this point, it should be pointed out that the advantage it offers, is the fact that using it, and accessing these applications does not require running the full Ethereum node on the computer of the user, as required by the Ethereum-specific browser called Mist. Its creators claim that their main purpose is to make the Ethereum accessible to more and more people in the world. In this application the Ropsten Ethereum used because it is an Ethereum test network which is used to test the Blockchain application before deployment into the main Ethereum network.

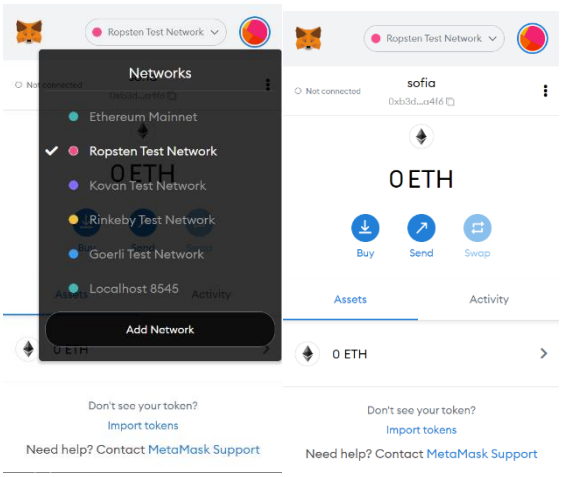


Figure 9 - MetaMask

3.4 Node.js Package Manager (npm)

It is the Node.js management program that manages JavaScript language packages. In the npm file, in addition to packages we will also find node modules. The node modules are applied in server-side programming. The module is a directory or a file that is uploaded by the Node.js with the definition require(). On the other hand the package is a file or a directory which is described by the package.json. It consists of three parts, the website, the command line client and the registry.

It is a really helpful tool that enables the user on one hand to exchange packages and on the other hand it has established specifications that are followed by all packages published in the file, in order to be fully understood by all developers.

3.5 Node.js

Node.js is a software development platform that is built into the JavaScript environment. Its main goal is to provide a much easier way to create scalable web applications. A node process relies on an asynchronous input-output communication model in contrast to most modern network application development environments. It uses an event-driven, non-blocking, I/O model and has high levels of efficiency using few resources. Apart from being an execution environment, it is also a JavaScript library.

Some of its most important features that makes it the best choice of software architecture are the above:

- License – MIT license released Node.js
- The applications that have been created with Node.js do not buffer data at all.
- Node.js uses a single threaded model but with highly scalable server. The event-driven programming helps out the server to respond with a program that does not block the execution of further operations. It also uses a program that is different from the traditional servers that they were used in the past, because it can provide service to a higher number of requests.
- When you want to execute a program, the process is really fast because it is being built on Google Chrome's V8 JavaScript Engine.
- Lastly, in the library the APIs are asynchronous, meaning that the server does not wait for the data to be returned by the API and it moves to the next one. This helps the server to communicate with the previous API to get a response by a notification mechanism of events of the Node.js.

3.5.1 Google Chrome's V8

The Google’s open-source high efficiency engine is written in C++ and JavaScript, and it is used by the open code browser Google Chrome, Node.js and to some other applications. It runs on Windows 7, 8, 10, macOS, and Linux systems that use x64, IA-32, ARM, or MIPS processors and also

implements WebAssembly and ECMAScript. It can be embedded into many C++ apps and furthermore it can run standalone.

For the present thesis, Nodejs was considered to be the appropriate tool for the rapid communication of smart contracts with the several pilot interfaces that allow the call or series of asynchronous recordings - calls of smart contract functions or simple functions.

3.6 MySQL

MySQL is distributed, developed, and supported by Oracle Corporation and it is one of the most popular Open-Source SQL database management system under the terms of the GNU General Public License [16]. A structured data collection specifies a database. These data could be anything from the costumer sales of a technological store with a lot of daily visitors to a big amount of medical information in a network. In order to "control" these data you need a MySQL Server because it is a database management system that gives the ability to the developer to have access, add and process the existing data inside the database. Some of the advantages of using MySQL are the following:

- On-Demand Scalability
- High Data Security
- High-level Performance
- Transaction Support is Comprehensive
- Round-The-Clock Uptime
- Workflow Control is Complete
- The Total Cost of Ownership is Reduced
- The Flexibility of Open Source is Significant

3.7 Conclusion

This chapter was all about introducing the Tools and the Technologies for a developer to make a Blockchain application. Also, the choice that was made for this research of the programming languages Solidity and JavaScript for building e Blockchain development and all the other Ethereum Blockchain that were mentioned before. Also, a small introduction was made to the database and other important tools to manage some important packages for this application.

4 Design and Implementation

4.1 Introduction

This chapter will present the design and implementation of the application developed for this thesis. It is called Healthchain and it is a web application that uses a Blockchain, smart contract system for secure health data sharing. The following is the main idea before the implementation of the application. After that, the most important implementations will be analyzed. Below you can see the architecture diagram and the main idea behind this application. Everything will be analyzed with details in the following chapters.

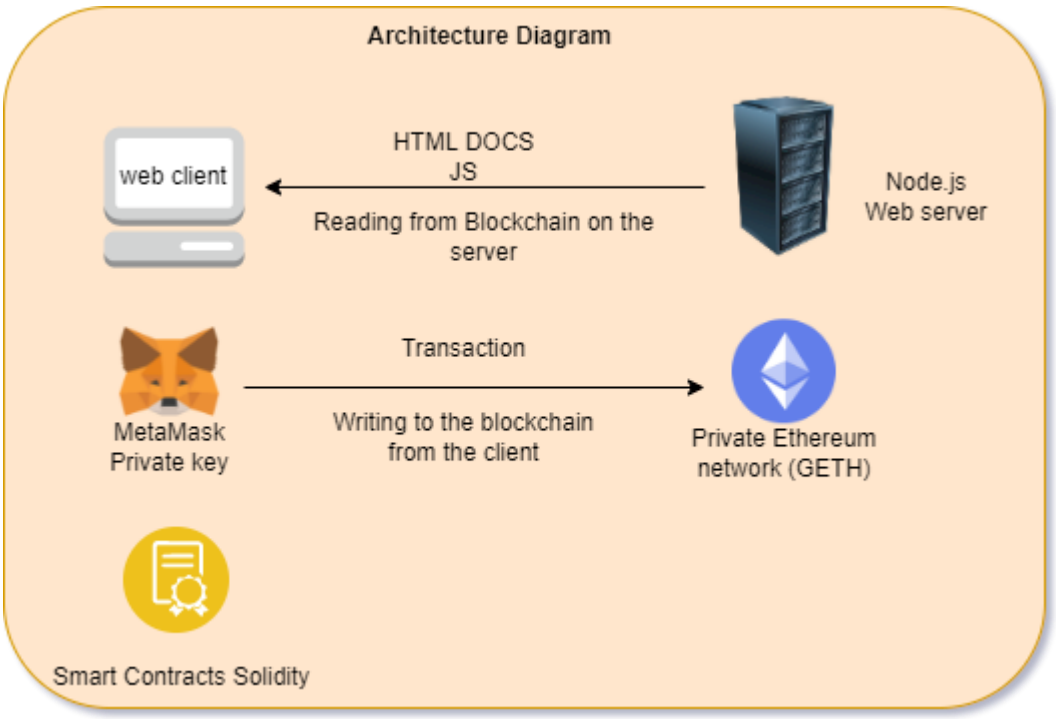


Figure 10 - Use case diagram

4.2 Smart Contract that was implemented

One of the most principal elements of this application was the creation of smart contracts. They are the main web of the application and contain the code that you run in Ethereum VM. When a Blockchain contract is created their code cannot be changed as it is final. As the contents of the Blockchain are unchanged, possible errors cannot be corrected. If an error is observed the only way to correct it is to create a new contract. That Is why their creation sparked a big interest.

This project runs in a private Ethereum network for Blockchain. It was developed a smart contract which was named as "healthchain.sol" and used in the creation of our application. The Solidity version that it was used was **pragma solidity ^0.5.0;**

Every user has a list of documents. A mapping structure was created for this cause in to order to provide to each user separate data storage.

```
mapping (address => string[]) public documents;
```

The addDocument function takes as arguments the medical records that the user adds to the system. So, this function is to add the request upload file for patient.

```
function addDocument(string memory documentHash) public returns (uint) {
   address from = msg.sender;
   // push returns the array length
   return documents[from].push(documentHash) - 1;
 }
```

The getDocuments function exist to get all medical records that are saved into the Blockchain for the user.

```
function getDocuments(address user) public view returns (string[] memory) {
   return documents[user];
 }
```

A user can specify, which doctors are allowed to view their medical records. It must be mentioned that access is granted when the user adds his address to a doctors list of patients. As soon as the user address is removed from the list, access for the doctor is revoked.

```
mapping (address => address[]) public doctorsPermissions;
```

This function was used to allow to a doctor to view all the patient's documents.

```
function giveAccessToDoctor(address doctor) public {
   doctorsPermissions[doctor].push(msg.sender);
```

```
}
```

If the patient wants to revoke a doctor's ability for viewing his data, this function is impending.

```
function revokeAccessFromDoctor(address doctor, uint index) public {
  require(doctorsPermissions[doctor][index] == msg.sender, 'You can only revoke access to your own documents.');
  delete doctorsPermissions[doctor][index];
}
```

Lastly the function that it was created to return all the patients addresses that gave the doctor access is the above.

```
function getDoctorsPermissions(address doctor) public view returns (address[] memory) {
  return doctorsPermissions[doctor];
}
```

In order to summarize what is the purpose of this contract, we will make a brief review of the things that happened above. For a start, as mentioned above it is written in Solidity programming language. In this contract, two mapping structures were created, one for the list of user files and another for the list of files that allows the patient to see the doctor. Then there are five very basic functions that execute the basic elements of the application. First is the insertion of a file in the Blockchain, then is the user getting all the files from the system, then is the ability for the user to choose which doctor will see his files, then is the revocation of the doctor's aptitude to see the medical data and finally the function that returns all patient addresses that have given access to the doctor.

Furthermore, it was also developed a Getweb3.js file and used in our Blockchain. Getweb3's role is to connect the front-end with the Blockchain network. As an example, when patient send the request about his disease to the doctor and asks for the treatment to the doctor, transaction emit and getweb3 runs, records is saved in private Ethereum Blockchain network.

4.3 MVC pattern

The application follows the design standard called MVC (Model-View-Controller) as it divides the application logic into three interconnected elements, the models, the projections, and the controllers.

This is chosen to be done, in order to separate the way they are presented to the user from the internal representations of information.

Models handle application data (storage, operation, change). There is a separate model for every single type of entity. The application includes the database of the models, records and users and the objects for each model are stored inside the database.

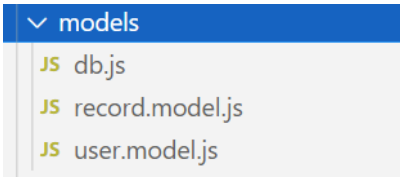


Figure 11 - Models

The views provide information to the user about the interaction. For each page, as well as for some reusable sections that appear in the application, there is a code file that is used to create them. For views, the JSX language is used in conjunction with HTML, JavaScript and CSS code for formatting. Some of the actions performed by the interaction of the user with the application correspond to the controller function call, which in turn calls other views to display several information.

Finally, the controllers interfere with the way the projection and the model interact. They call an action when the user interacts with a specific view, and every action is described by a specific function and there is also a separate function for each action of the controller. They are responsible for accessing information, identifying projections, and providing data.

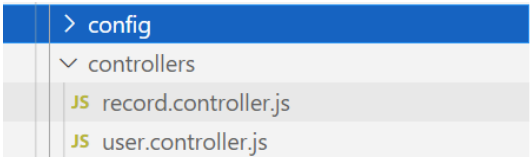


Figure 12 - Controllers

4.4 Front-end and Back-end development

Firstly, the front-end part of the project is related to the part of the code located in the client folder. It contains the nod_modules, public, src (source) folder and auxiliary files. The basic and most important part is source because it contains the actions, the components, the smart contract, the

images, the reducers, utils, App.js, etc. The steps that are followed to run our program properly are the following.

To begin with, the project runs from the **index.js->App.js>components/Layout/Landing.jsx**. Next there is the dashboard page from where the user can click the login button, and this runs from the code that is in this path **components/auth/login.jsx**. Also, in the dashboard page there is the register click that runs from the code in this path **components/auth/register.jsx**. More specifically, the component folder contains all the basic parts of the Blockchain application such as the login, register, patient, doctor, and manager part.

Secondly, the back-end part of the project is related to the part of the code located in the server folder. Node.js is the foundation on which the entire server side is built. At the same time, with the use of npm, many basic and complementary functions are introduced. Receiving and managing requests to and from the server is very important. Moreover, when it comes to the back-end part of the Blockchain application, it means that the back-end part carries out the request from the front-end with the database.

This part also contains the nod_modules, src (source) folder and the auxiliary files. The source folder is config, controllers, the middleware, the models, and the routes. The config folder is the one that carries out configure the database for the MySQL. There is also the controllers folder, that as it was mentioned before, it carries out to receive the request from the front-end and sends the models part. Moreover, in this part, there is also the models folder, that it was analyzed before, that receives the request from the controllers and then carries out the data to database i.e. save the data, delete, update, and get functions. Lastly, there is the routes folder that controls the url with request from the front-end.

4.5 Explanation of the database.

MySQL was used as a database where username is root with a secure password. The database name is healthchain and contains the users table and record table.

The table of the user saves the information of the user, and by that it means that it stores the personal information of patient, doctor, and manager.

No	Name	Type	Length	note
1	Id	Int	11	Unit key id
2	Email	varchar	255	User's email
3	Name	varchar	255	User's name
4	Password	varchar	255	User's pass
5	Address	varchar	255	User's wallet address (MetaMask)
6	Depart	varchar	255	User's job (patient, doctor, manager)

Table 2 - Database table of the user

Then there is the table of record, that contains all the request information and state.

No	Name	Type	Length	note
1	Id	Int	11	Unit key id
2	patient	varchar	255	Patient name
3	description	varchar	255	Disease name
4	value	varchar	255	Treatment value (ether val)
5	recipient	varchar	255	Doctor name
6	Approval_count	varchar	255	Doctors approve
7	Approve	Varchar	255	Managers approve
8	Finalize	Tinyint	255	Patients approve (transaction state)

Table 3 - Database table of record

At this point it must be mentioned that for the wallet of the user MetaMask's Ropsten test network was used because it is an Ethereum test network that allows the developers to test their Blockchain development, before they are ready to deploy it into the Mainnet, the main Ethereum network. This network was used because this project has no commercial purposes but mainly educational

4.6 Conclusion

Creating this application was quite challenging, but after researching and understanding the technology everything seemed much clearer. The first contact with the creation of a smart contract

and its implementation was something new but it was successfully carried out. In the end something a little bit tricky was to connect the front-end and the back-end development of the app,but everything was under control and after many hours of work everything was connected and the application took form.

5 The Healthchain application

This particular chapter will start with the overview of this application, the idea behind it and how all the technologies were used in order to implement this application. Then, there will be a step-by-step presentation of all the functions and capabilities provided by the application to each user and how users "communicate" with each other.

5.1 Overview of the application

The Healthchain is a system that helps companies, doctors, or patients to apply for multiple health procedures and moreover to be part of a secure and transparent environment in which all of the transactions are securely monitored by the Control Authority of the System. It was implemented by using Node.js and MySQL. Every user can enter the application from his own browser wherever he is. If a patient, a company, or a doctor wants to use the application, he must create a new account and after that he can log in using his own credentials.

In order to register in the application, the user must create a profile in MetaMask and have a personal email. If the user wants to sign up, he must provide a specific address manually created by MetaMask and document that confirms that this address is owned by the specific user.

The control authority of the system is in control for every part of the application. It acts as the administrator of the system and is responsible of creating campaigns for all the users. For abbreviation purposes we will refer to the control authority of the system as MOH. It should be mentioned that a campaign is the core of this system, and it is a contract that the manager creates.

Users can apply to campaigns by filling the correct form and in order to receive some data the campaign is implying. Likewise, only MOH has the ability to produce a new campaign. Every campaign has its own exclusive address and that is happening because it has to stand up from all the other campaigns and in order to be shown in the hash tree without a non-member or a hacker can see the transaction between the MOH and the entity that has made the requested.

The request has its own unique address, it is made when a user gives the appropriate paperwork, and after that the MOH can accept either reject the users request, depending on the paperwork. Every campaign is addressed to a very specific task. Only companies can apply to a campaign of the company, and the patients can only apply to a campaign addressed for them etc. This is because every account has different benefits.

The MOH has to create the particular template for a request to be made when a new campaign is created. This is going to happen by a specific dropdown menu from which the users of the system must choose their preferred health transaction.

MOH has the ability to reject or approve a request. When a request is approved or rejected, it is saved on the hash tree of the application. It must be mentioned that it is also saved in the private Ethereum Proof of Authority (PoA) Blockchain network as a transaction.

The PoA Blockchain is a network created to store the requests made by user and it is created by Geth**.** As it was mentioned in the previous chapters, Geth is responsible in building your own local copy of the network state of the Ethereum. Furthermore, it is really important the fact that the Blockchain application also requires a hash tree. As it was mentioned at the beginning of this thesis, hash tree is a list of requests everyone can see but has an address encryption in order to be unable to track and it is very secure. Every request that is made, is stored in this list. It has these specific values.

- The address of the campaign in which the request has been created
- The address of the request for users to find their own transaction.
- The result of the request (approve or reject).

5.2 Usage Manual

Since all the important parts of this applications have been analyzed, it is time to see how it actually works. This application runs localhost and does not have a domain name because it has been created only for educational purpose.

First of all, the user must own a MetaMask, as it was mentioned before. Then the user has to click the button of ‘add extension’, in order to add the Ropsten Test Network.

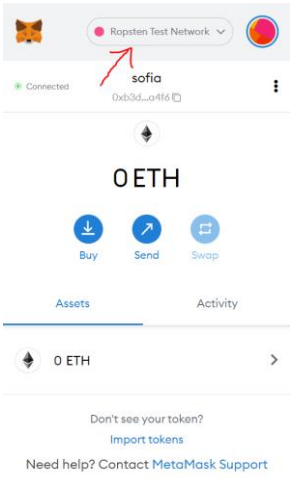


Figure 13 - MetaMask login in

When our project runs with the methods mentioned in the previous chapter, dashboard page appears as it is sawn below.

The source code url is **HealthChain\client\src\components\layout\landing.js**

From this page the user can login or sign up.

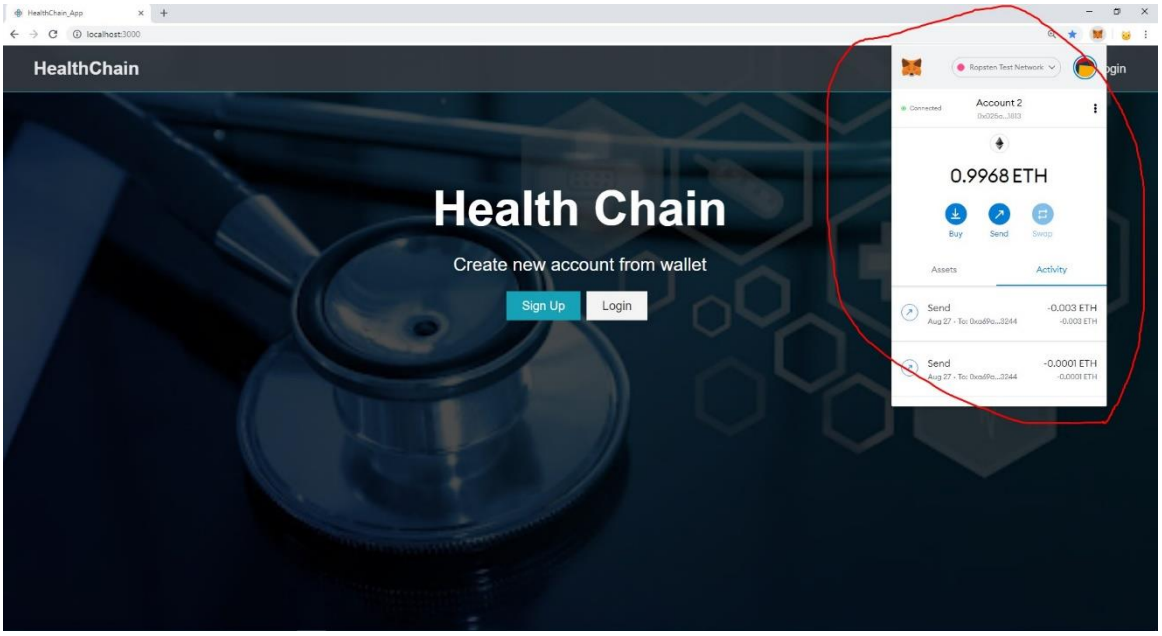


Figure 14 - Homepage

If the user does not have an account, he has to create a new one. He has to click the sign in button, and then the sign in page appears.

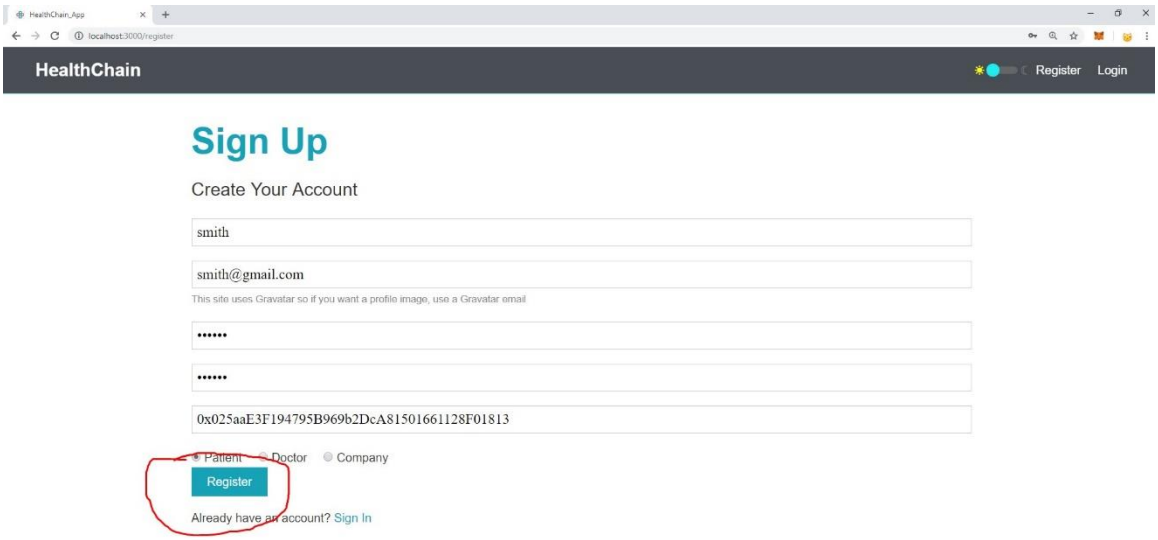


Figure 15 - Create an Account

In this part the user has to input the username that he wants to use, his email, a preferred password and his attribute (patient, doctor, company). At that time user wallet address inputs automatically.

The source code url is **HealthChain\client\src\components\auth\Register.jsx**

After the user inputs all of the data that the application asks him to do, he must click the register button and finally the user's information saved at the database table.

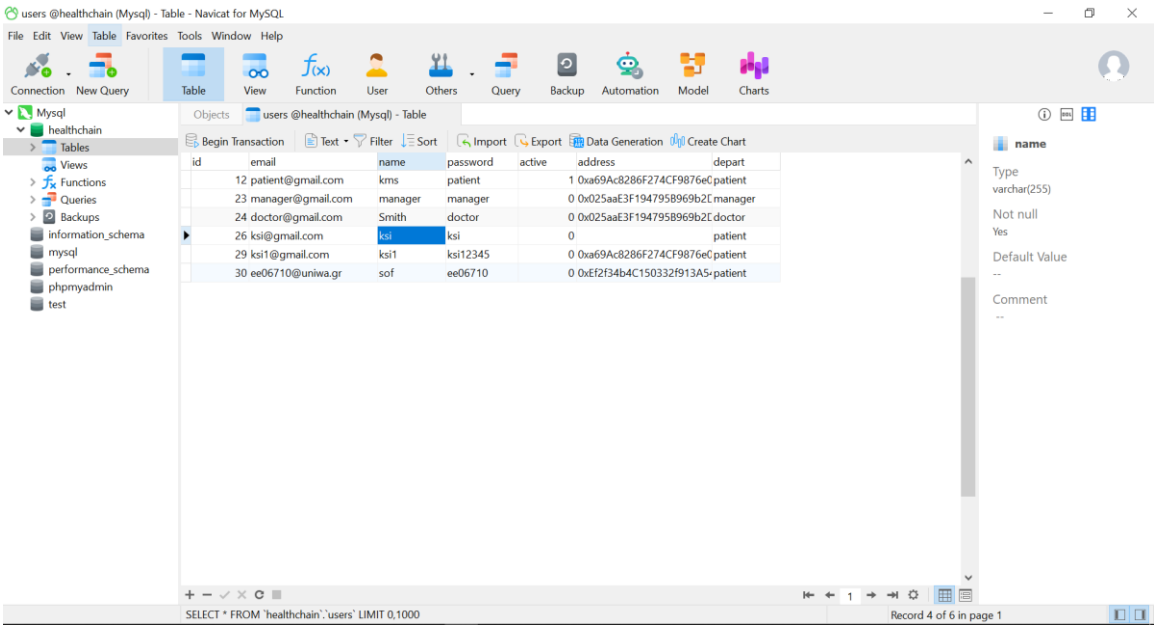


Figure 16 - Database (Users)

When register success, login page is appeared.

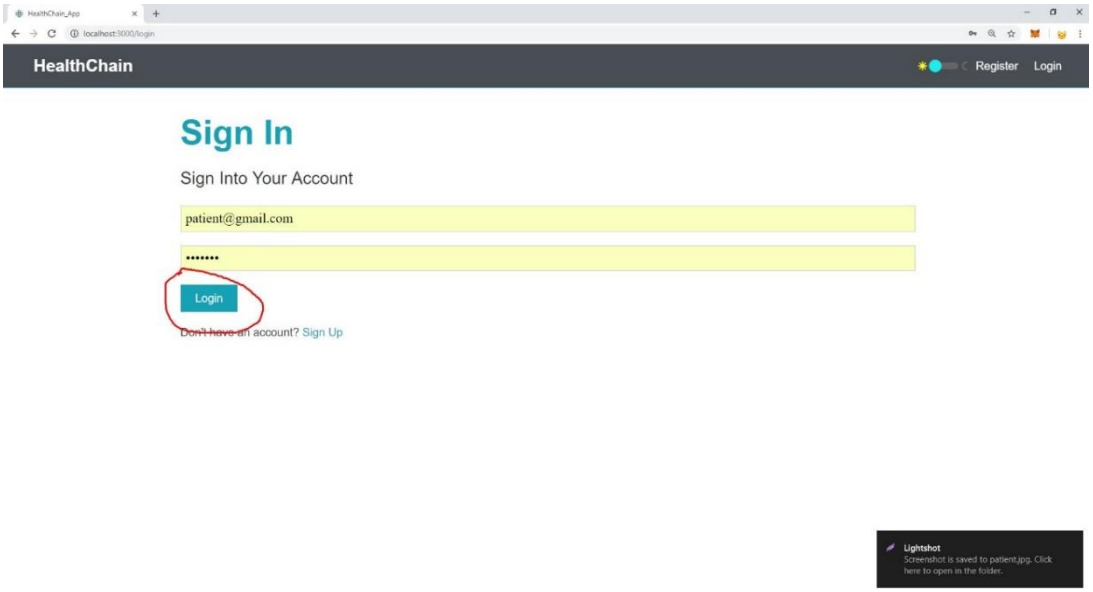


Figure 17 - Login

At this point, when the user clicks on the Log in button, log in page appears. The user has to input his email and password and click on the Login button. If he has already been saved in the database table, with his attribute, the suitable page appears.

For instance, if the user is patient, the patient page will appear. If the user is not saved in database table, error message will appear, and the user must by register to the application.

The source code url is **HealthChain\client\src\components\auth\Login.jsx**

If the user is a patient this is what appears to his page.

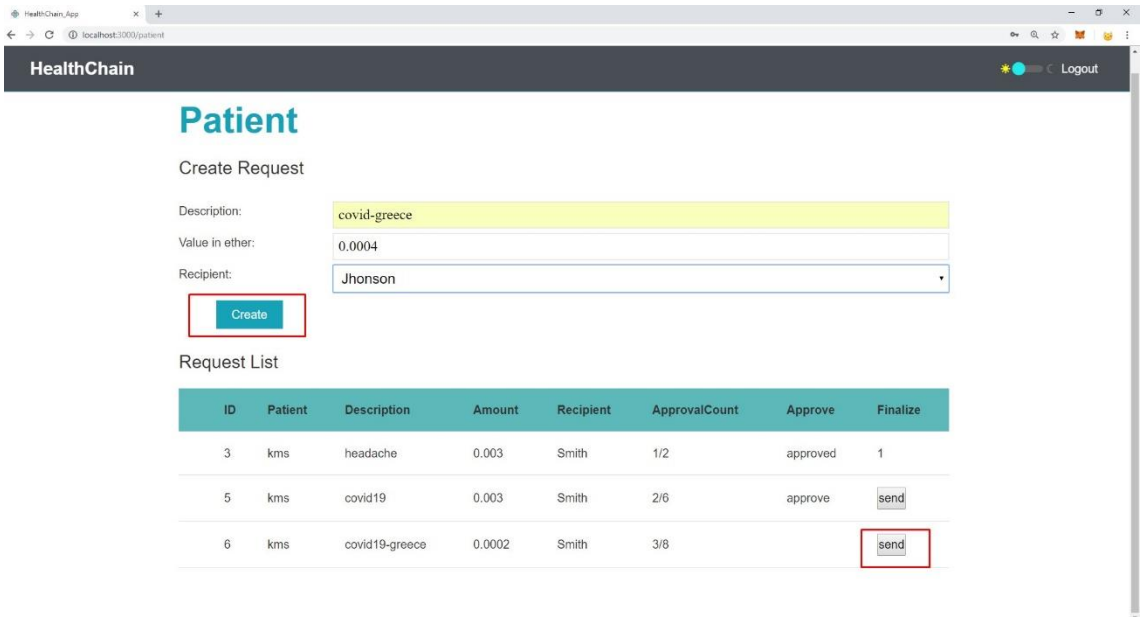


Figure 18 - Patient's Page

When the patient creates request, user input description about disease, value in ether, doctor name and them he clicks on the create button. And then, the request is saved in database record table as it is saw below. The source code url is **HealthChain\client\src\components\ patient \ patient.jsx**

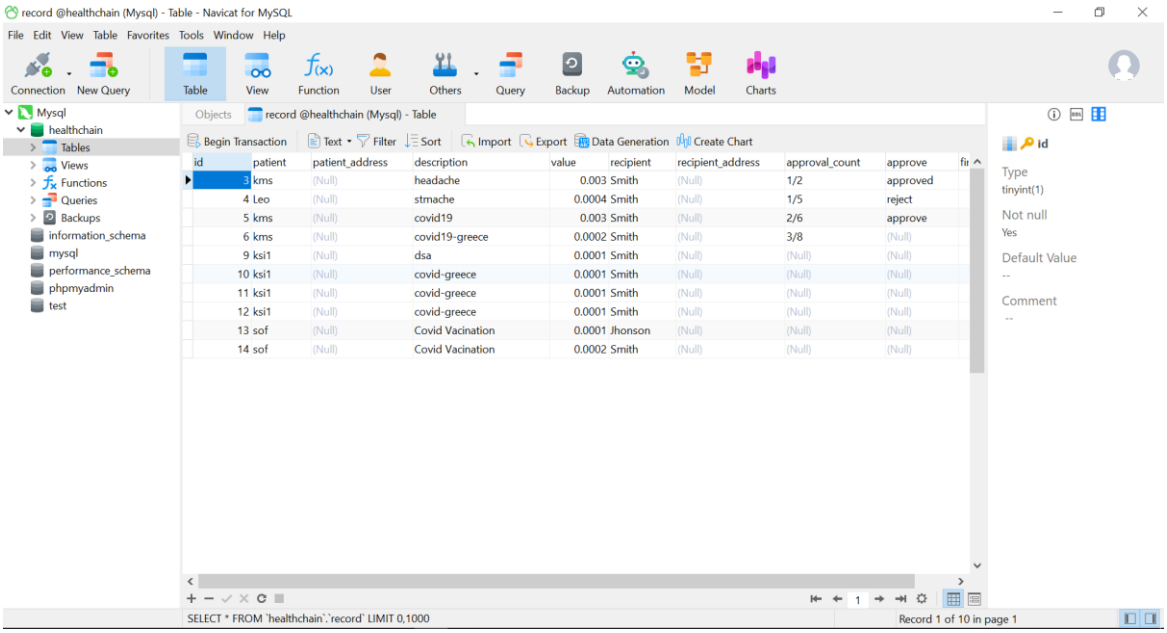


Figure 19 – Database (Records)

There is the Request List part which completes the transaction for smart contract. So, the request which patient sent before, is approved by doctor, manager and the patient emit the transaction, and

then the ether transfer from patient address to doctor address is done. In order to be fully understood, when the patient press the send button, smart contract connects MetaMask and sends the amount(ether) to doctor's wallet address on a Private Ether Network.

Healthchain.sol(smart contract)-> **HealthChain\client\src\contracts\healthchain.sol**

On the other hand, when the user is a doctor, the request list appears with the doctor's name. The doctor checks the request from the patient, and if it is possible, input the value into "ApprovalCount" field and clicks on the add request button.

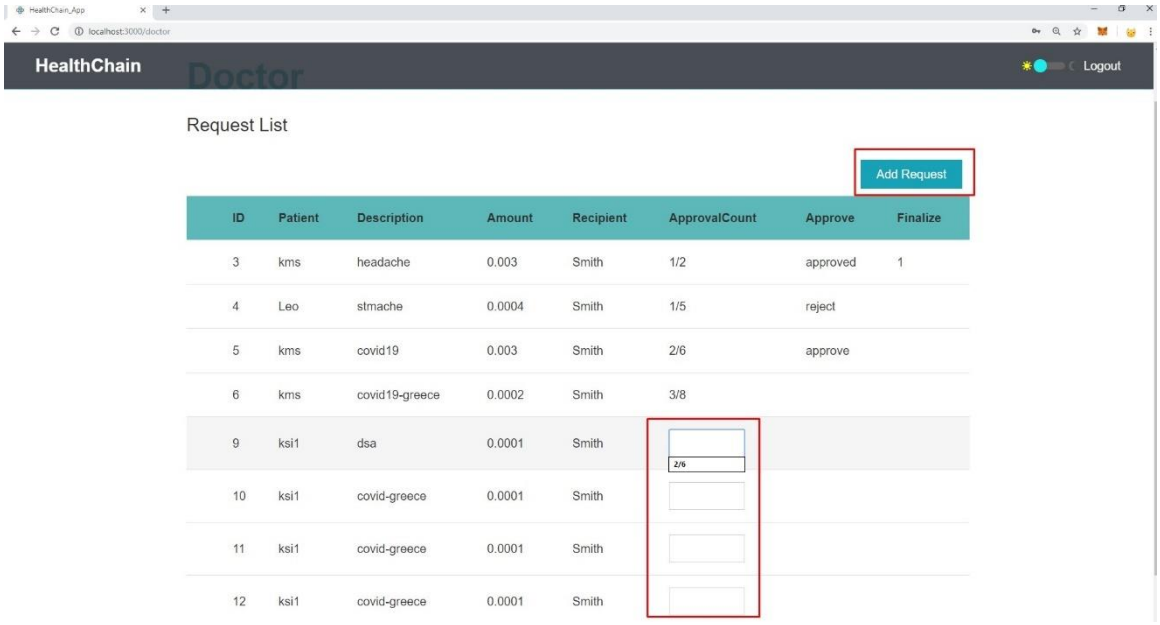


Figure 20 - Doctor's Page

The source code url is **HealthChain\client\src\components\ doctor \ doctor.jsx**

Lastly if the user is a manager (company) the following page appears.

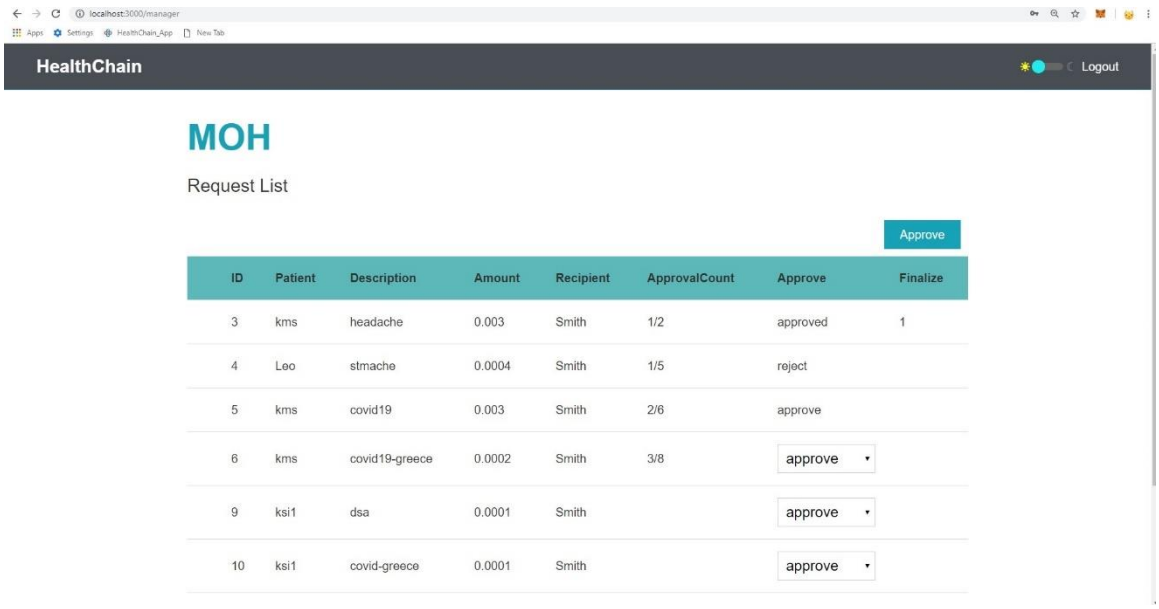


Figure 21 - Manager's Page

The manager who has been named as MOH, as we mentioned before has to carry out the approval or the rejection of the request that the patient and the doctor has made. If the request from patient and doctor is possible, manager check it and approve or reject, and click the "Approve" button. After manager approves the request, patient can emit the transaction and run the smart contract for the Blockchain.

The source code url is **HealthChain\client\src\components\ manager \ manager.jsx**

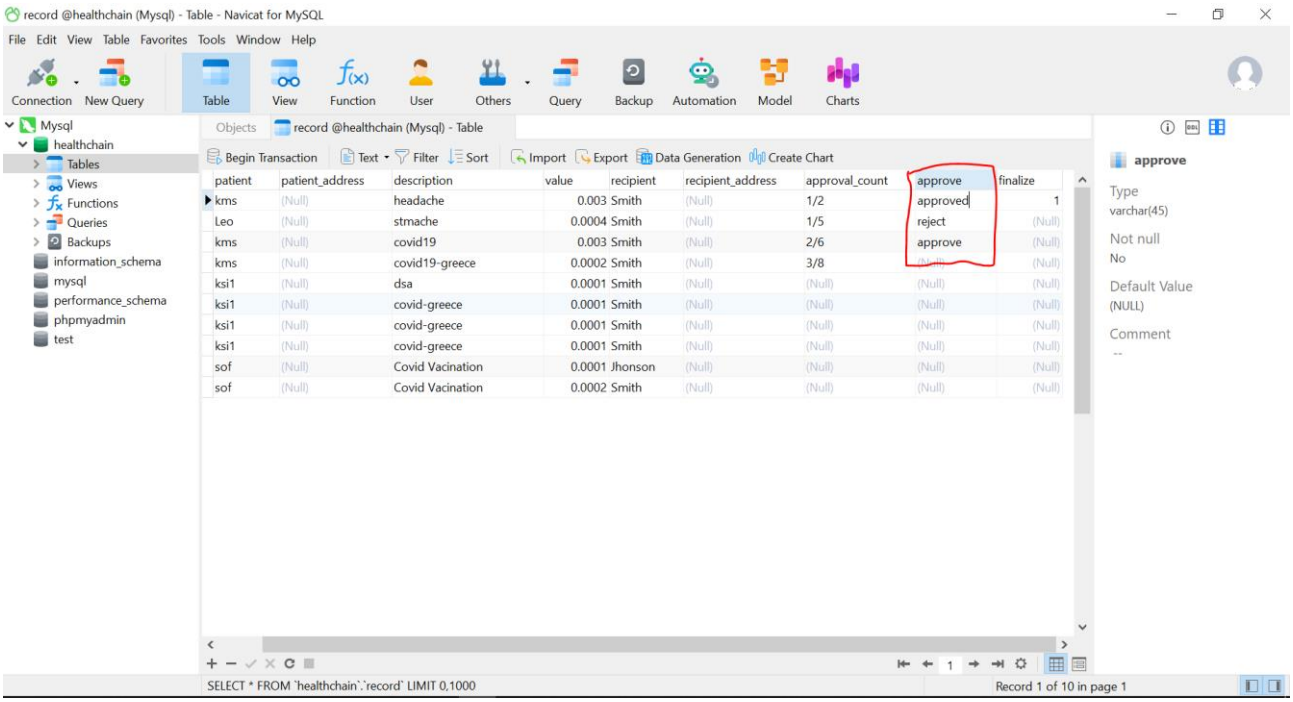


Figure 22 - Approved and Rejected Requests

5.3 Conclusion

After the detailed study of what was mentioned in this chapter and the detailed explanation of all the procedures that can be performed in the application, it is observed that its use is quite easy for any type of user and can be seen quite useful in today's society. This application has a purely educational and not commercial orientation, but such an application in the field, especially in our country, could be quite useful.

6 Conclusion and Future Goals

Blockchain technology works with encryption and is a distributed network. Its goal is to provide anonymity, security, privacy, and transparency to all its users. It also aims to directly assist the research sector and improve the quality of design models treated. The results of the research showed positive signs for the application of encrypted technology in medical care since the applications that already exist in the field are several. The purpose of the thesis was to build a tool that will help brick doctors and patients to have easier communication regarding the medical data of the consumer. As it turned out the results were positive

To meet operational and non-functional needs, as well as to design the application to be easy to use, took a process of months, which included continuous code development, research, and continuous code snippet reconstruction. The most demanding part of the process was understanding the operation of Blockchain and smart contracts. Another challenging part of the application was the correct appearance, processing, and addition of functions in order to make it easy to send patient requests to the doctor and the correct storage of data in our database.

In conclusion, the complete construction and maintenance of a large web application with back-end, front-end and a database closely linked to the other two parts, proved to be extremely interesting and useful. It proved to be quite demanding, and required many hours of work, combined with a good knowledge of the technologies used.

One of the original ideas was for each user to be able to upload the entire medical record as it is, whether it is a medical diagnosis, an x-ray or even the prescription of a doctor. In addition, its application in real conditions would be the ideal scenario in order to see that it is really functional but useful in the medical field, especially in times of crisis. But such a thing at the moment is just a future goal.

7 Bibliography

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, pp. 6--14, 2018.

[2] . B. Pon, "Blockchain will usher in the era of decentralised computing," *LSE Business Review*, 2016.

[3] D. Vuji, D. Jagodi and S. Ran, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *17th international symposium infoteh*, Jahorina, 2018.

[4] J. Lopez and . R. Dahab, "An overview of elliptic curve cryptography," 2000.

[5] A. Gervais, K. Wüst, G. O. Karame, V. Glykantzis, H. Ritzdorf and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016.

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, pp. 1--32, 2014.

[7] B. K. Mohanta, S. S. Panda and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018.

[8] P. Zhang, D. C. Schmidt, J. White and G. Lenz, "Blockchain technology use cases in healthcare," in *Advances in computers*, Elsevier, 2018, pp. 1--41.

[9] S. Khezr, M. Moniruzzaman, A. Yassine and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied sciences*, p. 1736, 2019.

[10] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proceedings of the International Conference on Data Processing and Applications*, 2018.

[11] S. Alla, L. Soltanisehat, U. Tatar and O. Keskin, "Blockchain technology in electronic healthcare systems," in *IIE Annual Conference. Proceedings*, 2018.

[12] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2017.

[13] W.-M. Lee, "Using the web3. js APIs," in *Beginning ethereum smart contracts programming*, Apress, Berkeley, CA., 2019, pp. 169--198.

[14] C. Dannen, "Introducing Ethereum and solidity," Berkeley: Apress, 2017, pp. 159--160.

[15] W.-M. Lee, "Using the metamask chrome extension," in *Beginning Ethereum Smart Contracts Programming*, Apress, Berkeley, CA, 2019, pp. 93--126.

[16] P. DuBois, MySQL, Pearson Education, 2008.