Arab International University

Faculty of Informatics and Communication Engineering

Senior Project Report on

Increasing the security and reliability of e-health system using Blockchain technology

Submitted to

Department of Informatics Engineering

in partial fulfillment of the requirement for the Degree of Bachelor in

Informatics Engineering

Submitted by

Salwan Arar **Sham Al-Boukaee** **Yara Saab**

Under the Supervision of

Dr. Sira Astour **Eng. Ali Ali**

August_2021

Aug 2021

Faculty of Informatics & Communication Engineering

CERTIFICATE OF APPROVAL

The undersigned certify that they have read and recommended to the Department of Informatics Engineering for acceptance, a project report entitled Increasing the security and reliability of e-health system using Blockchain technology Submitted by: Yara Saab, Sham Al-Boukaee, Salwan Arar in partial fulfilment for the degree of Bachelor of Engineering in Informatics.

Supervisor	**Head of Department**
Dr. Sira Astour	**Dr. Said Desouki**

Arab International University

The Arab International University (AIU) is a private Syrian university established in 2005. Its academic plans and the documents issued by it are approved and certified by the Ministry of Higher Education in the Syrian Arab Republic.

The university works to achieve the following goals:

- Preparing a distinguished generation of university graduates who are able to meet and advance the specific needs of society.
- Contributing to theoretical and applied scientific research that serves the purposes of national development. Work is being done to urge professors and academic staff to scientific research and participate in conferences and seminars that organize research.
- Achieving partnership with prestigious Arab and foreign universities with the aim of continuous development and modernization of academic work and conducting joint scientific research.
- Attracting distinguished academic and research competencies by providing the appropriate environment for their work.

The Arab International University is one of the first Syrian universities that have been established and inaugurated. It has been able to attract distinguished educational, research and administrative competencies, to create an integrated edifice from the academic, organizational and administrative aspects. It was able to graduate cadres of distinguished innovators by providing an educational environment based on unique qualitative and material ingredients, including:

- Modern and advanced study plans based on the credit hour system.
- Carefully selected educational cadres.
- Modern scientific laboratories and a laboratory for electronic libraries.
- Physical and moral incentives for students.
- Application of interactive teaching methods.
- Academic and educational guidance and counseling.
- A wide range of scientific cooperation agreements with local, regional and international universities of reputable reputation.
- Multiple agreements and memoranda of understanding with many civil society organizations.
- A proper campus with all the facilities of science, sports and entertainment, which we encourage you to visit and learn about their features.
- Student activities and clubs of all kinds: athletic, cultural, scientific and social.

The Arab International University life years are a time to invest in a student's future. The knowledge and experience that students acquire in the lecture hall and laboratories will help them in developing themselves. They will provide them with reasons for success in the chosen specialty. The student activities will help in expanding students' horizon. The activities of training, clubs and sports will enable students to develop their talents, and may even help in discovering new talents.
Students could invest time, mind and spirit in our university in order to reap the benefits of works and the time devoted in the coming years. We will be by our students in every step of their way.

Acknowledgements

It gives us immense pleasure to express our deepest sense of gratitude and sincere thanks to our highly respected and esteemed guide Dr. **Sira Astour** for her valuable guidance, encouragement and help for completing this work, her useful suggestions for this whole work and cooperative behavior are sincerely acknowledged. Her continuous support, immense knowledge and plentiful experience have encouraged us in all the time of this project.

We are also grateful to Eng. **Ali Ali** for his constant support and guidance.

At the end we would like to express our sincere thanks to all our families, friends and others who helped us directly or indirectly during this project work.

Abstract

The Blockchain technology is the buzzword of the year, and as this new technology slowly matured, it seems clear that from banking to supply chain logistics, it is ready for disruption. And in healthcare in particular, there is a massive opportunity for blockchain revolution to disrupt and lead the digital transformation. From medical records to pharmaceutical supply chains, to smart contracts for payment distribution, there are a plenty of methods to leverage this technology. Thus it has reached a great boom in the health sector, due to its importance to overcome interoperability and security challenges of health records systems in e-health. Medical records contain critical, highly sensitive private healthcare information, and the need to be frequently shared among peers, the idea of our project is born, which no one can own your data will be distributed between nodes and entities, and it is immutable so no one can change your data. Therefore, all the hospitals can share data on decentralized database, you have only to change or access to data.

Keywords

Blockchain, Ethereum, Smart Contract, Solidity, E-health, Healthcare, Cryptocurrencies, Cryptography, Security, …

Contents

Table of Figures

Abbreviations

AIU	Arab International University
BC	BlockChain
SC	Smart Contract
PoW	Proof of Work
PoS	Proof of Stake
EVM	Ethereum Virtual Machine
NPM	Node Package Manager
EHR	Electronic Health Records
Dapps	Decentralized applications
SHA-256	Secure Hashing Algorithm, 256-Bits
BTC	Bitcoin
P2P	Peer to Peer
ABI	Application Binary Interface
Solc	Solidity command line compiler

VOCABULARY DEFINITIONS

Ledger

Is the system of record for a business. Businesses will have multiple ledgers for multiple business networks in which they participate.

Transaction

Is an asset transfer onto or off the ledger.

Contract

Sets the conditions for the transaction to occur.

Centralized

Data networks are those that maintain all the data in a single computer, location and to access the information you must access the main computer of the system, known as “server”.

Distributed

A data network works as a single logical data network, installed in a series of computers known as “nodes” located in different geographic locations and accessible by multiple people.

Introduction

Cryptocurrencies are a form of digital or virtual currency that run on a technology known as blockchain. Cryptocurrencies are immune counterfeiting, don't require a central authority and protected by strong and complex encrypted algorithms. Blockchain can be described as a collection of records linked with each other strongly resistant to alteration and protected using cryptography. It is also called distributed ledger so a hacker will not be able to alter the data in the blockchain because each user has a copy of the ledger, the data within the blocks are encrypted by complex algorithms. We can implement on public blockchain or private blockchain, the public type is permissionless. That is anyone can join the network and read, write or participate within the blockchain. As well decentralized and that's way, it does not have a single entity which controls the network. Bitcoin and Ethereum are well known examples of public blockchain. On the other hand, the private type is permissioned blockchain that is, works on the basis of access controls which restrict the people who can participate in the network, thus only the entities participating in a transaction will have a knowledge about it, whereas others will not be able to access it. These permissioned networks will soon directly or indirectly influence every facet or human enterprise.

Chapter 1: Project Description

1.1 Background

With the evolution of the Internet of Things and overflow of health devices and health apps, a vast amount of medical data is recorded and transferred every day. This large database of medical information needs management regarding privacy, security, and availability. Hospitals and doctors need to access to the patient's medical information during the treatment process while ensuring security and privacy of sensitive information of patients as they share them with hospitals and medical institutes. Additionally, according to the Health Insurance Portability and Accountability Act, law enforcement and other specific public agencies may legally access health information. It is estimated that as many as 150 to 400 individuals may access a person's Electronic Health Records (EHR). Given that the data is shared widely and stored in multiple places, securing it becomes a more significant issue.

Blockchain Technology introduced a financial application that has started a revolution in many fields including healthcare information systems. Blockchain technology can provide a solution that not only helps to secure recording
and sharing of medical records but also to assure the privacy of each patient's data by giving their medical data ownership to the patients, themselves.

1.1.1 Overview

Blockchain allows every client in the network to reach consensus without ever having to trust each other. The idea behind blockchain technology was described as early as 1991 when researcher's scientists Stuart Haber and W. Scott Stornetta introduced a computationally practical solution for time-stamping digital documents so they could not be backdated or tampered with. The system used a cryptographically secured chain of blocks to store the time stamped documents.

1.1.2 Domain

Blockchain assures safety storage, management and delivery of healthcare data. Use of blockchain and healthcare is making diagnosis and treatment effectively by safe and secure data sharing.

1.2 Problem Statement

The healthcare industry is drowning in data, clinical trials, patient medical records, complex billing, medical research and more. Adoption and implementation of blockchains will be and evolution over time as blockchain applications are vetted and adopted. Therefore, this technology solves many issues that plague the industry today, to create a common database of health information that doctors and providers could access no matter what electronic medical system they used, higher security and privacy, less admin time for doctors so there's more time to spend on patient care, and even better sharing of research results to facilitate new drug and treatment therapies for disease.

1.3 Project Objective

The objective of the project is build an e-health system to make it more secure by using blockchain technology that manages electronic medical records data, protection of healthcare data and personal health record data management. Empower patients to be the center of their own health record so that, the patient doesn't have to rely on different institutions or hospitals they might visit.

1.4 Project Scope

Our proposed system uses blockchain technology to create a healthcare ecosystem that is iterative, scalable, secure, accessible and decentralized. This would allow patients to exchange their medical records freely and safely with doctors, hospitals, research organizations and other stakeholders-all while maintaining full control over the privacy of their medical data.

1.5 Project Features

Patient records own data and healthcare provider can access this data within minutes.

Places all patient health data into one accessible form.

The data was accessible to and controlled by the patient.

Using our application, the patient can record data and send it to healthcare providers in minutes no matter the distance between the patient and the provider.

1.6 Project Feasibility

1.6.1 Technical Feasibility

The project is required to have a mobile application to initiate and maintain a blockchain framework and database to save and update medical records that accessed by system.

1.6.2 Economic Feasibility

Have the potential to reduce or eliminate the friction and costs of current intermediaries. In the long term, a nationwide blockchain network for electronic medical records may improve efficiencies and support better health outcomes for patients.

1.6.3 Schedule Feasibility

Facilitate the process of transferring health information by making electronic medical records more efficient, disintermediated, and secure.

1.7 System Requirements

Understanding the Blockchain technology from scratch, building the smart contract to allow records and information to be stored on a digital ledger, managing patients' health information, records and data, learning solidity language, visiting some hospitals to get an idea about the standard forms of health records and knowing hacking scenarios in blockchain.

Chapter 2: Theoretical Study

This chapter will explain some terms in the smart contracts that are needed to comprehend this project.

2.1 Blockchain

2.1.1 What Blockchains Are

Blockchain, it's literally just a chain of blocks, most simply defined as a shared, immutable ledger.

2.1.2 What Blockchains do

Blockchain is used to record transactions across many computers so that any involved block cannot be ale altered retroactively, without the alteration of all subsequent blocks.

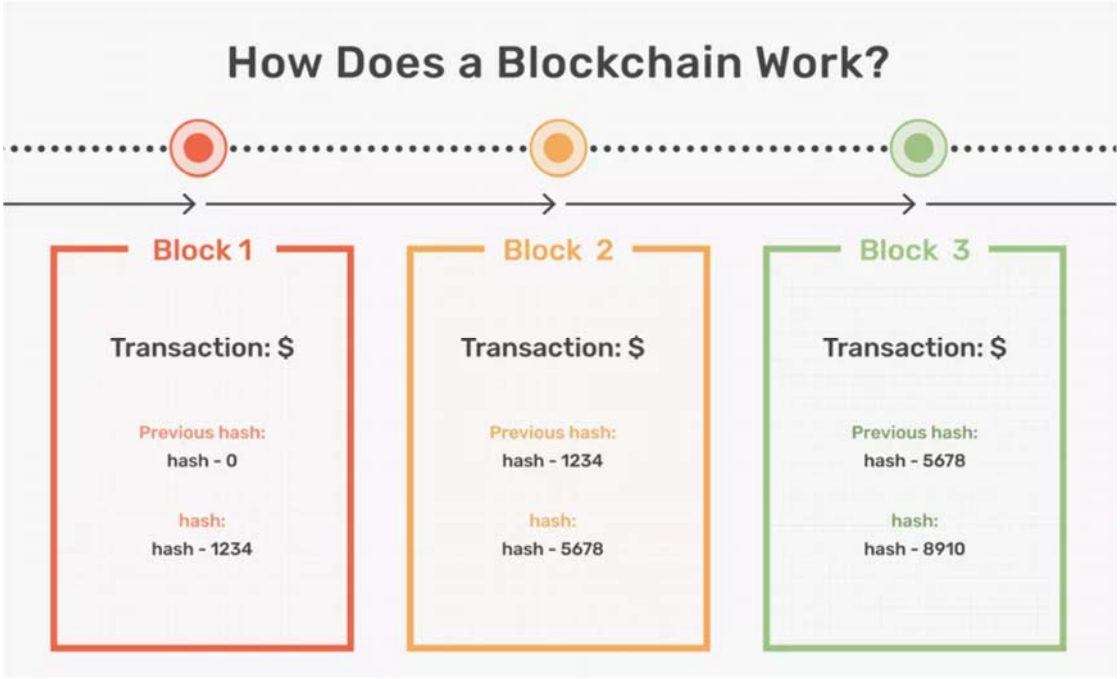

Figure 1: How Blockchain work.

2.1.3 Blockchain Healthcare Applications

Blockchain has a wide range of applications and uses in health care. The ledger technology facilitates the secure transfer of patient medical records, Placing the

patient at the center of the health care ecosystem and increasing the security, privacy, and interoperability of health data.

2.1.4 What Makes a Blockchain Suitable for Business?

Blockchain facilitates reliable identity management. Your customers and your employees have digital IDs that make it easy to verify their identity. If this information is stored on a blockchain network, it reduces the risk of identity theft, money laundering, fraud, and other cybersecurity concerns.

2.2 Smart Contract

2.2.1 What is a smart contract

Smart Contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as part of a transaction. Their purpose is to provide security superior to traditional contract law.

2.2.2 How do smart contracts work

Smart contracts work by following simple "if/when..then" statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results

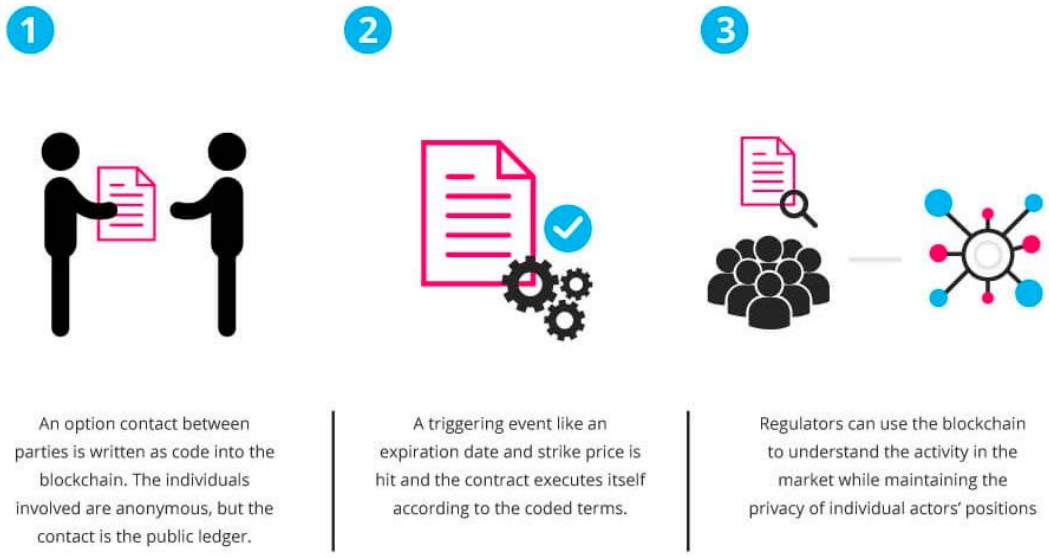

Figure 2: Work of Smart Contract.

2.3 What is Ethereum

Ethereum is a decentralized, open source blockchain with smart contract functionality. Ether (ETH or Ξ) is the native cryptocurrency of the platform. After Bitcoin, it is the second largest cryptocurrency by market capitalization. Ethereum is the most actively used blockchain.

2.4 What is solidity

Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It was developed by Christian Reitwiessner, Alex Beregszaszi, and several former Ethereum core contributors. The programs compiled by the Solidity are intended to be run on Ethereum Virtual Machine. With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

Chapter 3: Literature Review

Blockchain Technology

Blockchain technology is defined as distributed ledger technology, which records transactions in a secure, transparent, decentralized, and efficient manner with low cost. The blockchain is the technology underlies bitcoin, which was introduced by pseudonym Satoshi Nakamoto in 2008. In order to understand how blockchain works, first, it is better to know the bitcoin mechanism. Bitcoin is a peer-to-peer, distributed, and decentralized digital currency. There is no third party as a trusted intermediate in bitcoin transaction system, and anyone with bitcoin can participate in the network, read, write to, and hold a copy of the transactions records

3.1 Related Works

3.1.1 Bitcoin Blockchain

There are two challenges of the transaction system without central control agency: (1) single point of failure and (2) peer-to-peer double spending of the same digital asset like money. Blockchain technology solves this problem using two mechanisms: hash-chain time-stamping and proof of work algorithm [4]. First, in order to verify each transaction, it should be stored in each computation node in the network. All transactions are timestamped and distributed in the network. Bitcoin blockchain exploits hash-chain as distributed timestamp mechanism to determine the possibility of doing the transaction and maintaining a copy of transaction chain in every node [3]. Second, bitcoin blockchain uses the reward and punishment mechanism for preventing any possible interruption or malicious transaction. Miners are the participants who do the mining process in blockchain, creating new blocks with enclosed transactions list and chaining them to the previous blocks. Each block has two important parts: (1) Content: a validated list of transactions. The transacted digital asset can be digital money (Bitcoin, Ethereum) or any kind of data such as a school diploma, a medical record. (2) Header: which includes metadata, such as (a) Block reference number to the content of the block, known as the hash root, (b) The time the block was created known as timestamp, (c) A link back to the previous block, and

(d) A random number which is added to the block address according to the proof of work algorithm [3].

In bitcoin blockchain system miners use proof of work protocol in order to find a new address for the new block with specific properties. This property in bitcoin blockchain is a 32-bit crypto number with seventeen zero bit in the beginning. Miners run this algorithm multiple times to get such a number by trying different random numbers.

After finding a new address for the new block, the miner updates the ledger and send it to the entire network. Then the majority of the network should confirm the new block. This process is called proof of work in bitcoin blockchain system. The mining process is difficult, time taking and costly, this prevents creating invalid and fraud transactions.

Another benefit of using proof of work consensus protocol is that it let blockchain to be immutable audit trails by chaining blocks together using a hash function. Each block contains the hash value of the previous block's header (Prev.Hash), and therefore if an attacker tries to modify a block, all the upcoming blocks should be modified. Such a modification needs a high computation power, time and cost. Even if the attacker succeeds to create the fraud chain of blocks, replacing it with the honest chain requires the consensus of the majority of the nodes in the network. Thus, the bitcoin blockchain system is highly secure against any modification and failure, and this comes from its specific structure [3][7].

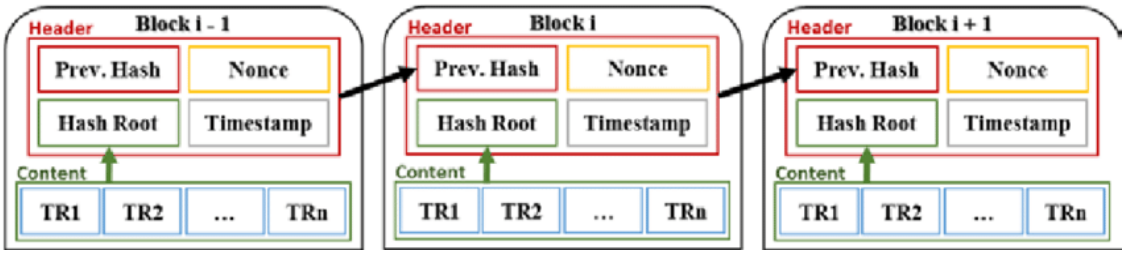

Figure 3: Blockchain Architecture.

3.1.2 Blockchain Technology for Other Sectors

Although blockchain was first introduced for finance, there are many other applications, which has been developed and implemented. Blockchain technology, as a horizontal technology, is revolutionizing the future of the transaction-based

exchange in different industries such as finance, insurance, telecommunication, and healthcare. According to Melanie Swan, there are three phases of blockchain adoption: Blockchain 1.0 is the first development of blockchain as a cryptocurrency, bitcoin. Blockchain 2.0 refers to smart contracts, financial records and tracking the ownership of the properties inside the blockchain system. Blockchain 3.0 will come in science, medicine, and education [4][5][9]

3.1.3 Blockchain Use Cases in Clinical Trials

Clinical trials in healthcare face many challenges, including personal data privacy, data sharing, and patient enrolment. Blockchain technology has the potential to address these challenges. It provides models for sharing clinical trial data that enable transparency and reproducibility securely proposed smart contracts on a private Ethereum network to address trust degradation and to strengthen data transparency on the clinical trials. The aim of this study was to improve the scientific credibility of findings from clinical trials, which could be undermined by problems such as missing data and selective publication. To enhance the capability of clinical trials and precision medicine, four new system components have been developed on top of the traditional blockchain by Shae and Tsai. These consists of blockchain based distributed and parallel computing prototype for big data analytics; data management component for data integration; identity management component for privacy protection of IoT devices; and data sharing management component for collaborative research ecosystem. In another study, proposed a novel data management framework based on permission blockchain technology using smart contract. The aim of this research was to reduce the administrative burden, time, and effort of ensuring data integrity and privacy in multi-site Clinical trials developed a consent workflow on top of clinical trial methodology. Their proof-of-concept protocol of blockchain, which is based on time stamping consent collection, includes smart contract enrollment. The historical traceability provides an opportunity to ensure verifiability and transparency of such extreme sensitive data, even when a full document is stored in a public storage, such as dedicated public website. [7][8]

3.1.4 Blockchain Use Cases in Pharmaceutical

Pharmaceutical companies are relentlessly trying to improve the quality of medicine as well as invent new medicine for diverse diseases. Such medicine is required to go through a long process ensuring patent protection, safety, efficacy, statistical validity and approval from regulatory authorities. Normally, this process takes many years, starting from discovery to commercialization, where clinical trials occupy a major part of the duration. Consequently, such a long process is vulnerable to drug recall and counterfeit due to the lack of security and privacy. This obstacle could be eliminated by using blockchain technology throughout the whole pharmaceutical process.

3.1.5 Blockchain Use Cases in Supply Chain Management

Claims and Billing Management

Healthcare service has its own cost which already makes the whole industry worth a trillion dollars, and it is increasing rapidly. The process of medical billing is an integral part of the healthcare sector. This is because, without billing, a proper service delivery cannot be ensured. This process starts from the time the patient is admitted to the hospital to the time it is checked-out. It involves several steps, such as check-in, confirming financial responsibility, coding and billing compliance, transmitting the claim, and receiving payment from insurance companies. The entire billing scheme can be challenging as some of the fees are entirely covered by the patient's individual health insurance plan, or paid by the patient. One of the main issues in medical billing is excessive billing due to the lack of transparency and trust among doctors, patients, and insurance companies. Claims and billing in the healthcare sector are being continuously abused, but can be resolved or diminished by using a transparent system for every stakeholder. Blockchain can ensure such transparent system keeping everyone engaged in the whole process and removing mistrust among them**.**

Quality management

A drug is considered as counterfeit, if it contains improper ingredients, and traded with the intent to hide or imitate its provenance, authenticity or even effectiveness. Furthermore, products and drug counterfeit greatly influence SCM. Their performance

in the pharmaceutical industry are competitive factors that disrupt the efficiency, authenticity and robust profitability in a particular healthcare industry enormously. Customers are often unaware of the exact sources of the products they purchase and consume in a global marketplace. Since this type of drug is malicious for a patient, it is a life-threatening issue around the world. This also causes a threat to the reputation of the original pharmaceutical companies, making drug manufacturers and distributors invest a huge amount of money in countermeasures. The study in found that techniques such as spectroscopic and chromatographic are effective for detecting counterfeit because of their detection of active ingredients and image sample composition. However, they have their limitations as it relies on electromechanical apparatus, which increased the overhead cost. One way to solve these challenges is to have pharmaceutical manufacturers' information, including product serial numbers and package number on the blockchain, whereby pharmaceutical companies, drug manufacturers and customers could verify the authenticity of the data by connecting to the blockchain. This process ensures low-cost quality control, product registration, drug tracking, and drug counterfeit through the entire SCM process.

3.2 Ethereum

Ethereum is also a cryptocurrency-based blockchain like Bitcoin, and is based on public network, but it can also be used to implement permissioned blockchain. Like Bitcoin, Ethereum also implements the PoW protocol. The most important feature of Ethereum is that it supports the execution of a smart contract, which allows decentralized applications to build on top of it. Ethereum is the first blockchain framework to introduce the concept of smart contracts, the reason it's very popular in developing smart contract-based decentralized applications, such as healthcare applications. Smart contracts in Ethereum can only be written in the Solidity programming language; therefore, to develop an application using the Ethereum framework, one must learn the Solidity programming language. The main reasons to select Ethereum were the capability to be configured as both a permission-less and a permissioned blockchain network, as well as the community-based development of the platform.

3.3 Hyperledger

Hyperledger Fabric is one of the projects of Hyperledger created by the Linus Foundation. With IBM's contributions, Hyperledger Fabric is among the most advanced blockchain platforms in the Hyperledger collection. Hyperledger Fabric is a completely permissioned blockchain network that is well designed for operations involving sensitive and confidential data. Compared to the other frameworks, Hyperledger Fabric is easily the most complete solution for developing healthcare applications. It has very robust privacy and security features, with support for granular access control, private channels, and zero knowledge proofs. Thus, the developers have a comprehensive toolset for easily implementing a variety of privacy and security policies. It also provides smart contracts, in addition, smart contract programming in Hyperledger Fabric provides support for different programming languages such as Node.js, Java, Go, and JavaScript. [16]

3.4 Experiment

3.4.1 Go-Ethereum

The blockchain network is construct using Go-Ethereum. Then, sent the transactions with specified data and checked the transaction input for both servers were the same. Finally, smart contracts are written, compiled, deployed and executed using Solidity on our blockchain network. An example smart contract pseudo code written in Solidity and executed on Ethereum. The whole process to build the blockchain network took about 30 minutes, while the learning time for an undergraduate student (DW) was about 7 days**.**

3.4.2 Hyperledger Fabric

The blockchain is built network using the Hyperledger Fabric images on Docker. Then, the transactions are sent to verify the connectivity of the network, and implemented/executed smart contracts using Chaincode in the Go language. The whole process to build the blockchain network took about 45 minutes, and the overall learning period for an undergraduate student (HY) was about 14 days.

3.4.3 MultiChain

Setup a blockchain network using MultiChain. Then, transactions are sent between nodes to ensure the validity of the network. Also, tried to create data streams to disseminate key-value paired data. Finally, smart filters were researched, and an example pseudo code. The whole process to build the blockchain network took about 30 minutes, while the overall learning period for a graduate student (HS) was about 2 days. [18]

3.5 Comparison

Based on implementation

Ethereum	Hyperledger Fabric	MultiChain
The installation of the software prerequisites is also easier comparing to Hyperledger Fabric	Hyperledger Fabric contains more layers in its network to increases manageability and security	is the easiest blockchain platform in terms of setup
provide the full-functional smart contract capability	provide the full-functional smart contract capability	The installation of the software prerequisites is also easier comparing to Hyperledger Fabric
supported and maintained by a large community of developers around the world	well-designed, multi-layered access control framework along with Hyperledger Fabric's own certificates leads to high versatility, security, and manageability of the blockchain platform.	the support of smart contract is limited.
		designed to be a permissioned blockchain that is very simple yet powerful to use and inherits proven features of the famous Bitcoin Blockchain by forking from it.

The smart contracts are highly readable and easily programmable. Considering the biomedical/healthcare applications.

Chapter 4: System Analysis

4.1 Functional Requirements

1. The user should be able to login/logout from the account.

2. The ability to view the user's transfer records history.

3. The patient can make a new request to select his doctor.

4. The patient can revoke the access from the doctor.

5. The doctor can approve the patient request.

6. The doctor can view all the medical records that have access on.

7.The ability to communicate with the hospital.

8. Adding a new block to blockchain.

4.2 Non-functional Requirements

1. User experience

It's important from a user experience perspective. Application should be easy to use. That first impression is very important for a new user.

2. Performance

The system must be fast to ensure reliability for all intended users.

3. Reliability

The system must be able to recover and resume working from any recurring error or crash.

4. Maintainability

The system should require a minimum effort for maintaining the process of collecting, storing and presenting the information.

5. Availability

The Applications should be available for all users 24/7 with limited to non-down time.

6. Security

our System will be secure in transferring data and in storing because we used a blockchain technique so no one can manipulate or fake any data.

4.3 Use Cases

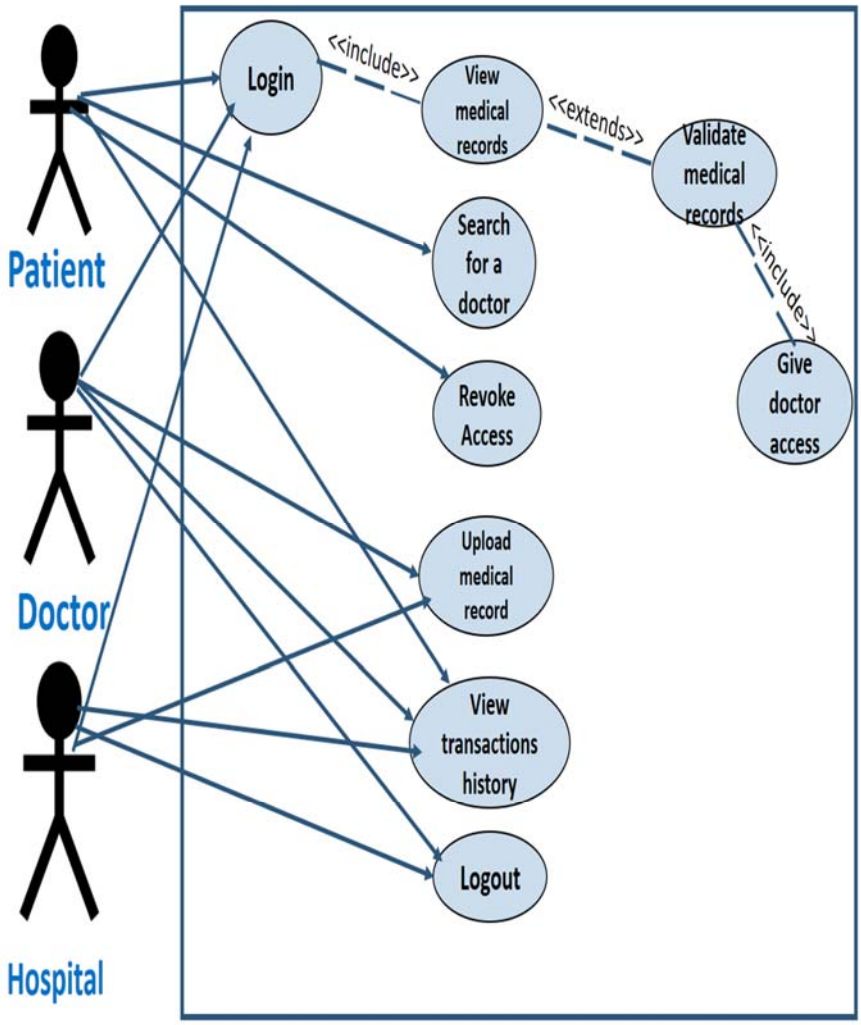

Figure 4: Use Case Diagram

Chapter 5: System Design and Implementation

5.1 Blockchain in healthcare

In this project Blockchain have a positive impact on the healthcare domain, such as providing a secure infrastructure and integrated private health records. We used blockchain to provide secure communication between patients and doctors and many hospitals, and allows sharing medical records in a secure manner. This technology also provides many advantages, including preserving patient's privacy and improving quality of medical care. It gives patients full control over their medical records. Patient information is very case-sensitive and must be stored and shared in a secure and confidential manner. Therefore, it is a prime target for malicious attacks, such as Denial of Service (DoS), Mining Attack, Storage Attack and Dropping Attack.

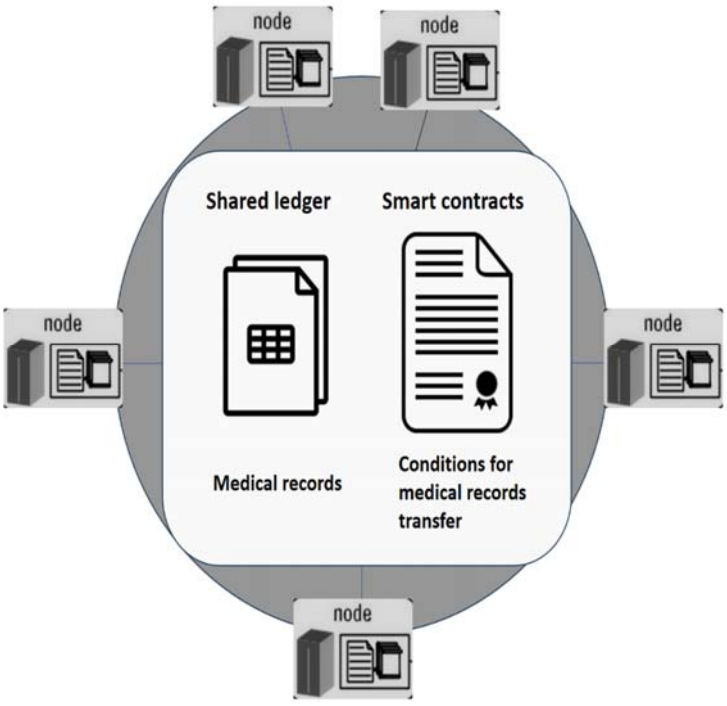

Figure 5: Blockchain in healthcare

5.2 System Architecture

This system is consisted of four main components:

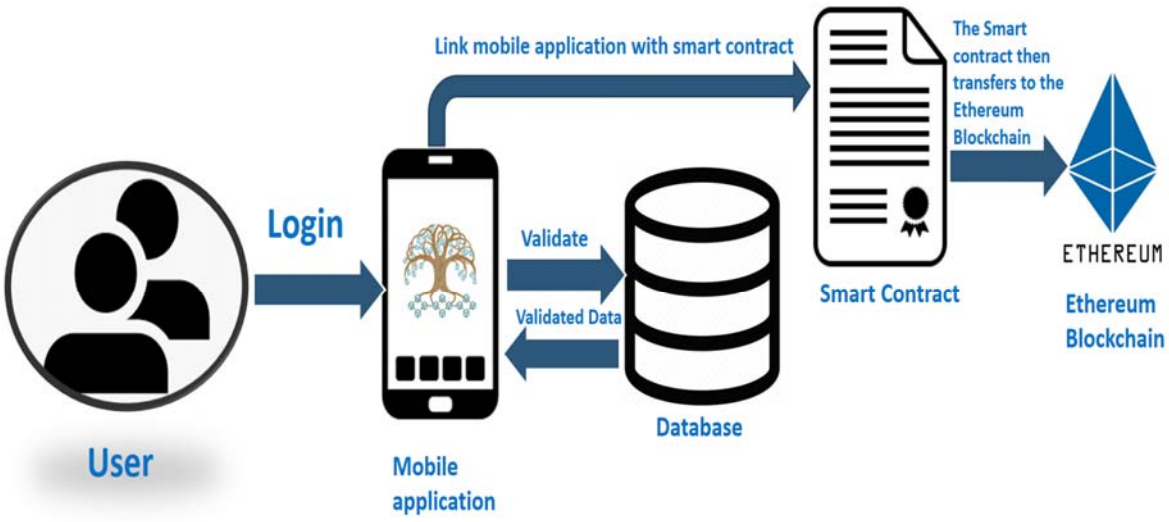

Figure 6:System Architecture

Server

Which is the main component it handles the Requests, parsing and inserting data into the database and the blockchain.

Database

MySQL databases, for saving user data and the all system required data as (‘auth data, permission, etc.’).

BlockChain

Blockchain framework (‘Ethereum’) to save all medical records and all transactions on it.

Mobile application

Which means the client side of the system from views and any other accessing method.

5.3 System Implementation

Few studies have been done in the aim of studying and implementing a e-health system based on blockchain. First of all we had to study the main principles of blockchain, we used python programing language and flask server to implement a small example to help us understand more clearly, then we learned about hashing algorithms like ('SHA256,...."), then we studied the main concepts of immutable ledger and distributed peer to peer network, then we studied about bitcoins and how mining works and about the 51% attack and byzantine fault tolerance and about consensus protocol defense against attackers, and we participated in a mining pool community to understanding the hole concepts of mining and cryptocurrency, then we studied about the smart contracts and how they work, We researched about the main principles of smart contracts and we found out that the best implementation tool to implement a smart contract is ethereum, after that we started an online course to understand the main principles of ethereum concepts, which forced us to learn about nodejs and truffle framework, then we started implementing an health blockchain system from scratch, because of some urgent situations we knew that we couldn't finish the whole system on time, which led us to search for an easier solution to implement our system and after many researches we found out that staying on ethereum is the best suitable solution, which led us to learn about solidity programing language, ganache and how to use remix IDE well. we had to learn briefly about nodejs and expressjs to use the truffle framework correctly, finally we needed to make user interfaces for our system, we used flutter and php programing language to link our mobile application. after all of that we integrated the application with our api's of ethereum so we could control our minor data in sql database and our risky data like medical records transaction in the blockchain system.

5.3.1 Medical Records Smart Contract

Our medical records smart contract ('LifeChain') contains many functions, the main work of these functions is to initially every user has a list of documents. Then to add a medical record and returns the index of the medical record after that you can get all medical records for specific user, know a user can specify, which doctors are allowed to view their medical records. 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. Finally returns all the patients addresses that gave the doctor access.

5.3.1.1 LifeChain Contract

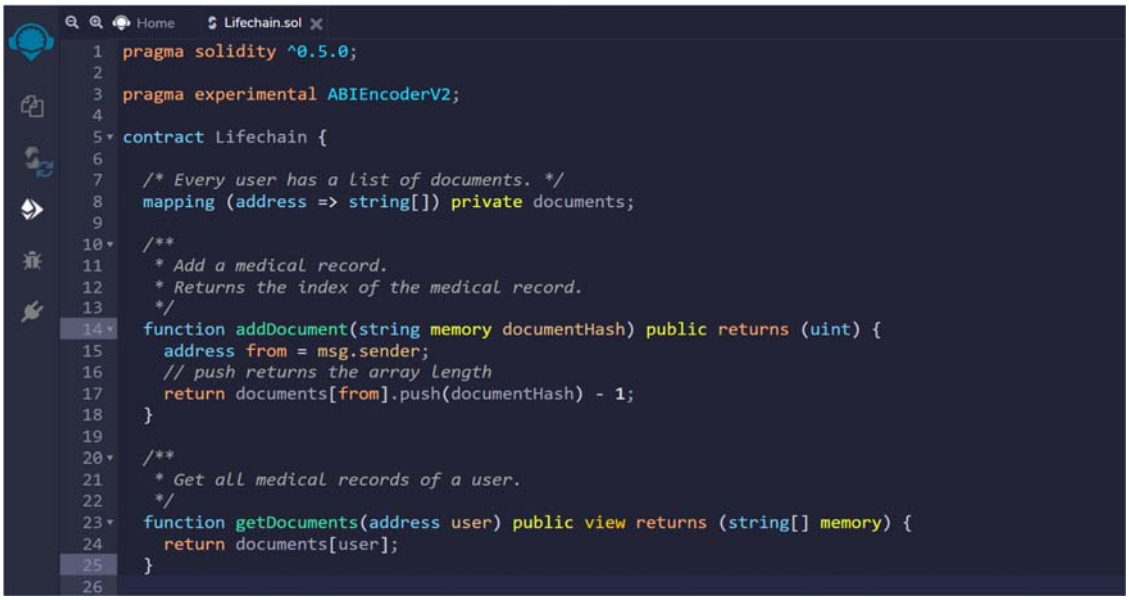

Figure 7 : Smart Contract Implementatin 1.

Figure 8: Smart Contract Implementation 2.

Figure 9: Smart Contract Implementation 3.

5.4. Technologies used

5.4.1 node.js

Node package manager or NPM and this comes bundled with nodejs, nodejs is an open source development platform for executing JavaScript code server-side.

5.4.2. truffle framework

Truffle framework is a framework that's going to allow us to create decentralized applications on the ethereum network. It's going to give us a suite of tools that allows us to write our smart contracts with the solidity programming language, it also gives us a framework for testing our smart contracts and it gives us the set of tools to deploy our smart contracts to the blockchain, we can also develop our client-side application inside of truffle.

5.4.3 Ganache

Ganache is local and memory blockchain that we used for development purposes and we installed it by going to the truffle framework website, enabling us to develop, deploy and test our dapp in safe and deterministic environment. Ganache sets up 10 default Ethereum addresses, complete with private keys and all, and pre-loads them with 100 simulated Ether each. There is no mining with ganache instead, it immediately confirms any transaction coming its way

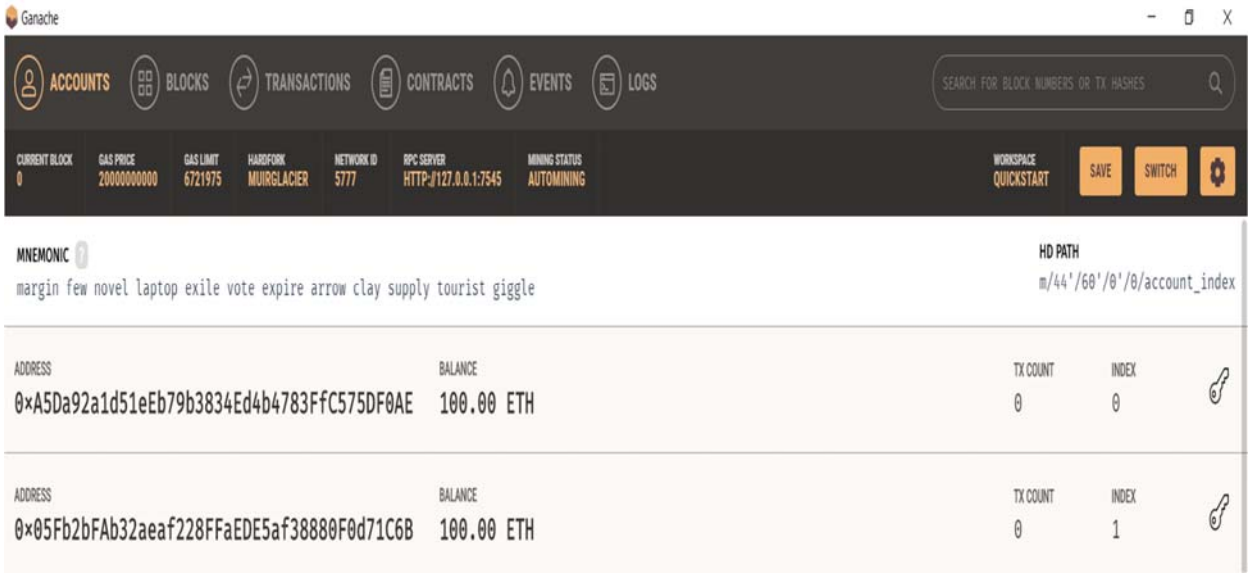

Figure 10: Ganache Cli.

The console in the above screenshot shows two user accounts with balance of 100 ETH (Ether - a currency for transaction on Ethereum platform). It also shows a transaction count of zero for each account. As the user has not performed any transactions so far, this count is obviously zero.

By entering the server HTTP 172.0.0.1:7545 web3provider now our contract is ready to be deployed. Once our contract is deployed a new block is added and every transaction occur a new block is added including the gas value is decreased.

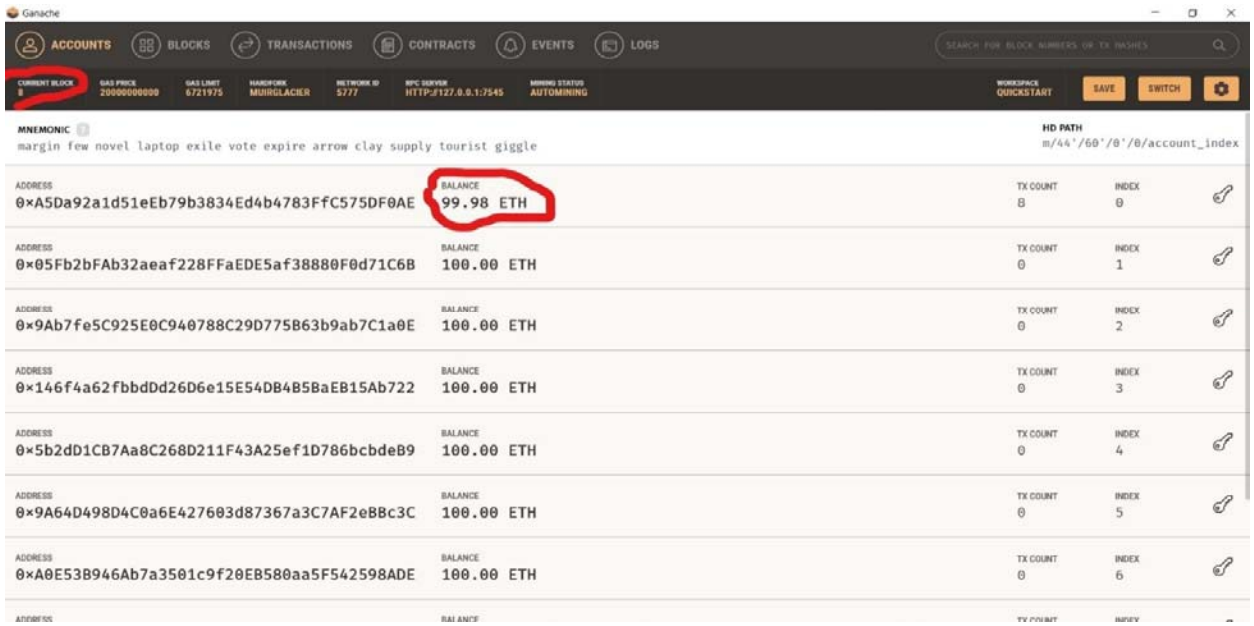

Figure 11: Deploying a contract process in ganache.

As you are aware, Blockchain is chain of blocks so whenever you perform any transaction, it gets added to block so this field show the current block number in that blockchain. Its value will be always zero when you perform fresh installation and when you restart your ganache blockchain. blocks get created when you perform some transactions, each block also references a previous block, known as the parent block, through the "previous block hash" field in the block header. The sequence of hashes linking each block to its parent creates a chain going back all the way to the first block ever created, known as the genesis block.

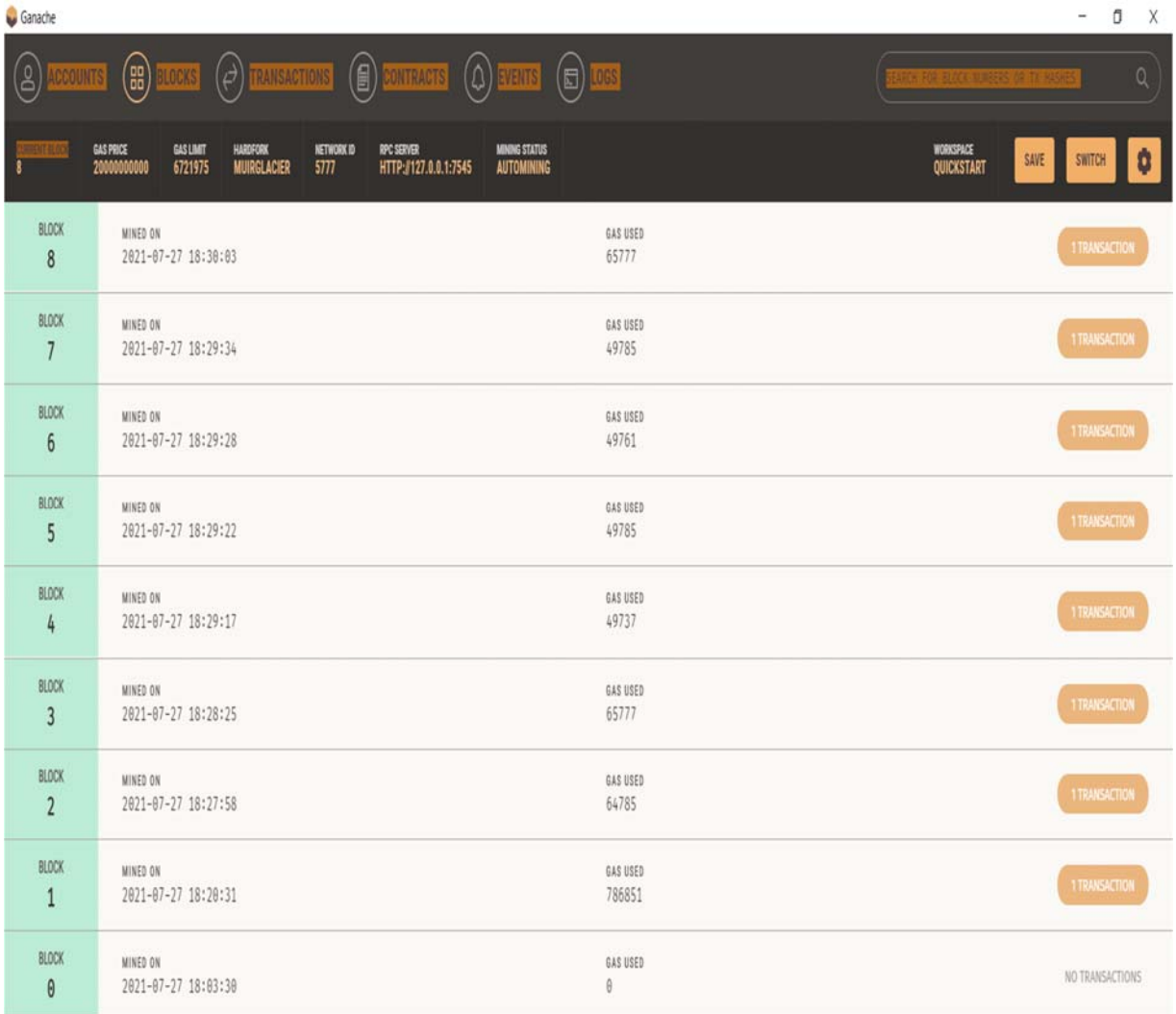

Figure 12: Blocks Creation and gensis block.

Gas Price and Gas Limit

These two parameters are related to Ethereum gas. For now, you remember that whenever you perform any action in Ethereum blockchain then need to pay some amount (money) and that amount is measured in Gas.

5.4.4 Meta mask

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows us to access our Ethereum wallet through a browser extension or mobile app, which then we used to interact with our decentralized application. Meta mask extension for google chrome is a special browser extension, we'll be able to connect to our local ethereum blockchain with our personal account and interact with our smart contract by using meta mask.

We can transfer ETHER between accounts in meta mask as shown in figures below:

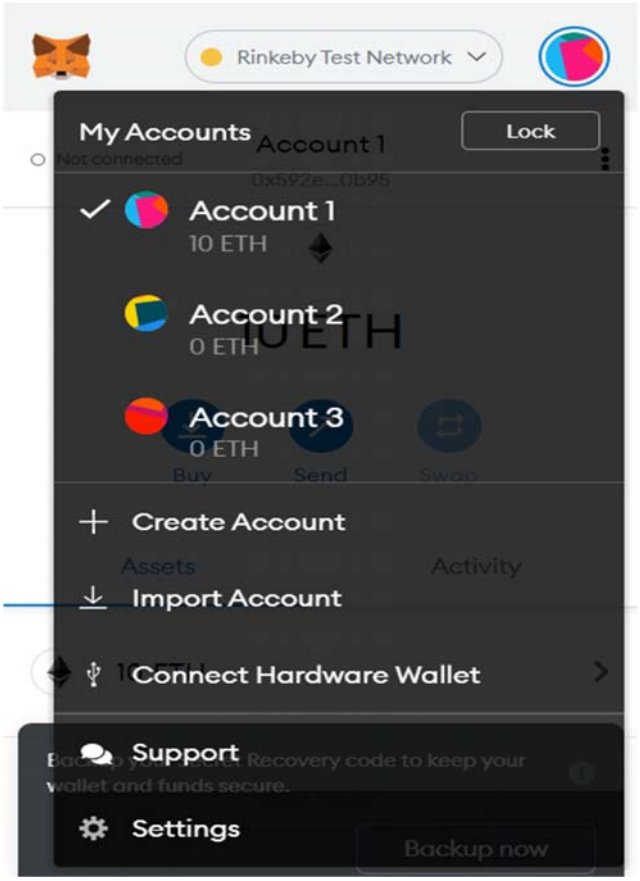

Figure 13: Multiple accounts in Meta Mask

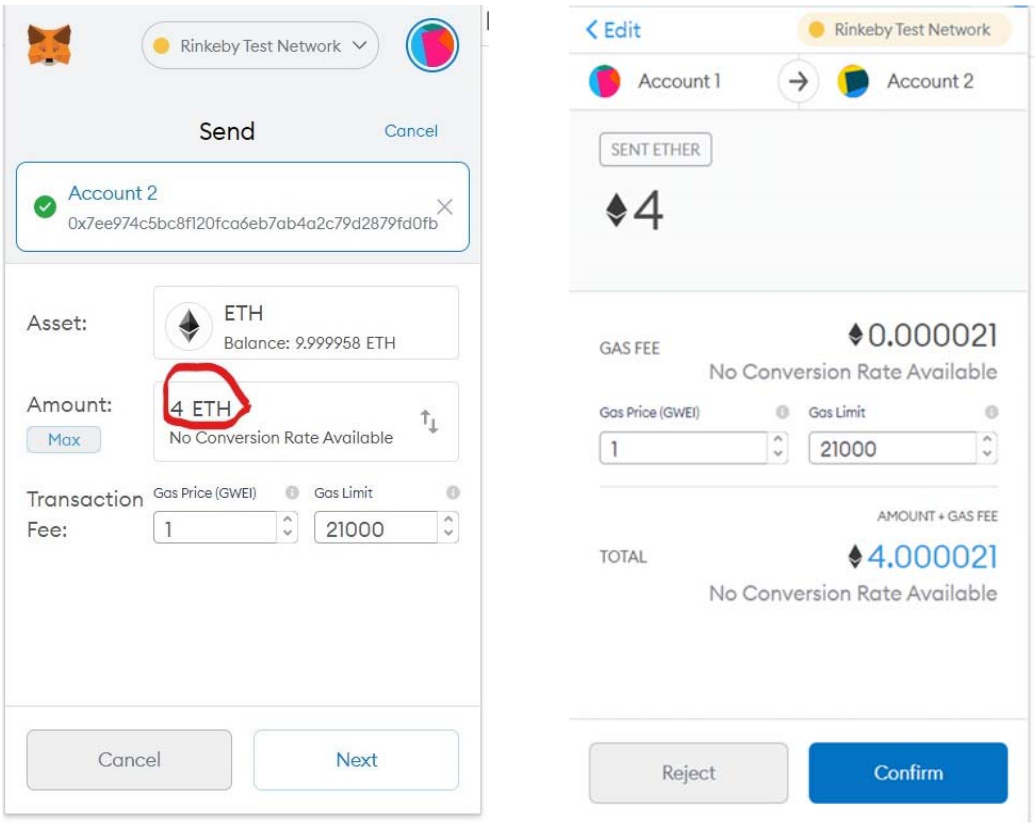

Figure 14: Transferring 4 ETH from Account1 to Account 2.

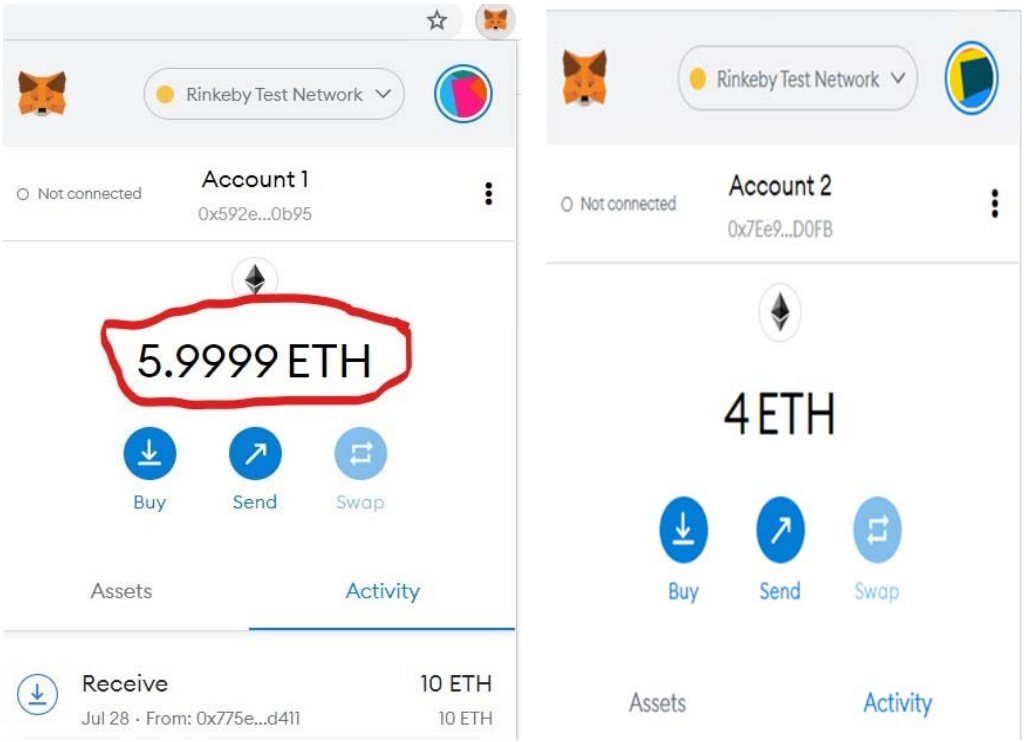

Figure 15 : Transferring ETH succeed.

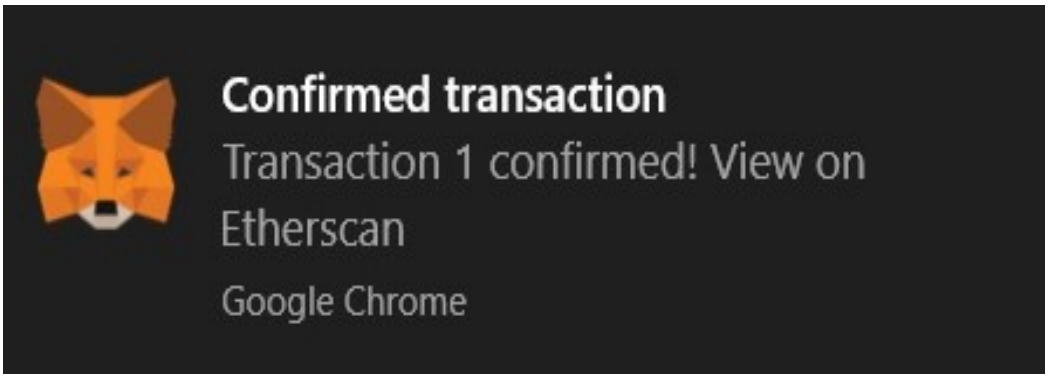

Figure 16: Meta Mask confirmed transaction.

5.4.5 XAMP

XAMPP is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing and deployment purposes. Everything needed to set up a web server – server application (Apache), database (MariaDB), and scripting language (PHP) – is included in an extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server extremely easy as well.

5.3.2 Remix IDE

Remix IDE is an open source web and desktop application. It fosters a fast development cycle and has a rich set of plugins with intuitive GUIs. Remix is used for the entire journey of contract development as well as being a playground for learning and teaching Ethereum. Also is a part of the Remix project which is a platform for development tools that use a plugin architecture. It encompasses sub-projects including Remix Plugin Engine, Remix libs, and of course Remix-Id. Remix is a powerful open source tool that helps you write Solidity contracts straight from the browser,and It is written in JavaScript and supports both usage, in the browser but run localy and in a desktop version. The environment of the IDE contains javascript VM, injected Web3, Web3 provider.

Javascript VM: It will run an isolated ethereum node in the browser. It is very useful when you want to test a contract.

Injected Web3: It will try to use the "Web3 provider" embedded in the browser. For example, MetaMask extension will embedd a "Web3 provider", you can configure to connect that provider to a testnet or to mainnet. This allow to interact with a real network.

Web3 Provider: It will ask for you to supply the RPC address of a ethereum client. This provides maximum control; you connect to your own node. For example, geth or parity instance.

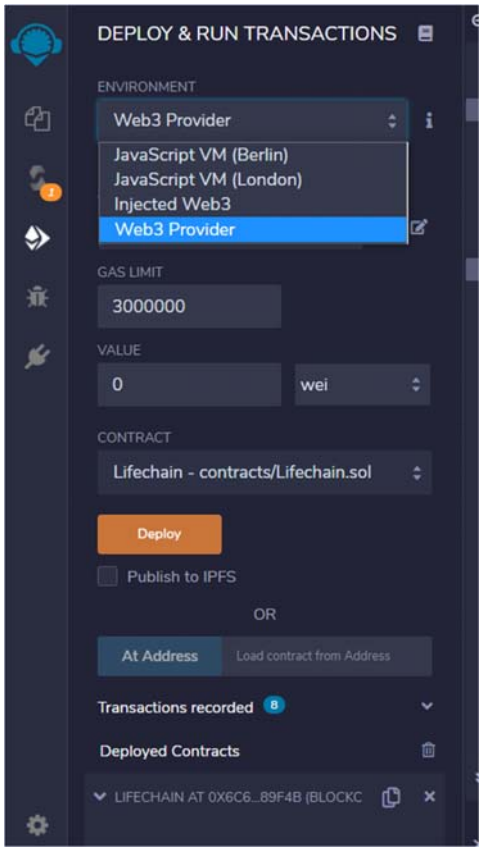

Figure 17: : Remix Environment

5.3.3 Consensus mechanism

In Ethereum, all the participant nodes must reach consensus over all the transactions, irrespective of whether or not an individual node participates in a particular transaction. It leverages the Proof of Work (PoW) consensus mechanism that mandates that all nodes must agree on a ledger to access the recorded entries in the network.

5.3.4 Used Programming language

Solidity

Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. When deploying contracts, you should use the latest released version of Solidity. This is because breaking changes as well as new features and bugs fixes are introduced regularly.

Php

PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widelyused open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML.

Dart

Dart is a programming language designed for client development, such as for the web and mobile apps. It is developed by Google and can also be used to build server and desktop applications. Dart is an object-oriented, class-based, garbage-collected language with C-style syntax.

5.3.5 Types of Blockchain Deployment

Private

Ganache sets a personal Ethereum Blockchain for running tests, executing commands, and inspecting the state while controlling how the chain operates.

Public Test(Testnet)

Like Ropsten, kovan and rinkeby which are existing public blockchains used for testing and which do not use real funds. Use faucet for receiving initial virtual funds.

Public Real(Mainnet)

Like Bitcoin and Ethereum which are used for real and which available for everybody to join.

In our project we used the private one.

5.5 MySQL Database

The main purpose for using the database is for the verification process checking that the person is authorized and to know if the medical record is existed or valid. Our database contains many tables including user table consist of his/her national id, and personal information, doctor table and majors table, medical records, records type, and hospital table.

5.5.1 ERD Diagram

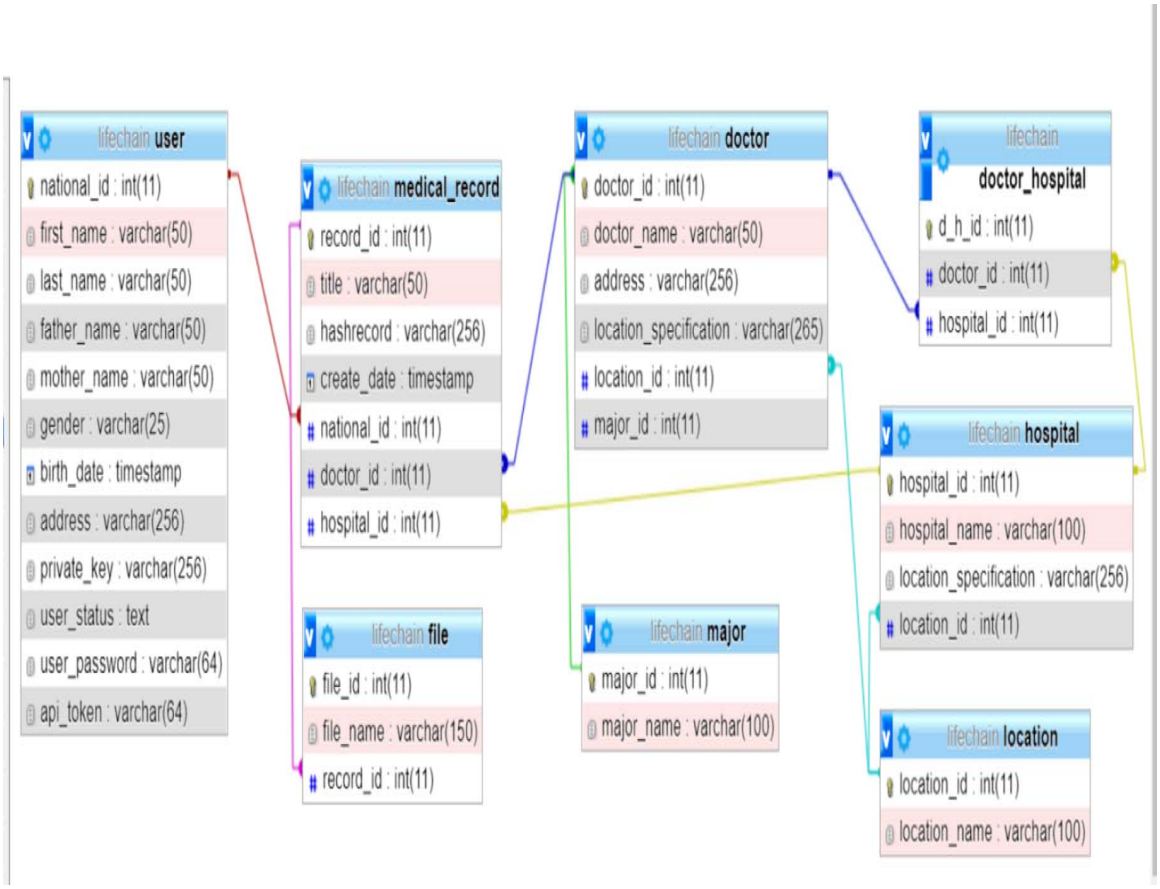

Figure 18: ERD Diagram

5.6 Application Implementation

Our application contains multiple interfaces, easily used by the user. By logging in via entering the national number and password the user can see all his/her information and can view his medical records that is composed of diseases, medicines and surgeries. Can also view all the transactions that is happening on the contract. Besides the ability of giving a specific doctor an access or revoke the access.

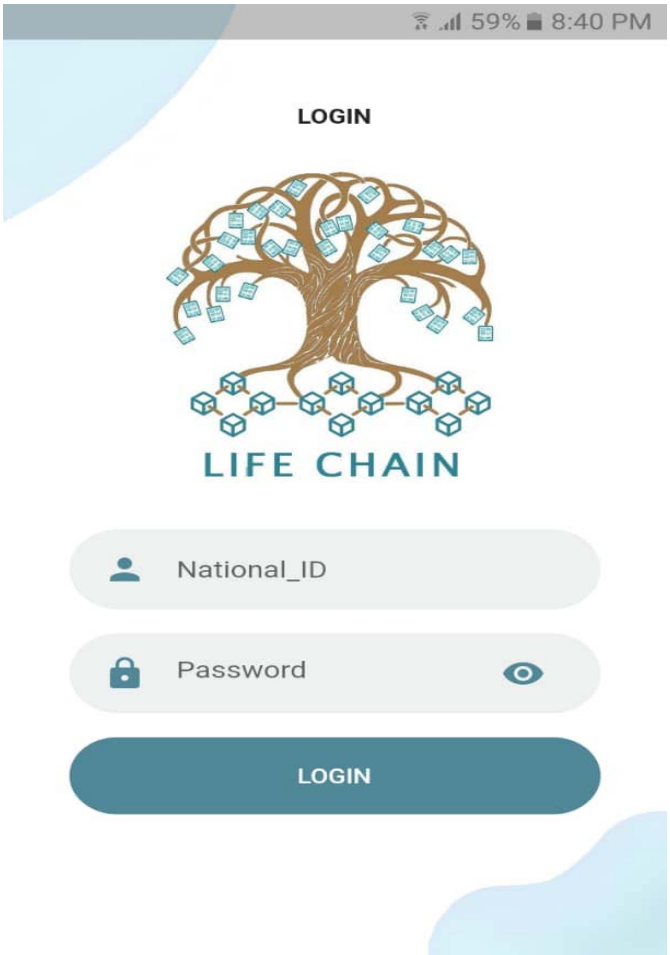

Figure 19: Login Interface

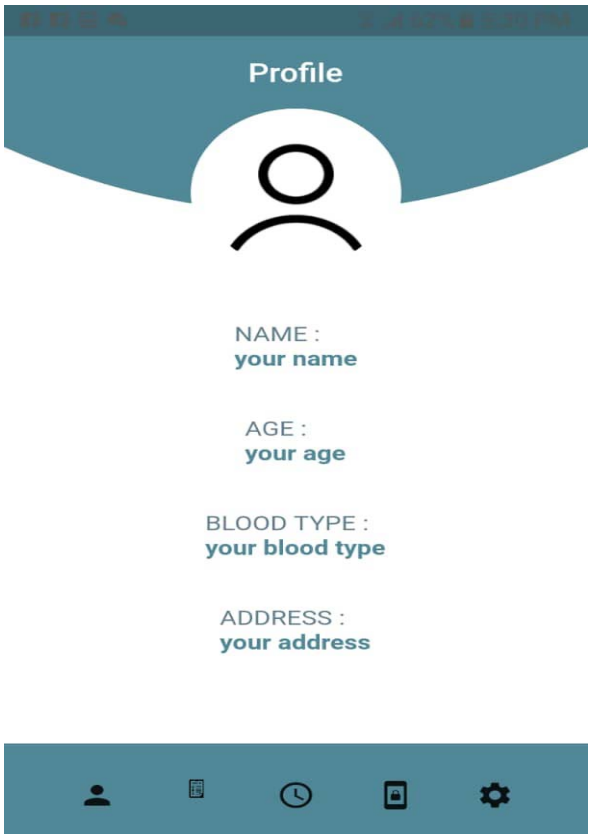

Figure 20: Profile Interface

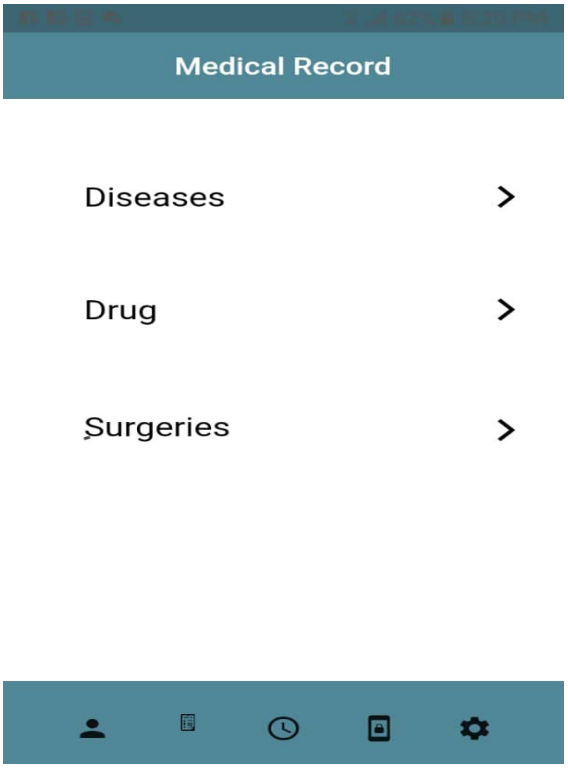

Figure 21: Medical Record Interface

In the interfaces above a user can view all his personal info and his recently medical record.

Figure 22: History interface

See all the history of the transactions happening on the smart contract.

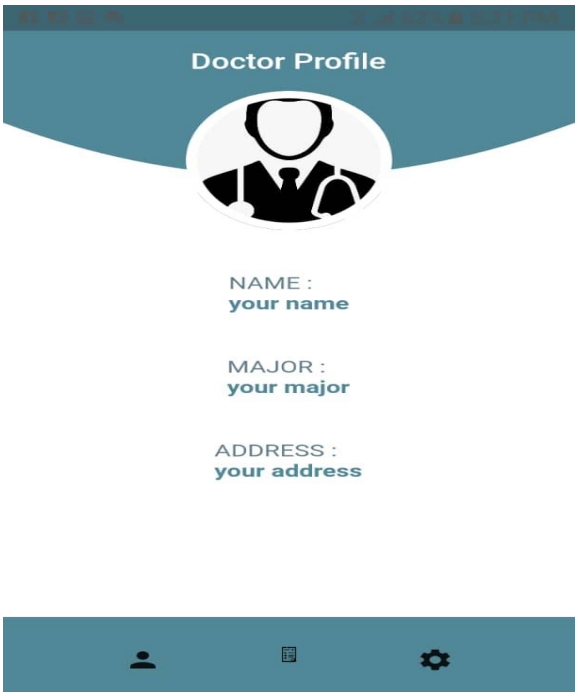

Figure 23: Doctor Profile Interface

In the doctor application a doctor user can view his personal information plus the ability of searching for a specific patient and accepting to have an access on his medical record.

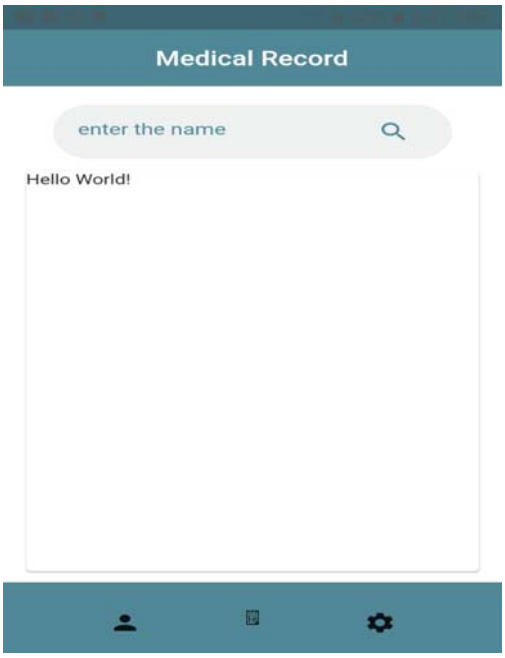

Figure 24: Search Interface

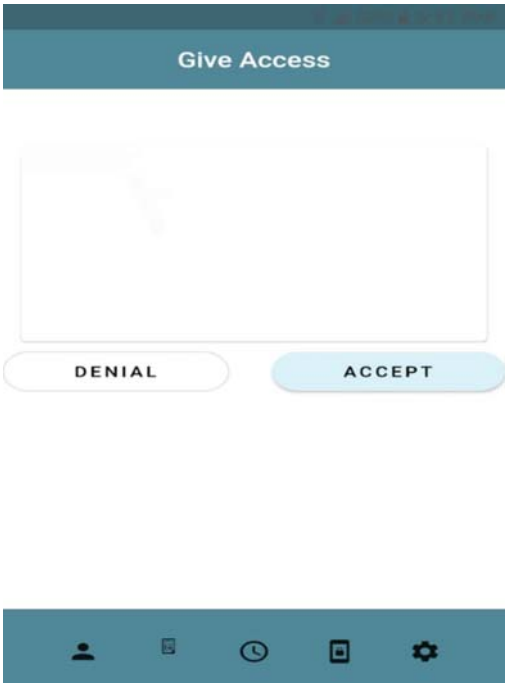

Figure 25: Access Interface

5.6.1 Setting up Flutter to interact with Smart Contract

In Ganache, we will need to link our Flutter project

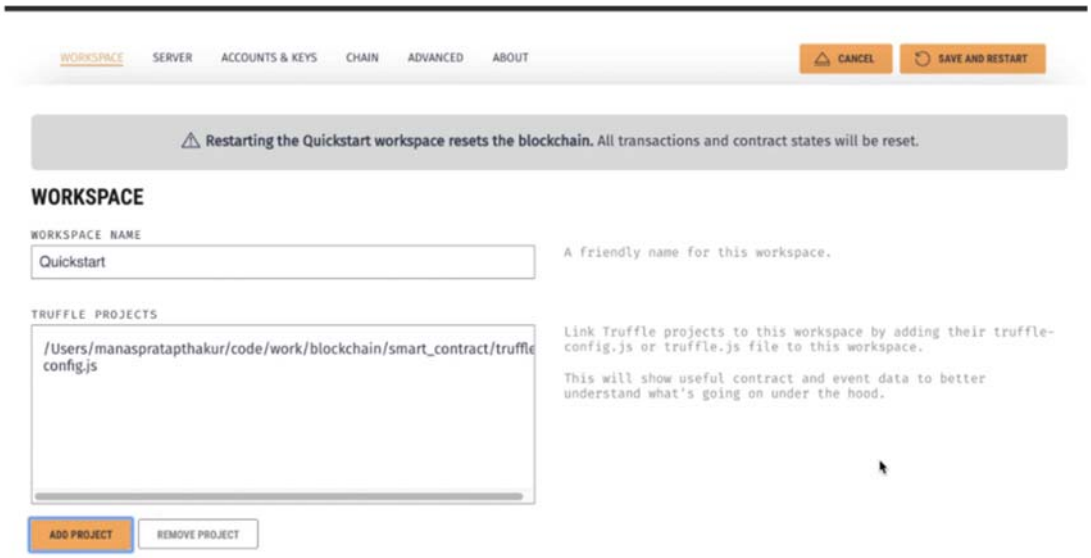

Figure 26: Linking between Ganache and flutter

Then in our truffle-config.js we need to have the following configurations

```
module.exports = {
    networks: {
        development: {
        host: "0.0.0.0",
        port: 7545,
        network_id: "*", // Match any network id
        },
    },
    contracts_build_directory: "./src/abis/",
    compilers: {
        solc: {
            optimizer: {
            enabled: true,
            runs: 200,
            },
        },
    },
```

Figure 27: Truffle configurations

In contracts build directory, we need to provide the directory where our contract application binary interface (ABI) will be stored. It is the standard way to interact with contracts in the Ethereum ecosystem.

In the compiles, solc stands for solidity command line compiler which Truffle uses. By default, the optimizer will optimize the contract assuming it is called 200 times across its lifetime. A higher number will result in higher deployment costs and cheaper function executions, and vice versa for lower number.

We used two packages web3dart and http

Web3dart

Is a dart library that connects to interact with Ethereum blockchain. It connects to an Ethereum node to send transactions, interact with smart contracts, and much more

First we initialized a client for each of them

```
Client httpClient;
Web3Client ethClient;
String rpcUrl = 'http://0.0.0.0:7545';

@override
void initState() {
    initialSetup();
    super.initState();
}

Future<void> initialSetup() async {
    httpClient = Client();
    ethClient = Web3Client(rpcUrl, httpClient);
}
```

Figure 28: Intializing a client

This will start a client that connects to a JSON RPC API, available at RPC URL. The httpClient will be used to send requests to the RPC server.

We can get the above RPC URL from Ganache

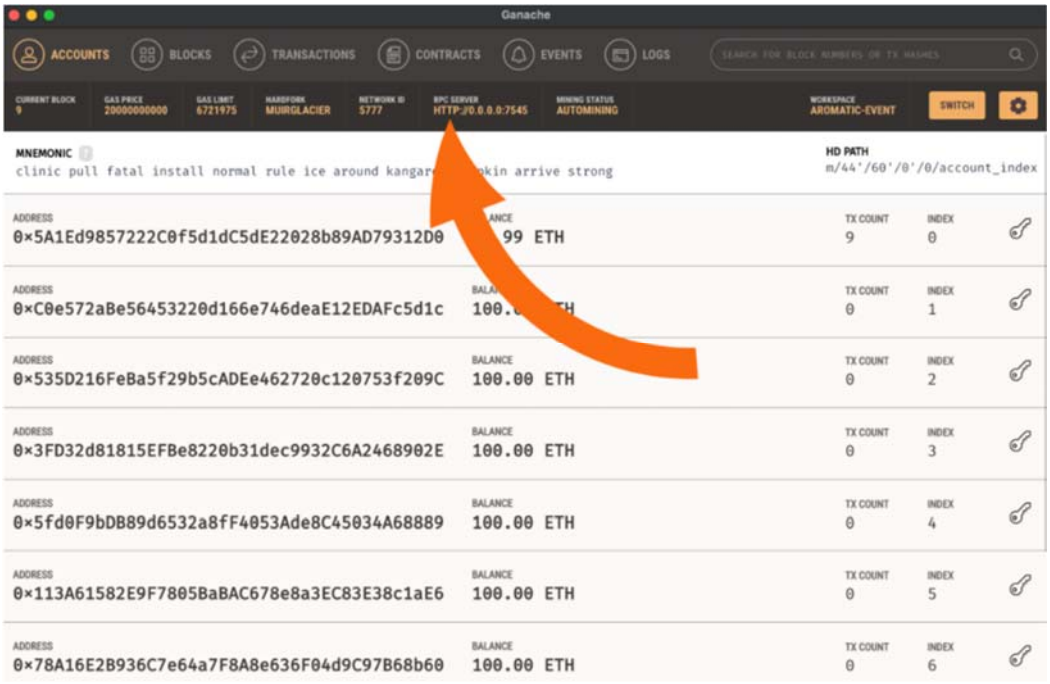

Figure 29:Getting URL from Ganache

Then, we can distribute the initialization process into three parts

```
Future<void> initialSetup() async {
    httpClient = Client();
    ethClient = Web3Client(rpcUrl, httpClient);

    await getCredentials();
    await getDeployedContract();
    await getContractFunctions();
}
```

Figure 30:Load Ethereum address

This will construct credentials with the provided and load the Ethereum address specified by these credentials.

but as a further enhancement to this app, we can configure to directly fetch the private key from an external wallet (Meta Mask)

```
String abi;
EthereumAddress contractAddress;

Future<void> getDeployedContract() async {
    String abiString = await rootBundle.loadString('src/abis/Investment.json'
    var abiJson = jsonDecode(abiString);
    abi = jsonEncode(abiJson['abi']);

    contractAddress =
        EthereumAddress.fromHex(abiJson['networks']['5777']['address']);
}
```

Figure 31:Parsing an Ethereum address

This will parse an Ethereum address from the hexadecimal representation, which Flutter extracts from the generated ABI.

Also, to allow Flutter to read the ABI, in pubspec.yaml, we added this to assets

```
assets:
    - src/abis/Investment.json
```

Figure 32:Read the ABI

After we are done with the above initialization process, we needed to create one function to read data from the blockchain, and another to write data to the blockchain,

```
Future<List<dynamic>> readContract(
    ContractFunction functionName,
    List<dynamic> functionArgs,
  ) async {
    var queryResult = await ethClient.call(
        contract: contract,
        function: functionName,
        params: functionArgs,
    );

    return queryResult;
}
```

Figure 33:To read data from the blockchain

This will call a functionName with functionArgs as parameters defined in the contract and returns its result

And to write

```
Future<void> writeContract(
    ContractFunction functionName,
    List<dynamic> functionArgs,
  ) async {
    await ethClient.sendTransaction(
        credentials,
        Transaction.callContract(
            contract: contract,
            function: functionName,
            parameters: functionArgs,
        ),
    );
}
```

Figure 34: Write data to the blockchain

5.7 Application Logo

The idea of our logo came under the concept of tree of life, the upper part of the tree is the frontend “leaves contains the medical records”, the lower part of the tree is the backend including the blockchain technology and the root is linking between the frontend and the backend of our system.

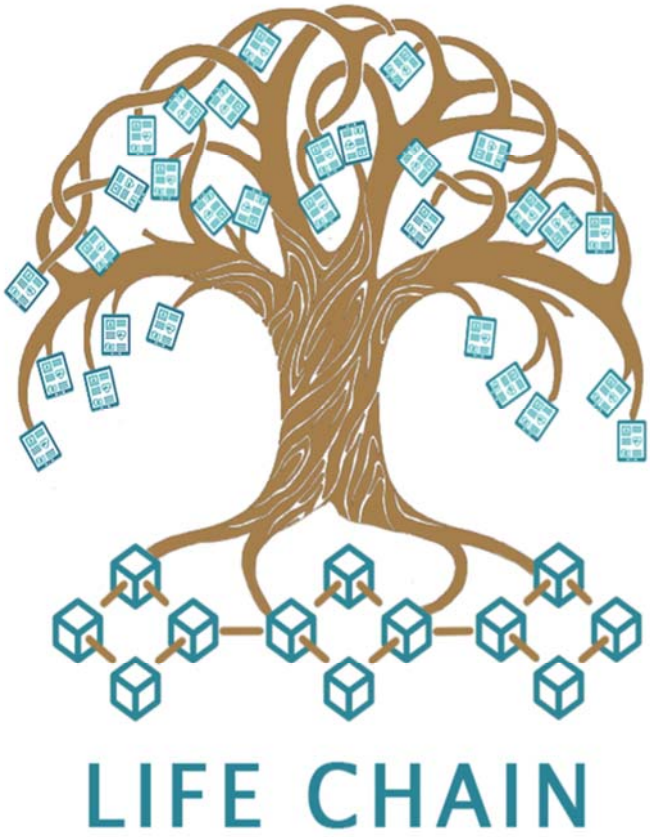

Figure 35: Application Logo

Conclusion and Future Work

System Efficiency

Our system is to build a decentralized application using blockchain technologies for healthcare records. Blockchain Technology will include application to verify a patient's digital identity, or prescriptions history and gives patients complete ownership of their medical records, allowing them to grant and revoke doctor access to their data. Data put away on the blockchain could be all around accessible to a particular individual through the blockchain private key components, empowering patients to impart their data to healthcare organizations considerably more flawlessly.

Limitations and Challenges

Interoperability

Extending our approach to a global context would require multiple deployments of the smart contracts to interoperate among each other. For example, a registered patient that travels to another country must register again under the new country's Controller smart contract. Since the Ethereum blockchain does not offer integration across different deployments, the patient will not have a global view of their medical records. However, a possibility to mitigate this limitation is to rely on a global healthcare DApp that can perform the required integration.

Smart contracts upgradability

In Ethereum blockchain, smart contracts are stored on-chain, making them immutable. However, this poses a major challenge in the development process of smart contracts, as immutability makes them lack upgradability. Once smart contracts are developed and deployed, they can no longer be modified. Therefore, it is not possible to patch security vulnerabilities or software bugs with an update.

Future Work

Whilst the healthcare sector is undergoing a digital overhaul, we are still only at the beginning of this process and without a centralized model to follow or adopt, it is a huge undertaking for healthcare systems to embark on. In order for blockchain technologies to become widely adopted in healthcare systems, industry leaders and policy makers, along with private and government bodies, will need to work together and adopt a joint approach

The time seems ripe for this type of collaboration, as COVID-19 has accelerated a digital explosion in healthcare. The focus has shifted from being able to handle more patients to being able to handle them more effectively and treating their conditions more easily. Blockchain's unique ability to both protect and flexibly hold data could play a vital role in underpinning healthcare's digital progress and overhaul how it is delivered.

Conclusion

Blockchain technology holds promise for augmenting health information exchange and fundamentally enabling greater data transparency, safer patient care, improved healthcare efficiency and more robust medical research. Despite the upside, there are several fundamental issues that must be resolved prior to a safe and successful widespread implementation.

As with any disruptive technology, healthcare organizations must appropriately assess blockchain in the context of their needs and equip providers with the skills to use these tools effectively. Although blockchain may offer a superior platform for information exchange, it is simplistic to assume that the aforementioned benefits will automatically ensue after implementation of a blockchain system. In order to achieve its full potential, blockchain platforms will need to possess a balance of guidelines to allow for broad use as well as flexibility to accommodate local practice variation. Furthermore, emphasis cannot only be placed on technical solutions but must include consideration for human factors that otherwise limit the use of any digital platform.

References

[1] J.D. Bruce The Mini-Blockchain Scheme (2013).

[2] Itlay Eyal, G sirer. Majority is not Enough: Bitcoin Mining is Vulnerable (2013).

[3] Antonopoulos AM (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies. *O'Reilly Media, 2014*.

[4] Ichikawa D, Kashiyama M and Ueno T (2017) Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR Mhealth Uhealth* 5(7): e111.

[5] Yue X, Wang H, Jin D, Mingqiang Li, Jiang Wei (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J Med Syst* 40: 218.

[6] Griggs KN, Ossipova O, Kohlios CP, Alessandro N Baccarini, Howson Emily A, et al. (2018) Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J Med Syst* 42: 130.

[7] Firdaus A, Anuar NB, Razak MFA, Hashem Ibrahim Abaker Targio, Bachok Syafiq, et al. (2018) Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. *J Med Syst* 42: 112.

[8] Fan K, Wang S, Ren Y, Li H, Yang Y (2018) MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J Med Syst* 42: 136.

[9] Li H, Zhu L, Shen M, Feng Gao, Xiaoling Tao, et al. (2018) BlockchainBased Data Preservation System for Medical Data. *J Med Syst* 42: 141.

[10] Roehrs A, da Costa CA and da Rosa Righi R (2017) OmniPHR: A distributed architecture model to integrate personal health records. *J Biomed Inform* 71: 70–81.

[11] Wang H and Song Y (2018) Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *J Med Syst* 42(8): 152.

[12] Zhang A and Lin X (2018) Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J Med Syst* 42(8): 140.

[13] Dubovitskaya A, Xu Z, Ryu S, et al. (2017) Secure and Trustable Electronic Medical Records Sharing using Blockchain. *AMIA Annu Symp Proc* 2017: 650–659.

[14] Mamoshina P, Ojomoko L, Yanovich Y, et al. (2018) Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget 2018*; 9: 5665–5690.

[15] Ji Y, Zhang J, Jianfeng Ma, Chao Yang, Xin Yao, et al. (2018) BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. *J Med Syst* 42: 147.

[16] Nugent T, Upton D and Cimpoesu M (2016) Improving data transparency in clinical trials using blockchain smart contracts. *F1000Res* 5: 2541.

[17] Benchoufi M, Porcher R and Ravaud P (2017) Blockchain protocols Cinclinical trials: Transparency and traceability of consent. *F1000Res* 6: 66.

[18] Zhou L, Wang L and Sun Y (2018) MIStore: a Blockchain-Based Medical Insurance Storage System. *J Med Syst* 42: 149.

الجامعة العربية الدولية

الجامعة العربية الدولية AIU جامعة سورية خاصة أُحدثت عام 2005، خططها الدراسية والوثائق الصادرة عنها معتمدة ومصدقة من قبل وزارة التعليم العالي في الجمهورية العربية السورية.

تعمل الجامعة على تحقيق الأهداف الآتية:

- إعداد جيل متميز من الخريجين الجامعيين القادرين على تلبية الحاجات النوعية للمجتمع والنهوض به.
- الإسهام في البحوث العلمية النظرية والتطبيقية التي تخدم أغراض التنمية الوطنية، ويتم العمل على حث الأساتذة والعاملين الأكاديميين على البحث العلمي والمشاركة في المؤتمرات والندوات التي تنظم الأبحاث.
- تحقيق الشراكة مع الجامعات العربية والأجنبية المرموقة بهدف التطوير والتحديث المستمرين للعمل الأكاديمي والقيام ببحوث علمية مشتركة.
- استقطاب الكفاءات الأكاديمية والبحثية المتميزة عن طريق توفير البيئة المناسبة لعملها.

الجامعة العربية الدولية من الجامعات السورية الأولى التي جرى تأسيسها وافتتاحها، وقد تمكنت من اجتذاب الكفاءات التعليمية والبحثية والإدارية المتميزة، لإنشاء صرح متكامل من النواحي الأكاديمية والتنظيمية والإدارية. وتمكنت من تخريج كوادر من المبدعين والمتميزين من خلال توفير بيئة تعليمية ترتكز إلى مقومات نوعية ومادية فريدة منها:

- الخطط الدراسية الحديثة والمتطورة المستندة إلى نظام الساعات المعتمدة.
- الأطر التعليمية المنتقاة بعناية كبيرة.
- المختبرات العلمية الحديثة، ومختبر للمكتبات الإلكترونية.
- المحفزات المادية والمعنوية للطلبة.
- تطبيق طرائق التدريس التفاعلي.
- التوجيه والإرشاد الأكاديمي والتربوي.
- مجموعة كبيرة من اتفاقيات التعاون العلمي مع جامعات محلية وإقليمية ودولية ذات سمعة مرموقة.
- اتفاقيات ومذكرات تفاهم متعددة مع العديد من مؤسسات المجتمع المدني.
- الحرم الجامعي اللائق والمزود بكافة المرافق العلمية والرياضية والترفيهية، والذي نشجعك على زيارته والتعرف على مزاياه.
- الأنشطة والأندية الطلابية بمختلف أنواعها: الرياضية والثقافية والعلمية والاجتماعية.

في الجامعة العربية الدولية سنوات الحياة الجامعية هي وقت للاستثمار في مستقبل الطالب. فالمعارف والخبرات التي يحصلها في قاعة المحاضرات والمختبرات ستساعده في تطوير ذاته، وستمنحه أسباب النجاح في التخصص الذي اختاره، والنشاط الطلابي الذي يمارسه سيساعده في توسيع أفقه، وفعاليات التدريب والأندية والرياضة ستمكنه من تطوير مواهبه، ولربما تساعده في اكتشاف مواهب جديدة.
ليستثمر وقته وذهنه وروحه في جامعتنا كي يجني فوائد عمله والوقت الذي كرسه في السنين القادمة. ونحن سوف نكون بجانب طلبتنا في كل خطوة على دربهم.

الجامعة العربية الدولية

كلية الهندسة المعلوماتية والاتصالات

مشروع التخرج

زيادة الأمن والموثوقية في نظام الصحة الإلكترونية باستخدام تقنية البلوكتشين

تم تقديمه إلى

قسم الهندسة المعلوماتية

تقديم

سلوان عرار **شام البقاعي** **يارا صعب**

بإشراف

د.سيرا استور **م.علي العلي**

اب/2021