Ain Shams University
Faculty of Computer & Information Sciences
Information Systems Department

2020 - 2021

Drug Authentication

By Blockchain

Acknowledgment

We would like to express our gratitude for everyone who helped us during the graduation project starting with endless thanks for our supervisor Dr. Tamer Mostafa who did not keep any effort in encouraging us to do a great job, providing our group with valuable information and advice to be better each time. Thanks for the continuous support and kind communication which had a great effect regarding to feel interesting about what we are working on. Also, we would like to thank everyone who gave us every valuable piece of information which was a part of our successful project. It has been a great opportunity to gain lots of experience in real time projects, followed by the knowledge of how to design and analyze real projects. Special thanks to the graduation project unit for the efforts they did to provide us with all useful information and making the path clear for the students to implement all the education periods in real-time project design and analysis. Finally, we sincerely thank all the people who helped, supported, and encouraged us to successfully finish the graduation project.

Abstract

Health is a crown to the heads of healthy people, and it is one of the most important blessings that God has given us, so we must preserve it well so that we can complete our missions and messages in the life for which we were created. But unfortunately, the drug counterfeit problem has become global and so huge that it has drawn significant attention from everyone. The fake drug industry is worth $10B per year as estimated by survey. Also estimated by WHO, about a million die per year due to fake drugs. The distribution of fake drugs is a crucial issue. One of main reasons behind drug counterfeiting is imperfect supply chain. There are many loopholes in our drug supply chain. In the present scenario of supply chain, either the information is not at all shared between the parties during the hand-off process or a little or irrelevant information is shared, which has led to counterfeiting. The counterfeit drug not only affects the health condition of patients but also results in the financial loss of genuine manufacturer.

After 6 months of non-stoppable thinking and implementation and optimization we are now able to publish a powerful system to the users which easily provides the mentioned services, with an easily understanding user interface, we now can connect several places in Cairo with different transports that passes by these several locations.

List of Figures

Table of Contents

Chapter 1

Introduction

1.1. Motivation

Drug manufacturing is expensive, and it takes approximately two billion dollars to manufacture a single type of drug. Replacement of these drugs with counterfeit drugs is a prevailing problem and causes about 150 billion-dollar, loss to the pharmaceutical industry annually. In addition to loss of money, counterfeit drugs also pose a threat to lives, and sabotages reputed brand names. The counterfeit drug problem is encouraged because of lack of coordination and traceability of the drug itself within the pharmaceutical supply chain. The pharmaceutical supply chain is a highly complex and branched chain where many players are involved in moving the drug from one point to the other. Since there is no system in place to accurately trace the drug movement, counterfeiters enter the supply chain, and replace the authentic drugs with fake ones, this inspired us find a solution that limits this problem and its damages by developing Drug Authentication system using blockchain.

1.2. Problem Definition

The main problems that we are trying to solve are:

Making all medicine data secure and prevent anyone from changing it: many dishonest people can take the original drug and replace it with the fake one and replace the serial number of the original drug and change it with the fake one in the database so we must ensure that the medicines data is hard to be replaced and not fake.

Deliver original medicine from manufactures to countries: we need to make a system that makes a direct connection between manufactures and countries to control any illegal issues which may occurs and make the country ensure that the original medicine reached the country without any replacement with any fake drugs.

How to make all people check the medicine after buying it: we face an issue in how to check the correctness of the drug, so we want to make an app which make this check very easy for the normal user.

1.3. Objectives

Creating a web application reduces the health risks resulting from manipulation and changing medications or lack of citizen awareness.

This application will reduce costs resulting from the ability to check whether the drug is correct or fake.

This application will provide the possibility of direct contact between the manufacturer and pharmacies to make quick orders.

We strive for the application to be highly transparent, as it provides complete and clear information about medicines, companies, and pharmacies for all users of the application in addition to securing drug information, a high security that is difficult to penetrate and tamper with.

1.4. Document Organization

This documentation is composed of 8 chapters:

Chapter 2: Background

Will contain all the information we worked on including: the challenges, how we started, what were the problems arising throughout the whole process, the similar projects and why our system is better than all the other projects, what are the enhancements done.

Chapter 3: Related Work

This chapter include any previous systems or applications like our system.

Chapter 4: Analysis and Design

Will include how everything is connected to each other in our system, regarding the database, how the user interacts with the system, what are the main functions of the system, what are the inner characteristics of the system, the detailed structure of how the system components interact with each other.

Chapter 5: Implementation

This chapter is dedicated to explaining how the system is built, how all its modules are structured and how it is operated and used to achieve the intended goal.

Chapter 6: User Manual

A complete guide for both authenticated users and any other user for our system, the main purpose is to provide simple collection of steps to the user to be able to interact with our system easily and make everything looks simple enough without any complications in dealing with the interface.

Chapter 7: Conclusion and Future Work

Results of the complete process of continuous hard work and think, what are the future plans to extend the current application and make it more popular among the society.

Chapter 8: References

Include all Links for Research papers, Courses, Books and Websites that helped us to understand and develop the system.

Chapter 2

Background

In this chapter we introduce an overview of the Field of the project and the scientific background.

2.1 Field and scientific background of the project:

2.1.1 Blockchain and counterfeit drugs

Imagine a situation, where someone dies because of fake medicine. It is not distant possibility, and this has become a reality for most developing countries even for some. developed countries. Fake medicines have turned to be multi-billion-dollar problem. on a global level. The shape, size, color of the pharmaceuticals and even the packaging exactly look like the original. Small amounts of the active ingredients can be found in these bogus products or sometimes none at all or may be even worse like some fatal ingredients, It is beyond doubt that fake medicines are an increasing threat to consumers and the pharmacy industry. So, the real-time visibility of drug production and management is necessary. Blockchain is the answer for dealing with counterfeit drugs. It can be accessed freely because the transactions are stored in digital ledger format without compromising on the security and privacy of the users. Blockchain technology concept came

from bitcoin cryptocurrency, where no third party is required for transaction. In blockchain, transaction is being carried out in a distributed peer-to-peer system. It has been a common thought that blockchain can only be used for financial sector as it is based on the idea of bitcoin. Only recently, the true potential of blockchain has been realized by the researcher community. This decentralized technology has many useful applications, such as health care, logistics, Internet of Things (IoT), reputation system, public service, supply chain which are beyond the financial sector. If only health care sector is considered, it may further be divided into many parts like medical record management, health care data access control, clinical trial, drug supply management, insurance claim adjudication, etc.

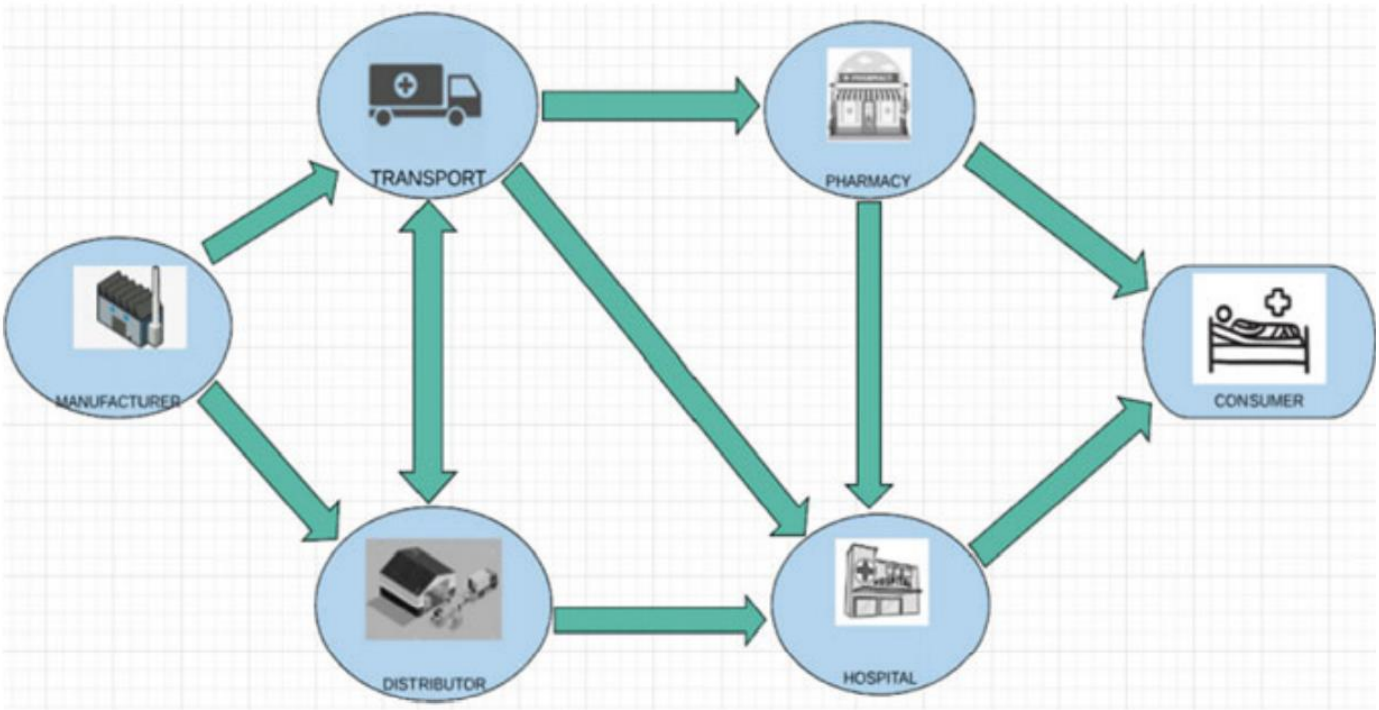

Fig. 1 Distributed architecture diagram of drugs supply chain

2.1.2 Blockchain

Blockchain technology allows large amounts of correlated data to be distributed but not copied. Although these types of digitally distributed ledgers have been around for years, blockchain uses new technology, like specialized algorithms, to validate and authenticate transactions within a decentralized architecture while progressing in real time through protected layers of digital encryption. The decentralized framework of blockchain, in addition to distributed digital ledger that records and transfers data in a secure, transparent, and fast manner may be use. A drug supply chain based on blockchain depends on a trusted network geared with blockchain. The required entities or nodes of the blockchain network are the manufacturer and pharmacist or hospital. A supply chain is to be created including all the stakeholders such as suppliers and pharmacies, hospitals.

Let's dive in a little deeper into the features of blockchain:

- **Immutability:** Blockchain technology works slightly different than the typical banking system. Instead of relying on centralized authorities, it ensures the blockchain features through a collection of nodes.Every node on the system has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof. So, without the consent from most nodes, no one can add any transaction blocks to the ledger. Another fact, that backs up the list of key blockchain features is that, once the transaction blocks get added on the ledger, no one can just go back and change it. Thus, any user on the network won't be able to edit, delete or update it.

- **Decentralized**: The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Rather a group of nodes maintains the network making it decentralized. This is one of the key features of blockchain technology that works perfectly. Let me make it simpler. Blockchain puts us users in a straightforward position. As the system does not require any governing authority, we can directly access it from the web and store our assets there. You can store anything starting from cryptocurrencies, important documents, contracts, or other valuable digital assets. And with the help of blockchain, you will have direct control over them using your private key. So, you see the decentralized structure is giving the common people their power and rights back on their assets.

- **Enhanced Security:** As it gets rid of the need for a central authority, no one can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the system. Every information on the blockchain is hashed cryptographically. In simple terms, the information on the network hides the true nature of the data. For this process, any input data gets through a mathematical algorithm that produces a different kind of value, but the length is always fixed. You could think of it as a unique identification for every data. All the blocks in the ledger come with a unique hash of its own and contain the hash of the previous block. So, changing or trying to tamper with the data will mean changing all the hash IDs. And that's kind of impossible. You will have a private key to access the data but will have a public key to make transactions.

- **Distributed Ledgers**: Usually, a public ledger will provide every information about a transaction and the participant. It is all out in the open, nowhere to hide. Although the case for private or federated blockchain is a bit different. But still, in those cases, many people can see what really goes on in the ledger. That is because the ledger on the network is maintained by all other users on the system. This distributed computational power across the computers to ensure a better outcome. This is the reason it is considered one of the blockchain essential features. The result will always be a higher efficient ledger system that can take on the traditional ones.

- **Consensus:** Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions. In simple terms, the consensus is a decision-making process for the group of nodes active on the network. Here, the nodes can come to an agreement quickly and relatively faster. When millions of nodes are validating a transaction, a consensus is necessary for a system to run smoothly. You could think of it as kind of a voting system, where the majority wins, and the minority must support it. The consensus is responsible for the network being trustless. Nodes might not trust each other, but they can trust the algorithms that run at the core of it. That is why every decision on the network is a winning scenario for the blockchain. It is one of the benefits of blockchain features.

- **Faster Settlement**: Traditional banking systems are quite slow. Sometimes it can take days to process a transaction after finalizing all settlements. It also can be corrupted quite easily. Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

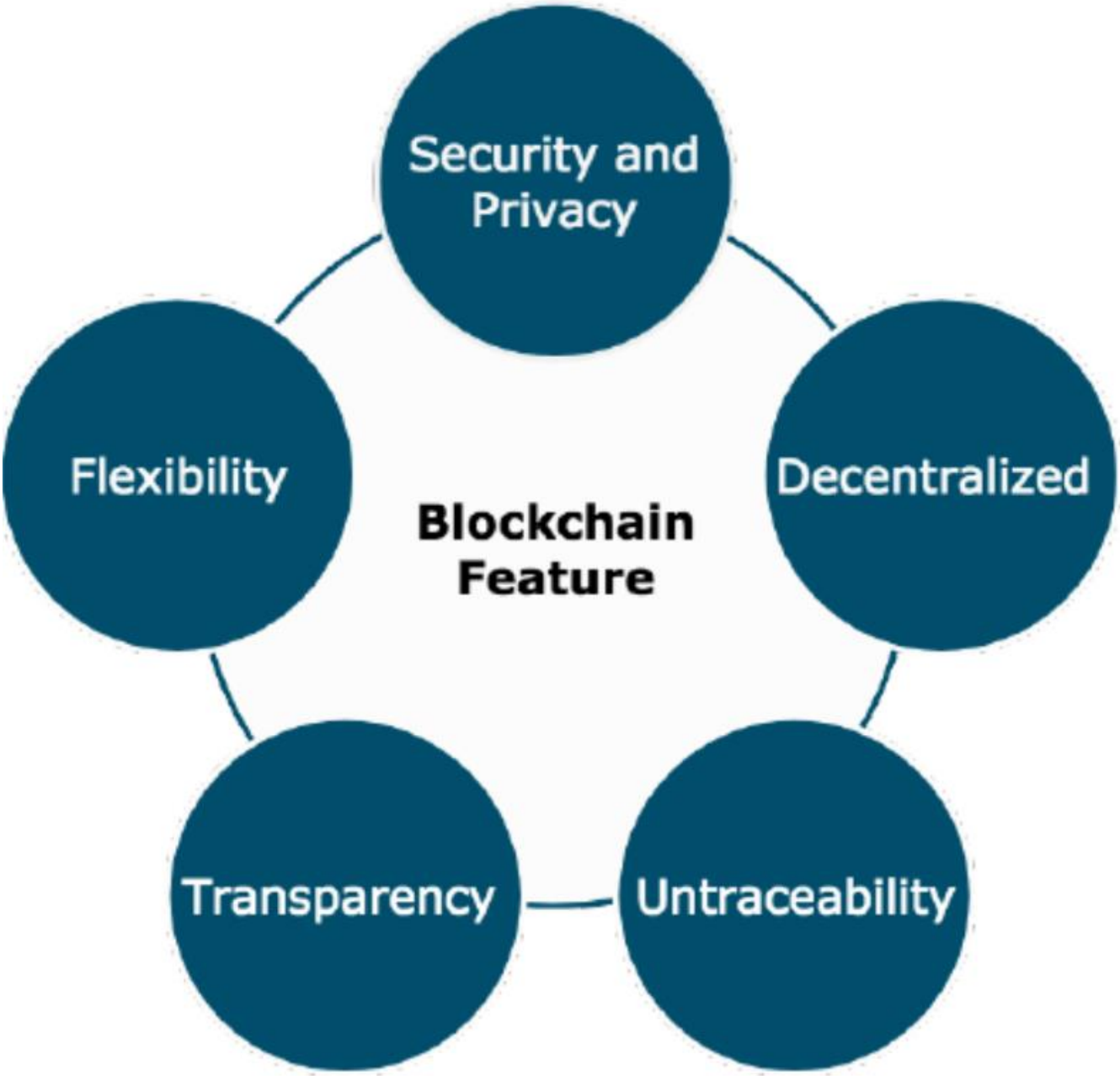

Figure 2. characteristics of Blockchain

The need for blockchain technology keeps rising, and many of the platforms are going mainstream. Among these, enterprises are more than ever eager to go for blockchain solutions, and they are willing to put a considerable number of resources into that. Platforms like Hyperledger Fabric and Ethereum are already making headlines every day. Both platforms are hugely famous for their unique structures. More so, both offer a lot of features that can change or reshape the way of our business models. but we will focus on Ethereum as it used in our project.

2.1.3 Ethereum

Ethereum is an open source Blockchain platform that allows the creation of decentralized applications, and It is a distributed public blockchain network. Ethereum Blockchain focusses on providing a platform for seamless running of codes for any decentralized application.

Unlike Bitcoin, Ethereum Blockchain allows the miners to work to earn Ether. Ether is a token that will enable the entire system function. In the Ethereum blockchain, there is another type of token which is used to pay the miners; it is known as gas. Every smart contact for its execution requires a certain amount of gas to be sent to the miners to put it in the Blockchain.

Ethereum was created to enable developers to build and publish **smart contracts** and distributed applications (dapps) that can be used without the risks of downtime, fraud, or interference from a third party. Ethereum describes itself as "the world's programmable blockchain."

2.1.4 Smart contract

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

It is a special kind of program that encodes business logic that runs on a special-purpose virtual machine baked into a blockchain or other type of distributed ledger. Blockchain is ideal for storing smart contracts because of the technology's security and immutability. Smart contract data is encrypted on a shared ledger, making it virtually impossible to lose the information stored in the blocks.

Flexibility is another advantage of blockchain technology being incorporated into smart contracts. Developers can store almost any type of data in a blockchain, and they have a wide variety of transaction options to choose from.

Blockchain-based smart contracts are helping make transactions and other business processes more secure, efficient, and cost-effective, thereby reducing transaction costs.

The most popular smart contract platform is Ethereum, which is also a widely used cryptocurrency platform. The Ethereum community has developed the **Solidity language** for writing smart contract applications that are designed to run on the Ethereum Virtual Machine (EVM) execution environment.

There are several potential business advantages from using smart contracts:

- **Cost efficiency:** Smart contracts promise to automate business processes that span organizational boundaries. This can eliminate many operational expenses and save resources, including the personnel needed to monitor the progress of a complex process that executes in response to conditions that span companies.
- **Processing speed:** Smart contracts can improve the processing speed of business processes that run across multiple enterprises.
- **Autonomy:** Smart contracts are performed automatically by the network and reduce the need for a third party to manage transactions between businesses.
- **Reliability:** Smart contracts can also take advantage of blockchain ledgers and other distributed ledger technologies to maintain a verifiable record of all activity related to execution of complex processes and that cannot be changed after the fact. It also supports automated transactions that remove the potential for human error and ensure accuracy in executing the contracts.

2.1.5 Solidity language

is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behavior of accounts within the Ethereum state.

Solidity was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM).

Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

2.2 Surveying Procedure

Before implementing any project, you must go through the surveying process, to know if your system is strongly needed by the users, what type of users are you targeting, how people think about your system, **our surveying process is summarized into the following steps:**

- Asking people about the thoughts of the project
- Asking people for enhancement ideas to be added
- Asking people about their opinion towards our interface and their ideas to be simpler and more appealing
- Learning from past experiences and checking peoples reviews on the similar applications in order to avoid other's faults.
- Checking the field's top algorithms and comparing them to each other in terms of (speed, accuracy, reliability)
- Checking professional developer's reviews about the implementation process and what do first and how to start the implementation process without any complications.

2.3 Challenges

Now since the outlines are clear, we started building up the projects step by step, of course we predicted some of the challenges in the beginning, but some of them were unexpected and arouse during the implementation process, here are some of the challenges we faced: With multiple entry points and so many loopholes and absence of a transparent and robust security system, tracking the drug supply chain has become a herculean task.

The hindrances to the present supply chain system are as follows:

- Absence of unified and inter-operable labeling and identifications standard.
- Soiled, fractured, and opaque supply chain infrastructure. There is no easy and clear way to track down the product's journey in the supply chain that can unveil the real origin and hand-off points.
- Improper monitoring and management of cold chain supply.
- Hand-offs between various parties, including packager and transport agencies, as the drugs are transferred between multiple stages, which could be the possible points of entry of spurious drugs.
- Different systems have been adopted by different manufacturers. This leads to a compatible problem where the distributors and transport agencies to keep different type of solutions along their supply chain systems. Which can cause a confusion in the information or delivery of the drugs and eventually risk to consumer.

2.4 Proposed Model

Basically, we can divide the whole drug supply chain from the manufacturers to the

consumers into six parties:

1. Manufacturer
2. Distributor
3. Transporter
4. Pharmacy
5. Hospital
6. Consumer.

The model can be described as follows. The manufacturer sends the drugs to the distributor or to the transport agency according to their requirement. The distributor can directly collect drugs from the manufacturer or order it through a transport agency.

The distributor sends drugs to hospitals and pharmacies again through the transport agencies. If the hospital's requirement is very large, it can directly order from the manufacturer through transport agency, or it can collect drugs from the distributor directly. The smaller hospitals can order drugs from their nearby pharmacies. At last, the consumer or patient will get the drugs either from the hospital or from the pharmacy store. Excluding the last party (the consumer), a blockchain framework can be created among the first five parties. It is obvious question that the last party, which is the consumer, must be kept out of the blockchain. This is because every node in

the blockchain framework participates in the transaction verifying process.

The consumer community is very diverse from illiterate to highly educated, from high school kid to senior citizens, from a person who lives in a remote area to the person who lives in a city, so they all cannot participate in the transaction verifying procedure.
And one more thing is that if every consumer is added to the blockchain framework, then the system will be heavily loaded as there are billions of consumers in our nation. Managing such a huge data will be expensive, and the complexity will also increase. But there is a platform where every consumer can check the authenticity of the drug, which has been discussed later in this section. As our traditional system consists of some loopholes, so a decentralized blockchain framework is to be created with a shared distributed ledger with the five entities. Each entity should be verified before adding them into the blockchain framework. First, all the drug manufacturers must have to be certified by the Central Drugs Standard Control Organization (CDSCO). Each manufacturer should have a unique id. The drug manufacturer should be a trusted entity. It must make sure that all the registered manufacturers produce genuine drugs, and the Government of country must take responsibility of the genuineness. Once a drug is produced, it must be labeled by the unique id of the manufacturers, the drug name, the composition of the drug and the other details. The drug information is added to the shared ledger with all the details of the drug. Now, the manufacturer will transfer the drugs to the distributor.

All the distributors registered in the blockchain should also be assigned with a unique id. During the hand-off from manufacturers to distributor, both parties should digitally sign using their private keys in the distributed ledger, and the transaction is added to the block. And all the entities in blockchain should verify the

transaction before adding another transaction so that no one can deny or tamper this transaction in future. Now the only objective of the distributor is to distribute the drugs according to the requirement of hospitals and pharmacy stores through transport agencies.

Once the distributor receives the drugs from the manufacturer, all the parties in the blockchain will know that distributor has received the drugs. The transport agency will now take the drugs from the distributor to pharmacy stores and hospitals.

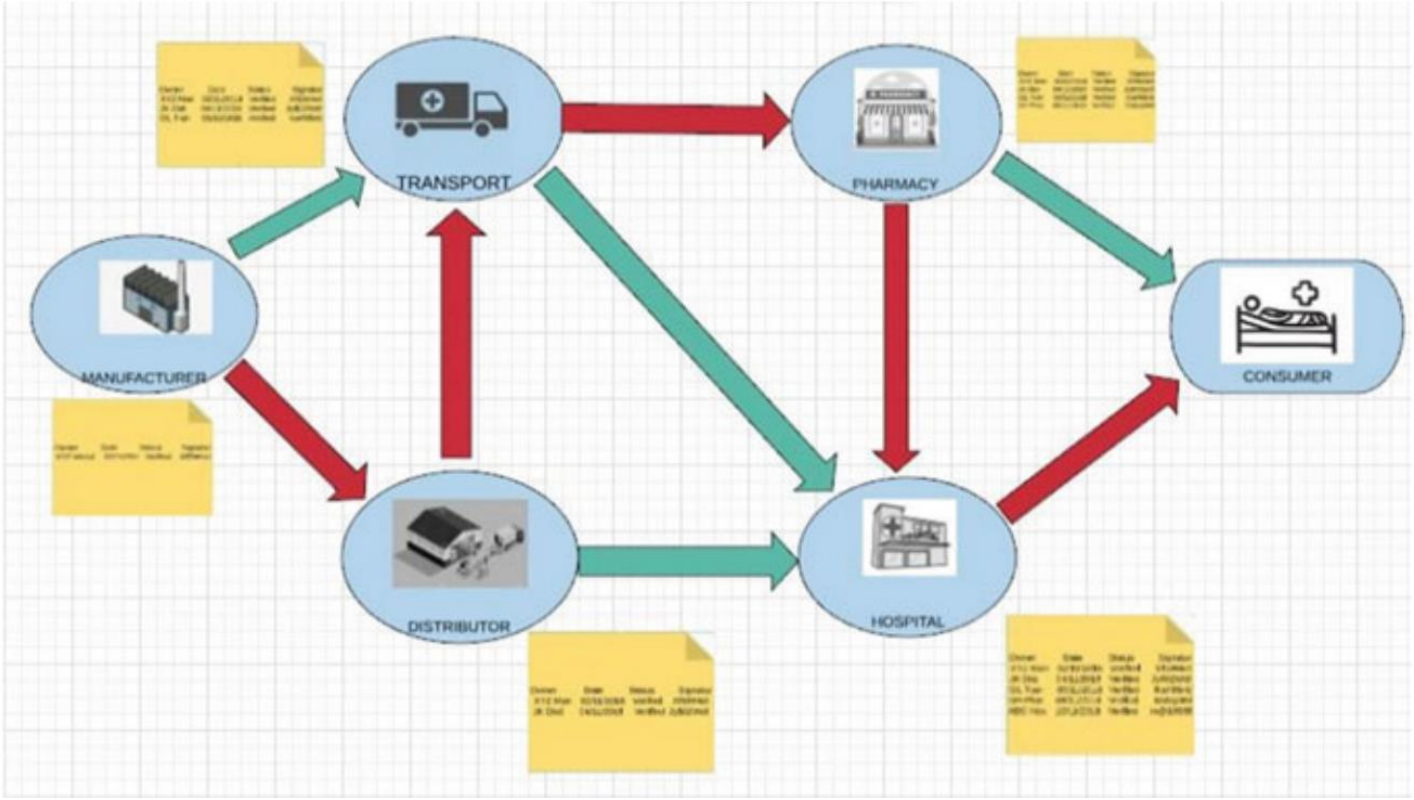

Fig. 3 Blockchain-based drugs supply chain architecture

Chapter 3

Related Work

As said “Never interrupt your enemy when he is making a mistake.” by - **Napoléon Bonaparte**

it means that you must look at what have other’s done and avoid these mistakes and solve it in your own way, before starting we searched for similar applications and started using them like any other users and we started the process of testing these applications to find out what are the cons of these applications, here what we find out:

- **NAIROBI**

  A cell phone application for identifying approved medicines and drugstores is helping Kenya to fight counterfeit and substandard medicines. The app uses a barcode and location tracking technology to identify medicines throughout the supply chain.

- **FD Detector**

  a group of local teenage girls from Nigeria decided to act and create a mobile application that detects fake drugs at the point of purchase. The app allows health professionals and customers with a smartphone to scan the barcode in a drug. The app then indicates whether the drug is authentic or fake and displays the drug’s expiry date. The innovation also has a provision for users to report any fake drugs directly to the regulator.

Chapter 4

Analysis and Design

This chapter presents the outcomes of the analysis and design phases of the project. It discusses the functional and nonfunctional requirements of the system.

4.1. System Overview: -

4.1.1. System Architecture:

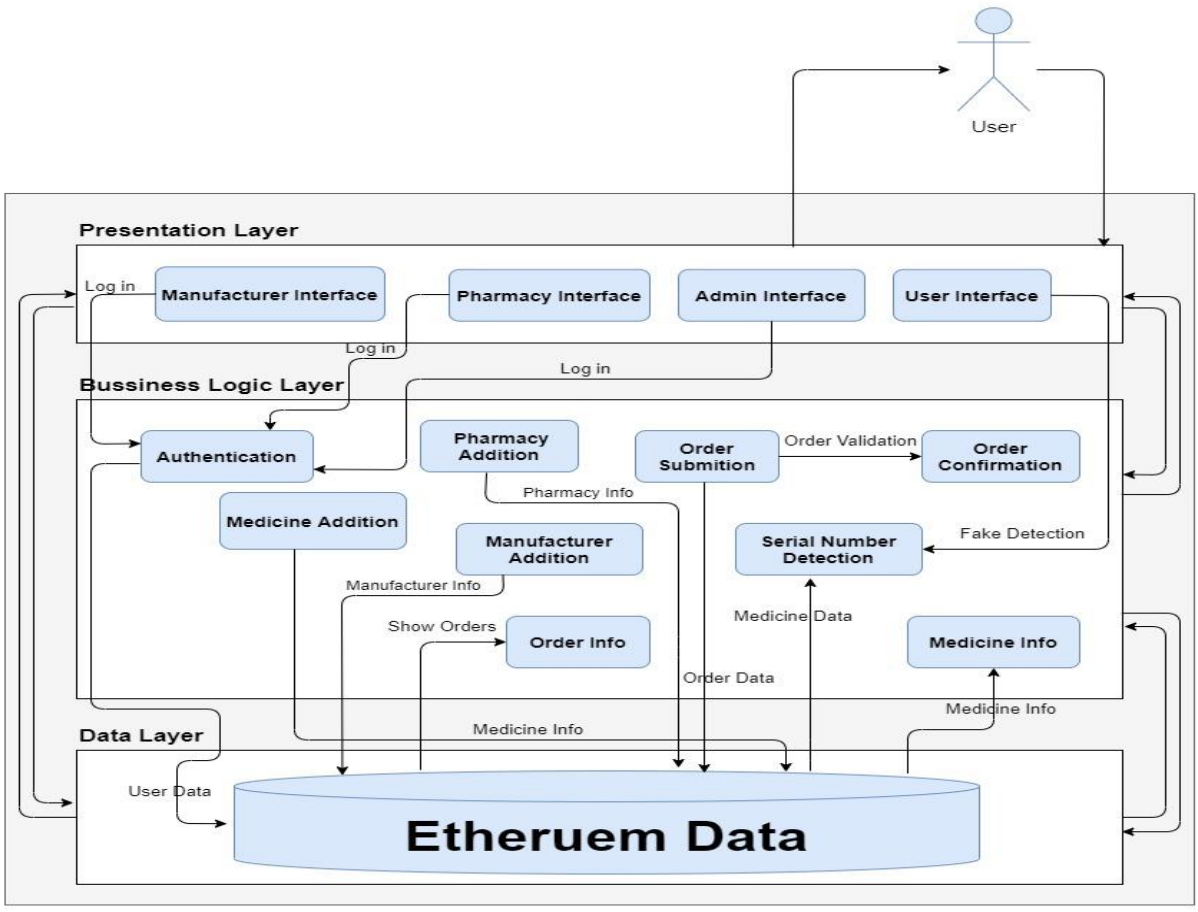

Fig. 4 System Architecture

- **Presentation Layer:**

  It is the front layer in the system architecture where the user interacts with the applications through the interface, it includes manufacturer interface, user interface, pharmacy interface and admin interface.

- **Business logic layer:**

  It is the middle layer in the system architecture which contains the business logic that supports the application's core functions. This layer includes the following **main functionalities:**

  - **Authentication:**

    to verify user information.

  - **pharmacy addition and manufacturer addition:**

    the admin can add them in data Ethereum.

  - **medicine addition:**

    The manufacturer can insert the medicine in data Ethereum.

  - **order submission:**

    The pharmacy can select the available medicine and send order to manufacturer.

  - **order confirmation:**

    when the pharmacy send order to manufacture, the manufacturer can accept or reject order.

  - **serial number detection:**

The user can enter the serial number of the medicine know the fake medicine from the real

- **Data Layer:**

It is the bottom layer in the system architecture, this layer is used to store data needed by the system and includes data Ethereum.

4.1.2. Functional Requirements:

1- Manufacturer:

- **Request to join:**

Description:

This function allows unregistered Manufacturer to enroll and to create a new account with the website, in order to create a new account, the Manufacturer has to provide required information to admin Such as username, and password.

Input:

username and password.

Source:

Manufacturer.

Pre-conditions:

The manufacturer must not have an existing account with the website.

Post-conditions:

A manufacturer account is created.

Output: None.

➢ Login/Logout:

Description:

This function allows a registered Manufacturer to login this account and log out after the work is done.

Input:

The manufacturer of the website logs into the application with the username and password provided him.

Source:

Manufacturer.

Pre-conditions:

manufacturer is not logged in to system. Manufacturer has previously
enrolled in the system.

Post-conditions:

Manufacturer is logged in to system, OR Manufacturer is not logged in because he/she entered unrecognized information.

Output:

The website displays the homepage of the Manufacturer.

➢ Insert Medication:

Description:
This function allows the Manufacturer to add medicine information in the data Ethereum.
Input:
The Medicine information (Name, Serial Number, Production Date, Expire Date).
Source:
Manufacturer.
Pre-conditions:
The manufacturer must have an account with the website.
Post-conditions:
Medicine information has added in the data Ethereum by manufacturer.
Output:
None.

➢ Confirm order:

Description:
This function allows the Manufacturer to accept or reject the order that is sent from pharmacy.
Input:
None.
Source:
Manufacturer.
Pre-conditions:
The manufacturer must have an account with the website.
Post-conditions:
Order has accepted or rejected.
Output:
None.

➢ Show order and medicine:

Description:
This function allows the Manufacturer to view the medicine information that has added from manufacturer or order that has sent from pharmacy.
Input:
None
Source:
System
Pre-conditions:
The manufacturer must have an account with the website.
Post-conditions:
None.
Output:
Show all information about available medicine or order.

2- Pharmacy:

- **Request to join:**

Description:

This function allows unregistered pharmacy to enroll and to create a new account with the website, in order to create a new account, the pharmacy has to provide required information to admin Such as username, and password.

Input:

username and password.

Source:

Pharmacy

Pre-conditions:

The Pharmacy must not have an existing account with the website.

Post-conditions:

A Pharmacy account is created.

Output:

None.

➢ Login/Logout:

Description:

This function allows a registered Pharmacy to login this account and logout after the work is done.

Input:
The Pharmacy of the website logs into the application with the username and password provided to him.
Source:
Pharmacy.
Pre-conditions:
Pharmacy is not logged in to system. Pharmacy has previously enrolled in the system.
Post-conditions:
Pharmacy is logged in to system, OR
Pharmacy is not logged in because he/she entered. unrecognized information.
Output:
The website displays the homepage of the Pharmacy.

➢ Show medicine:

Description:
This function allows the pharmacy to view the medicine information that has added from manufacturer.
Input:
None
Source:
System
Pre-conditions:
The pharmacy must have an account with the website.
Post-conditions:
None.
Output:
Show all information about available medicine.

➢ Send order:

Description:
This function allows the pharmacy to select available medicine and send order to manufacturer.
Input:
available medicine that is selected.
Source:
pharmacy.
Pre-conditions:
The pharmacy must have an account with the website.
Post-conditions:
the manufacturer has accepted or rejected the order from pharmacy.
Output:
None.

➢ Detect Medicine:

Description:
This function allows the pharmacy to detect medicine, is it fake or real through enter the serial number for medicine.
Input:
serial number for medicine
Source:
pharmacy.
Pre-conditions:
None.
Post-conditions:
None.
Output:
Show the medicine information if the serial number is unique and the medicine is real or message "the medicine is fake " if the serial number is not unique.

3- User:

➢ Detect Medicine:

Description:
This function allows the user to detect medicine, is it fake or real through enter the serial number for medicine.
Input:
Serial number for medicine
Source:
user.
Pre-conditions:
None.
Post-conditions:
None.
Output:
Show the medicine information if the serial number is unique and the medicine is real or message "the medicine is fake " if the serial number is not unique.

4.1.3. Non-Functional Requirements:

The System was designed to fulfill the following non-functional requirements.

- **Performance:**
  - Response time should be less than 2 second most of the time. Response time refers to the waiting time while the system accesses, queries and retrieves the information from the data Ethereum.
  - The system shall show no visible deterioration in response time as the number of users.

- **Security Requirements:**
  - There is several middleware used to allow the access to authenticated users to send reviews and view their profile also it prevents the non-admin users from using the admin's dashboard interface.

- **Software Quality Attributes:**
  - The system is very user friendly, interoperable and flexible.

- **Reliability:**
  - System shall be available 24 hours a day, 7 days a week.
  - System shall always provide real time information about medicine.
  - System shall be robust enough to have a high degree of fault tolerance.
  - the system should not crash and shall system the invalid input and produce a suitable error message.

- **Supportability:**
  - The code and supporting modules of the system will be well documented and easy to understand.

➢ Usability:

- System shall provide an easy-to-use graphical interface so that the users do not have to learn a new style of interaction.
- The web interface should be intuitive and easily navigable Users should be able to understand the menu and options provided by system.
- Any notification or error messages generated by system shall be clear, succinct, polite and free of jargon.

➢ Integrity:

- Only system administer has the right to change system parameters. The system should be secure and must use blockchain to protect the data.
- Users need to be authenticated before having access to any personal data.

➢ Availability:

- Users can interact with the application from any place around the world at any time.

4.1.4 System Users:

➢ Intended Users:

The system is built for normal users and administrators.

- Normal users are able to enter the serial number of medicine and receive all possible medicine information if the medicine is real.
- Administrators are able to manage the whole system including all users, pharmacy and manufacturer.

➢ User Characteristics:

This system does not require any skills as its main purpose is to be for everyone regardless of his characteristic.

4.2. System Analysis and Design:

4.2.1. Use Case Diagram:

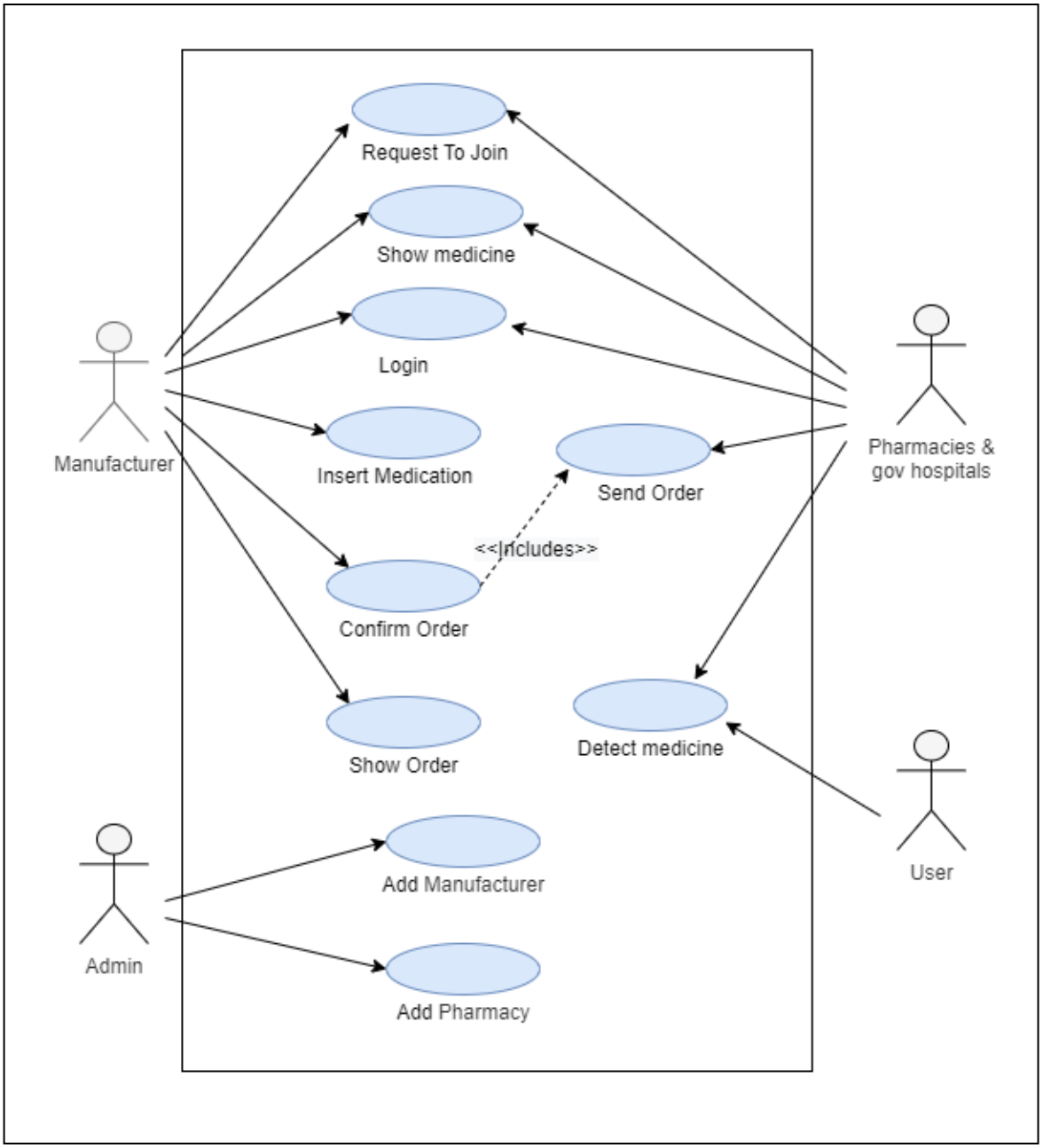

Fig. 5 use case Diagram

4.2.2. Class Diagram:

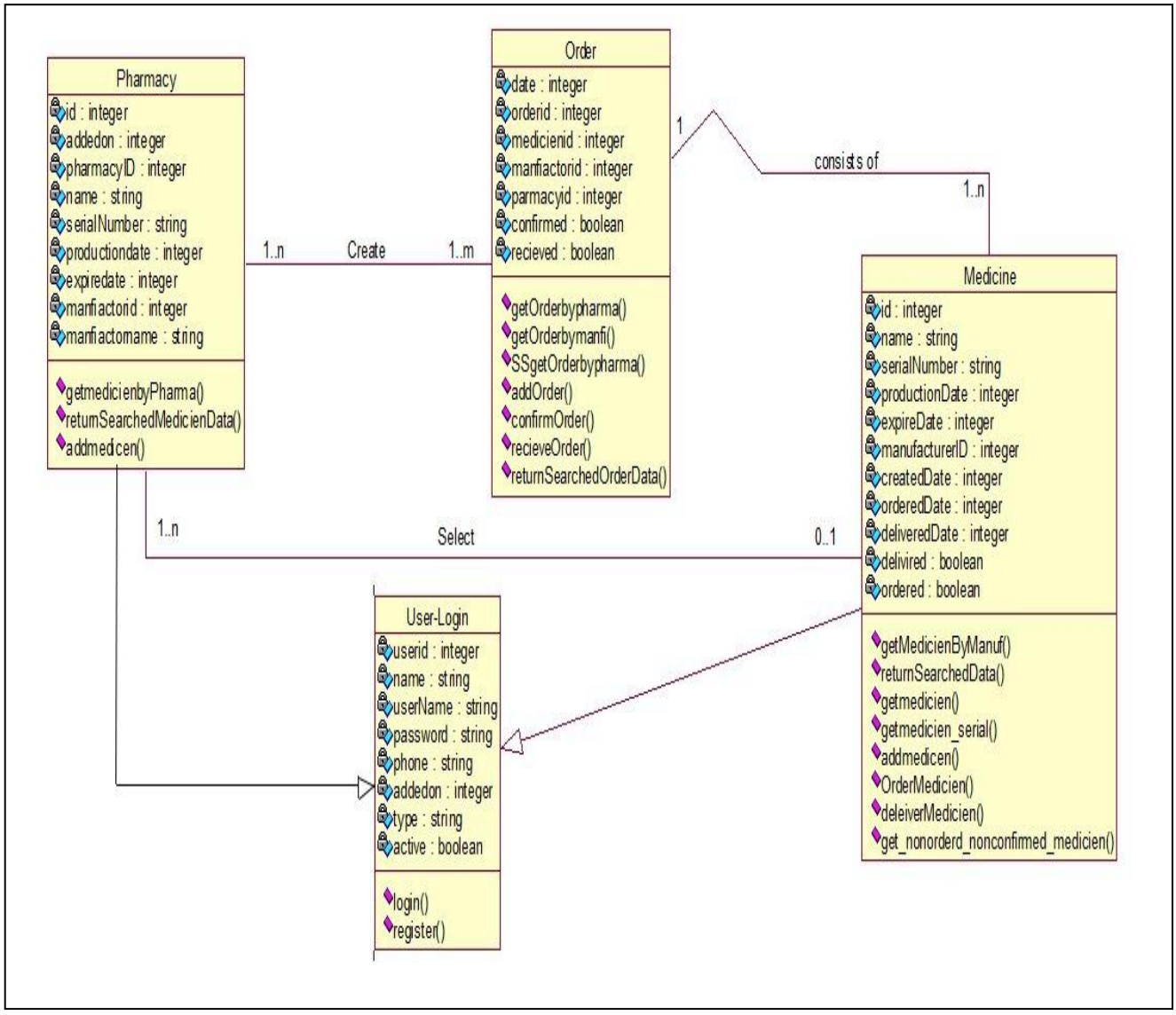

Fig. 6 Class Diagram

4.2.3. Sequence Diagram for send order:

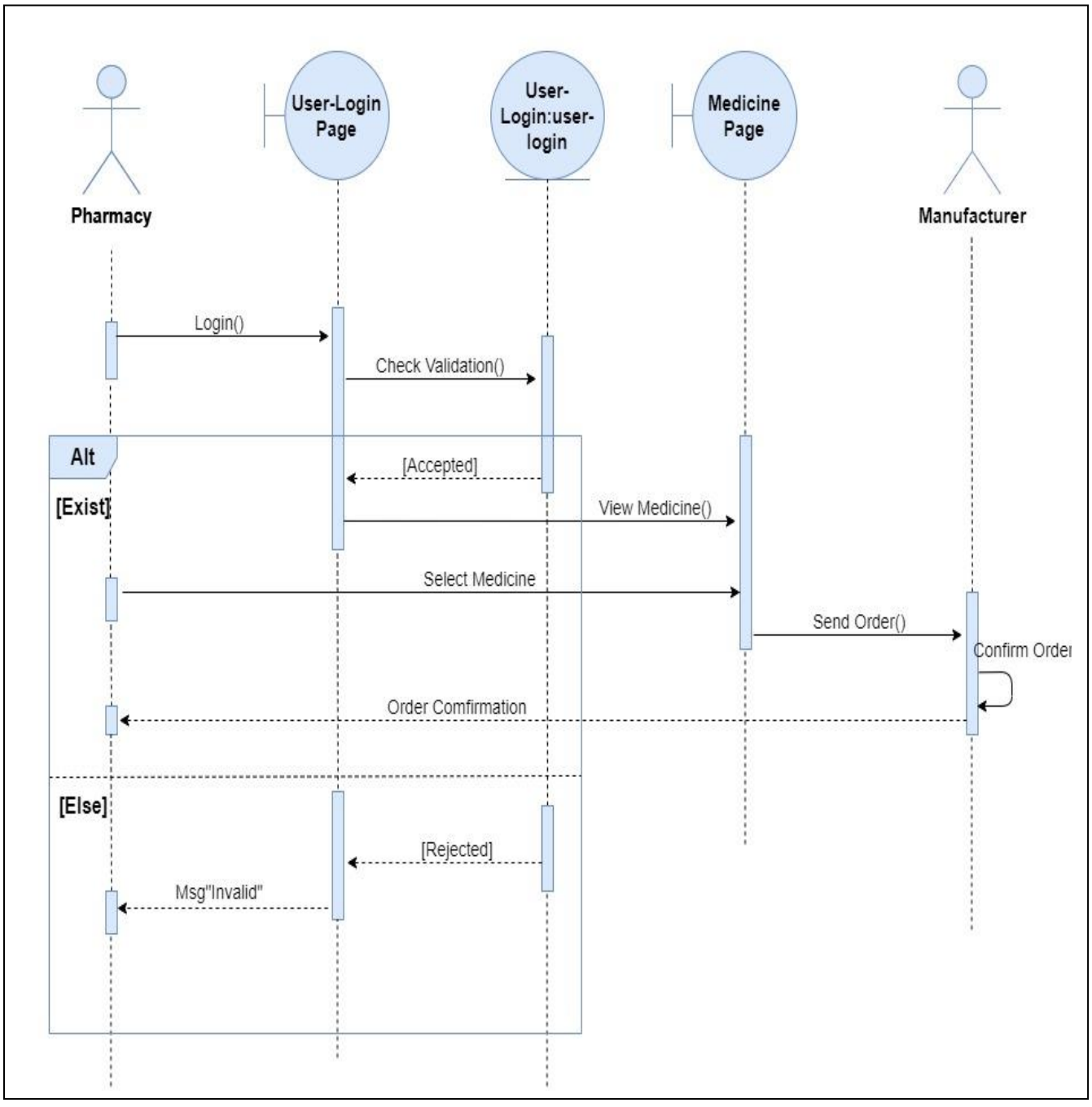

Fig. 7 Sequence Diagram for send order

4.2.4. Sequence diagram for detect medicine:

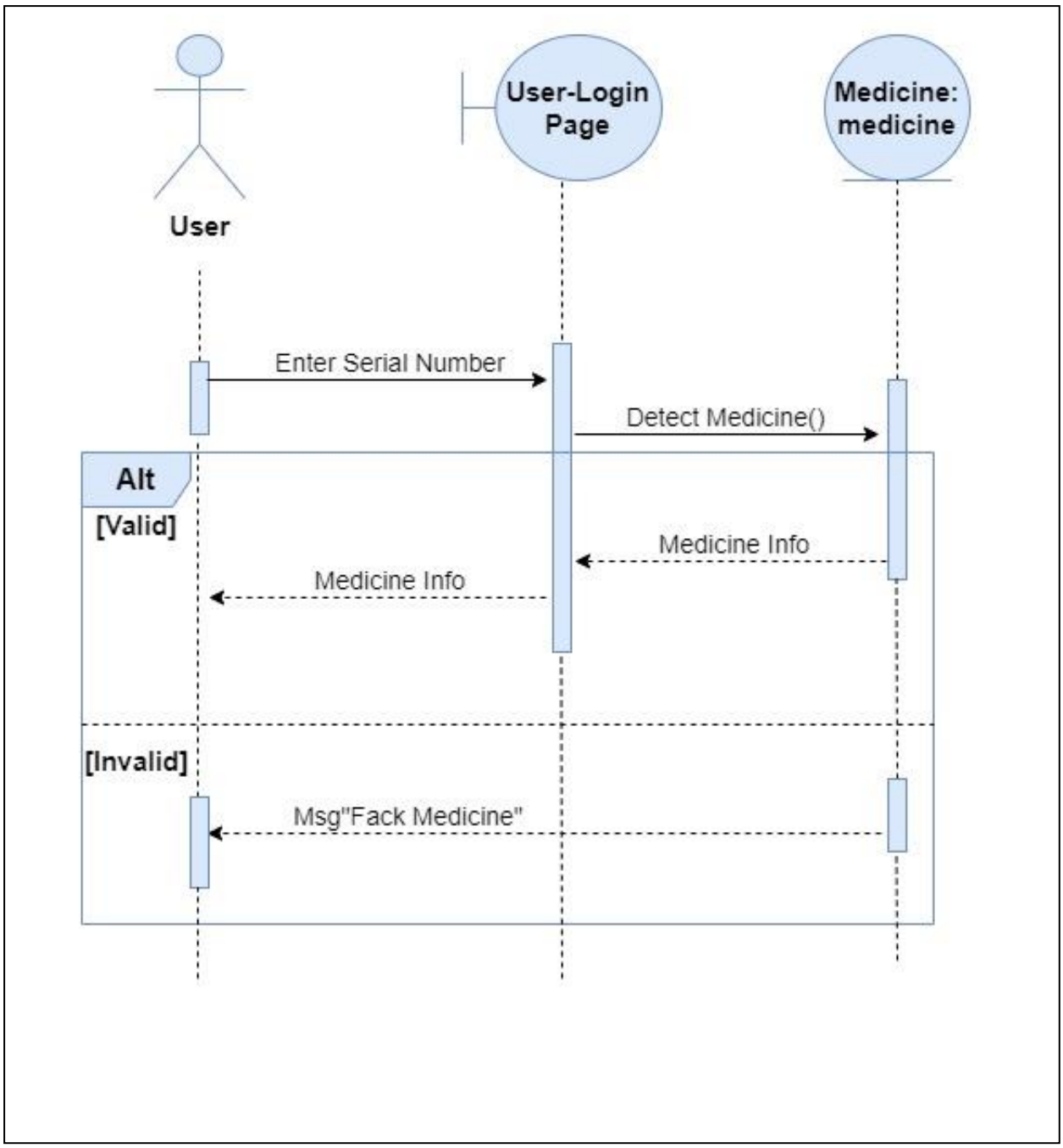

Fig. 8 sequence diagram for detect medicine.

Chapter 5

Implementation

This chapter explains all the functions in the system, the technologies and tools used in the implementation of the system.

5.1 Description of all the functions in the system

5.1.1 Registration functions:

a) Sign-up

- In case Admin want to add new pharmacy to system, he will enter the username, password, Name, Phone of Pharmacy.
- In case Admin want to add new manufacture to system, he will enter the username, password, Name, Phone of manufacture.
- The system will check and validate all fields and reject any duplicates in emails.
- When the user clicks on the sign-up button, redirect to his/her Login Page.

b) Login

- First the user will enter username and password.
- The system will check if the user credentials and whether it is in the database or not.
- If the values of username and password found in the blockchain database and choose Pharmacy or Manufacturer or Admin option, then new session will be established for the user and will be redirected to the selected page else display error message.

5.1.2 Pharmacy functions

a) All Available Medicines:

- This function Display all medicines from all manufacturers to select them and add them to cart.

b) All Orders:

- This function displays the ordered medicines and need the confirmation of the manufacturers.

c) My Medicines:

- This function displays all the medicine in the stock of the pharmacy.

d) Cart:

- This function stores the list of medicines from manufacturers that pharmacies want to buy. And confirm the list to be send to manufacturers.

5.1.3. Manufacturers functions

a) Add Medicines:

- This function is implemented to add new medicines to blockchain system, so no one can change the medicine data after inserted it.

b) All Medicines:

- This function is implemented to display all inserted medicine for each manufacture from blockchain directly.

c) All Orders:

- This function is implemented to display all orders that are needed by hospitals and pharmacies and waiting confirmation form manufactures to send them.

5.1.4. Detect Medicines

a) Check counterfeit Medicines:

- This function allows the pharmacy to detect medicine, is it fake or real through enter the serial number for medicine then show the medicine information if the serial number is unique and the medicine is real or message "the medicine is fake " if the serial number is not unique.

5.1.5. Admin functions

a) View Reviews:

- This function allows the admin to see all the reviews and all the users who sent these reviews and check the every pharmacy and manufacture and make sure that they have all papers and licenses to join to system.

b) Adding Manufacture:

- The function allows the admin to add a Manufactures to system, so they are able to add their medicines to blockchain.

c) Adding Pharmacies

- This allows the admin to add a Pharmacies to system, so they are able to buy their medicines from blockchain and make orders easily.

5.2 Description of all the techniques implemented

5.2.1. Languages and framework used:

Front end	Back end
HTML and CSS	Ethereum
Java script	Solidity
React	Web3.js

5.2.2. Algorithm and techniques:

- Our main concept is encryption data by way that prevent anyone changing or delete it so blockchain use an efficient algorithm for encryption it's sha 256 and Blockchain consensus algorithms.

- SHA-256, or Secure Hash Algorithm 256, is a hashing algorithm used to convert text of any length into a fixed-size string of 256 bits (32 bytes). Originally published in 2001, SHA-256 was developed by the US Government's National Security Agency (NSA). This algorithm is commonly used in SSL certificates for websites and in the DKIM message signing standard for email clients.

- SHA-256, like other hash functions, takes any input and produces an output (often called a hash) of fixed length. It doesn't matter if the input is a single word, a full sentence, a page from a book, or an entire book, the output of a hashing algorithm like SHA256 will always be the same length. Specifically, it will be 256 bits, which is 32 bytes, which is displayed as 64 alphanumeric characters. All outputs appear completely random and offer no information about the input that created it.

- Other important characteristics of SHA-256 include the fact that it is deterministic (it will always produce the same output when given the same input) and the fact that it is a one-way function. There is no way to reverse engineer an input from knowledge of the output. Lastly, SHA-256 is computationally efficient and an ordinary computer can perform the operation dozens or even hundreds of times per second.

- Blockchain Consensus algorithms ensure each new block added to the network is the only version of the truth, which is agreed by all the nodes in a distributed/decentralized computing network consensus algorithm is a mechanism in computer science used to establish agreement on a single data value across distributed processes or systems. A consensus algorithm is a protocol through which all the parties of the blockchain network come to a common agreement (consensus) on the present data state of the ledger and be able to trust unknown peers in a distributed computing environment. For blockchain networks, the consensus algorithms are an essential element because they maintain the integrity and security of these distributed computing systems, **now we'll look at the one of blockchain consensus algorithm that are used in Blockchain:**

  - Proof Of Work (PoW) Based Blockchain Consensus is the process of producing a cryptographic hash In a PoW system, blockchain validators must take data from a block header as an input, and continuously run it through a cryptographic hash function. Validators hash slight variations of the input data by including an arbitrary number called a nonce every time the input data is run through the cryptographic hash function. PoW needs high levels of electricity of processing power to decide what data gets added to the next block in a blockchain. Specialized computers called ASICs are required to compute complex mathematical problems needed for the PoW system.

Technique of Execution In system

- Ethereum is a Blockchain platform that can build smart contracts using a Turing completeness programming language. Anyone can write smart contracts or other decentralized applications on Ethereum. Users can set access permissions, transaction formats, state conversion equations, and soon, and build any desired rules. Users of Ethereum will first write a smart contract using Solidity, then they will change their smart contract Solidity code into Ethereum bytecode, add the bytecode into a transaction and deploy the transaction into the network. When miners of Ethereum receive the transaction, they will record the transaction in a block and run the bytecode in the Ethereum virtual machine each time a transaction of this smart contract is called.

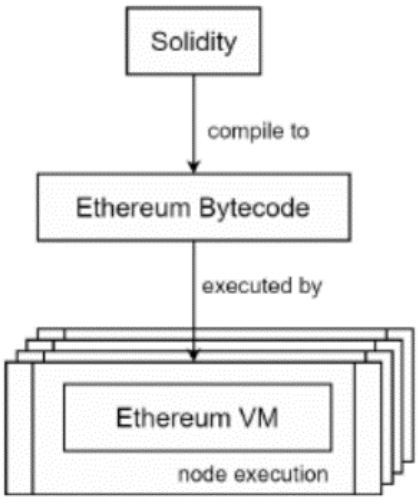

Figure 9. state change in Ethereum smart contract

- To interact with a smart contract on Ethereum, the user has to send the information packaged in a transaction to communicate with the smart contract and interact with the smart contract by following the rule established within the smart contract. If successful, the smart contract will then have state changed on each miner's local storage

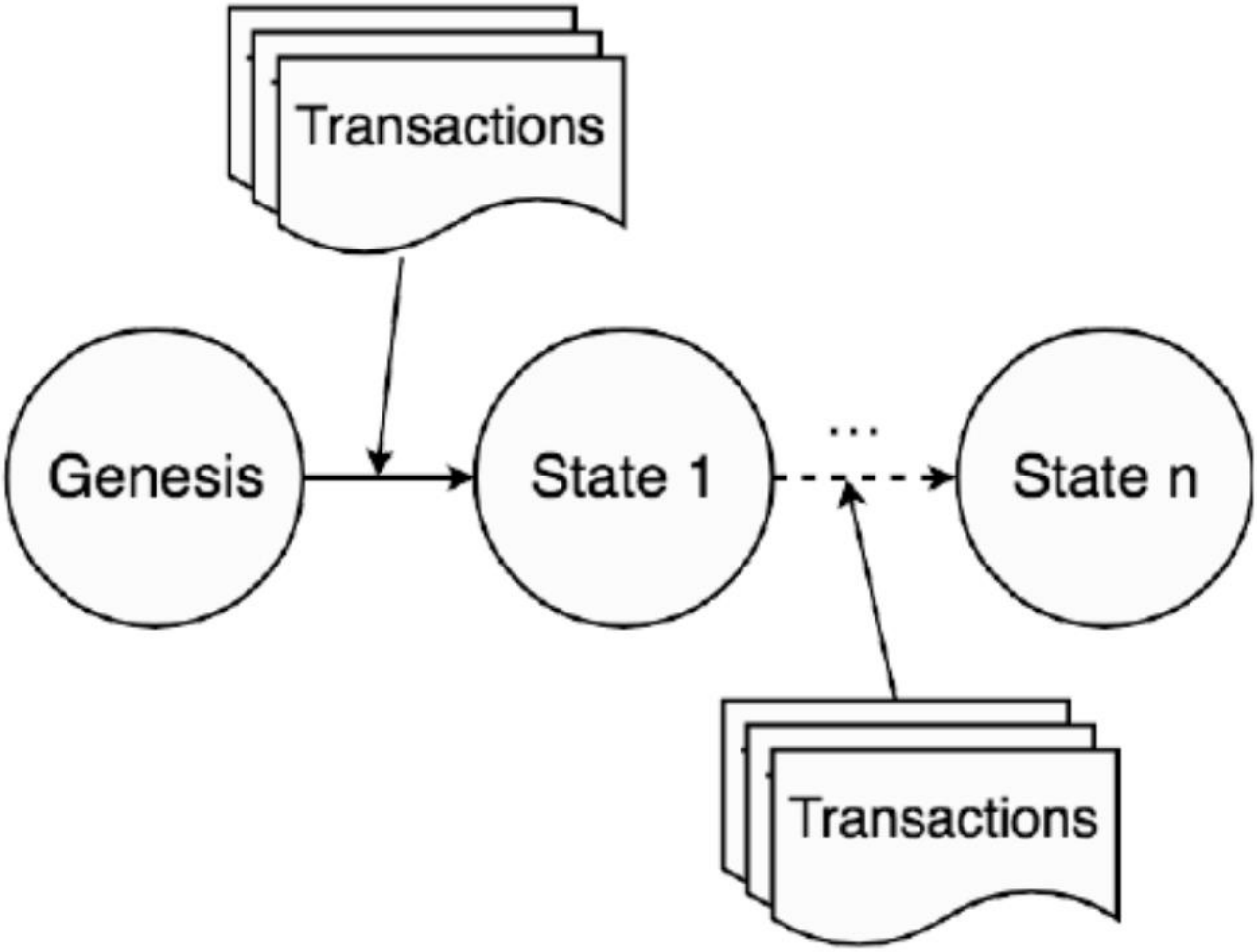

Figure 10. Architecture overview of our system

- The proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts. Solidity supports inheritance, libraries importing, etc. Solidity is designed for Ethereum Virtual Machine(EVM), Unlike Bitcoin's scripts, Solidity provides loops and it is Turing complete

- On the system, the public smart contract is based on Ethereum's Blockchain. we use Geth to build a Private chain and push the smart contract on this Private chain, so that the Private chain simulates the situation of the Public chain. Plus use Mist for account balance and contract information management. The user interface seen by the user is a web page. The server side of the web page is made using the http-server suite, which was provided by react.js and web3.js is used as the link between the smart contract and the user interface. The Private Chain and Address information can be connected after setting the server. The overall system relationship is shown in the following diagram.

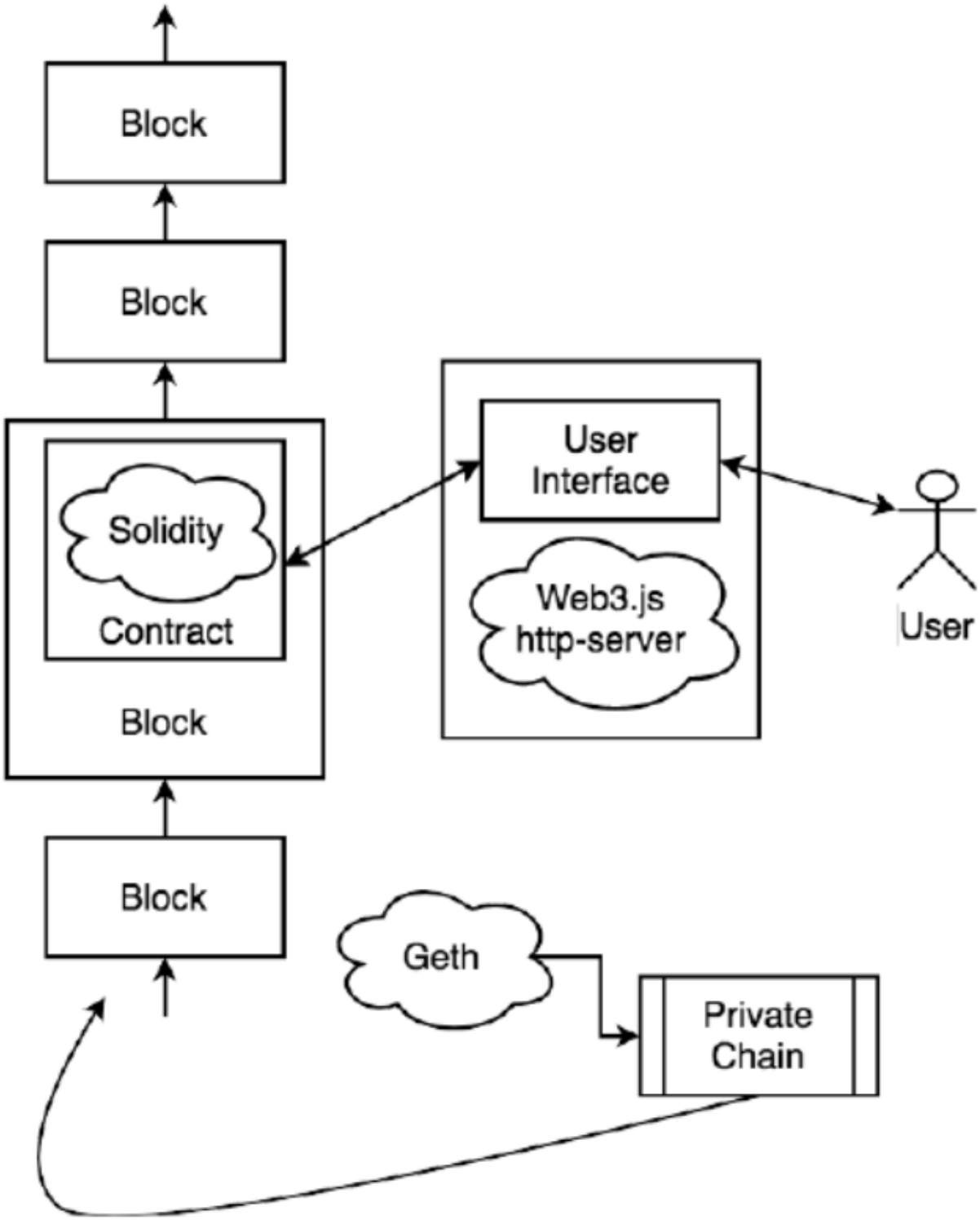

Figure 11. Architecture overview of our system

Chapter 6

User Manual

6.1 Drug's validation check:

a. Input:

i. Drug Serial Number

b. Outputs:

i. Validation result

c. How it works:

i. User should enter the drug's serial number and click search.

ii. If the drug is valid, system will view the tracking of the medicine and the result is valid, if not then the system will view invalid in the result.

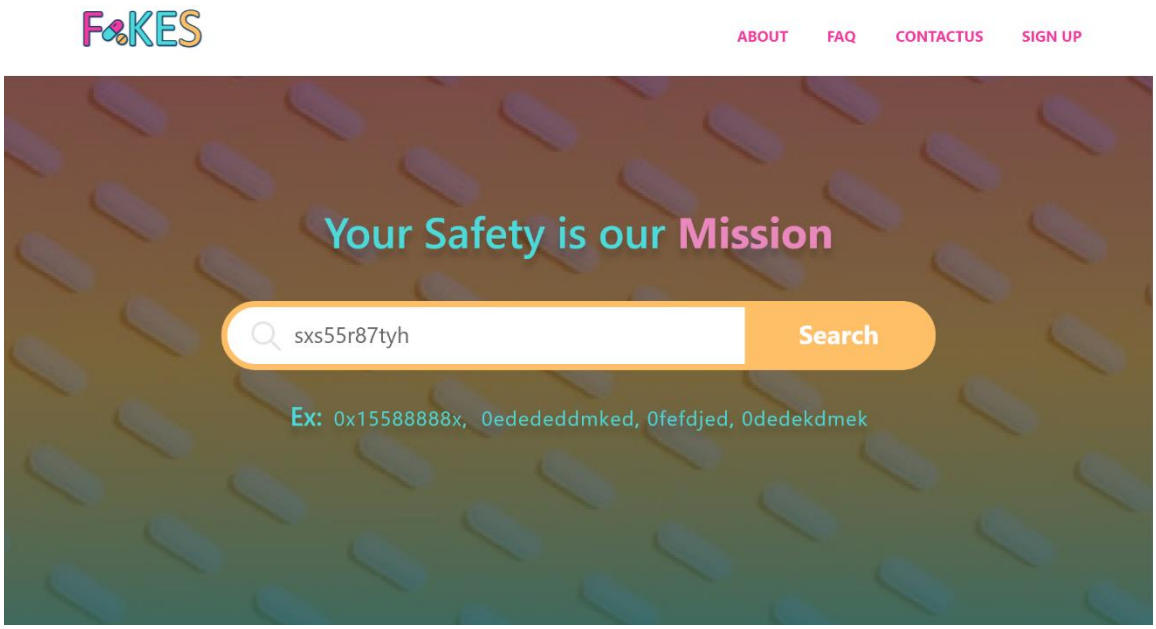

Figure 12 – Drug's validation check

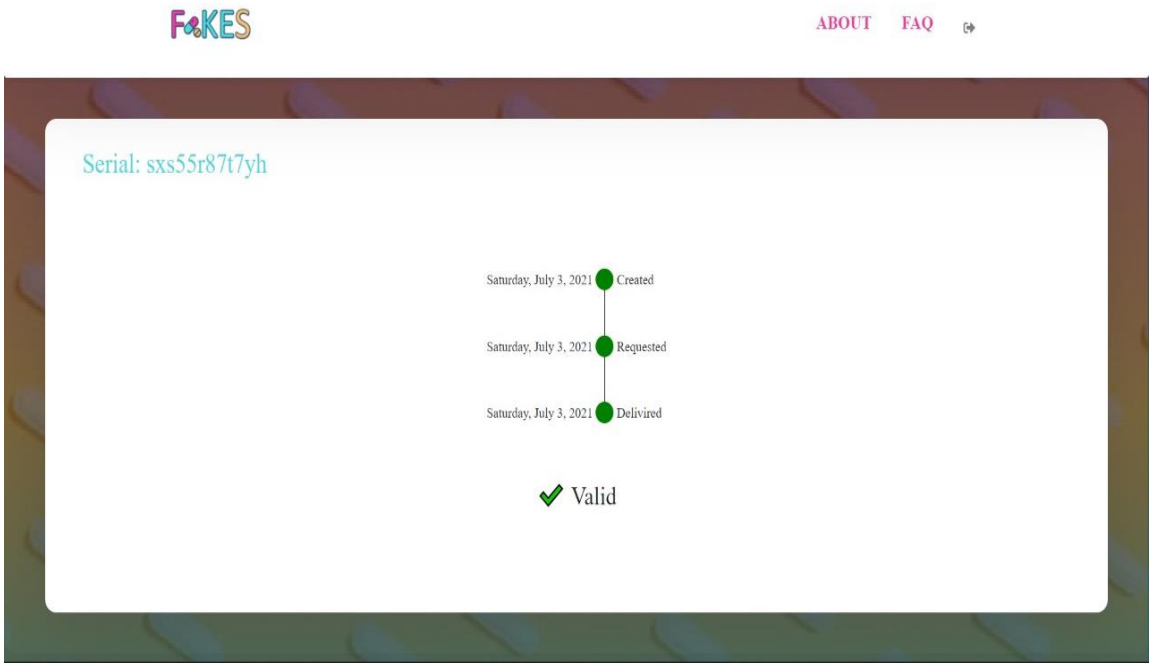

Figure 13 – Drug's validation check result

6.2 Specific User Login:

a. Input:

i. Username.

ii. Password.

iii. User Type.

b. Outputs:

i. Page open according to user type entered.

c. How it works:

i. User should enter the username, password, and type.

ii. If the user is a manufacture, then a manufacture Panel will appear with its tools and options. If the user is a Pharmacy, then a Pharmacy Panel will appear with its tools and options. If the user is an Admin, then an Admin Panel will appear with its tools and options.

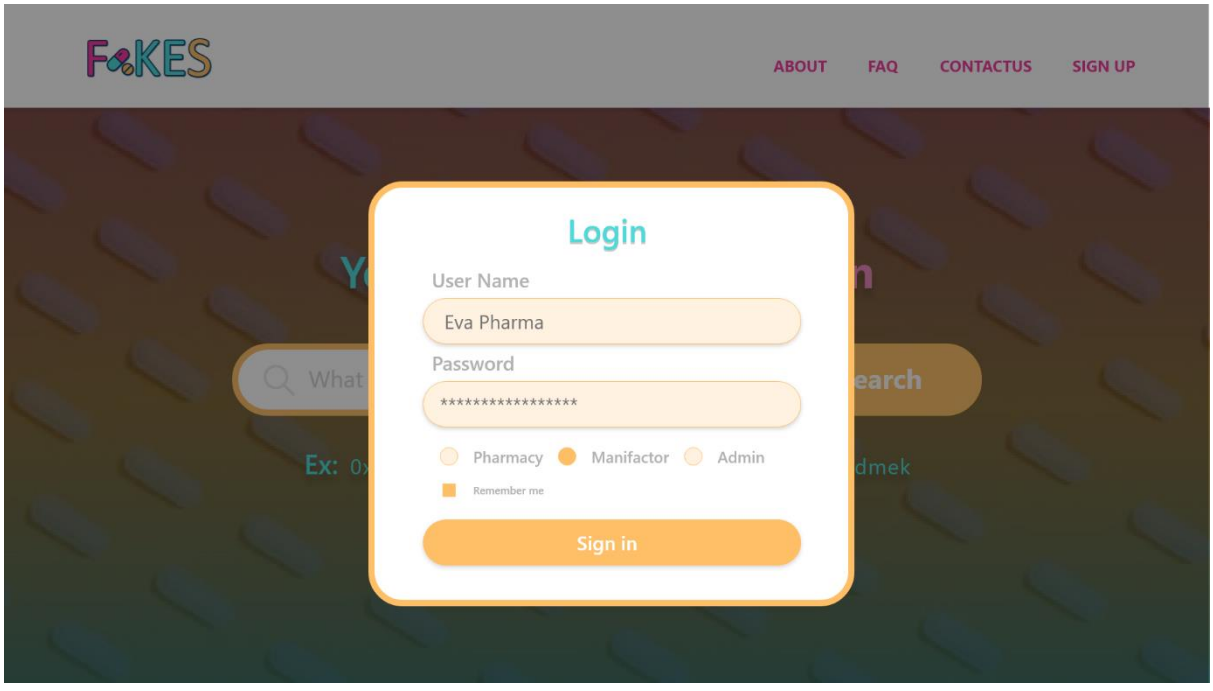

Figure 14 - Login page

6.3. Manufacture Panel:

When a user login as a manufacturer, a panel will open with three options will appear in which.

The three options are: "Add Medicine" , "All Medicines" , "All Orders".

a. Add Medicine:

i. in which user can add a new medicine with its information.

ii. information of medicines is:

1. Drug Name.
2. Drug Serial Number.
3. Drug Production Date.
4. Drug Expire Date.

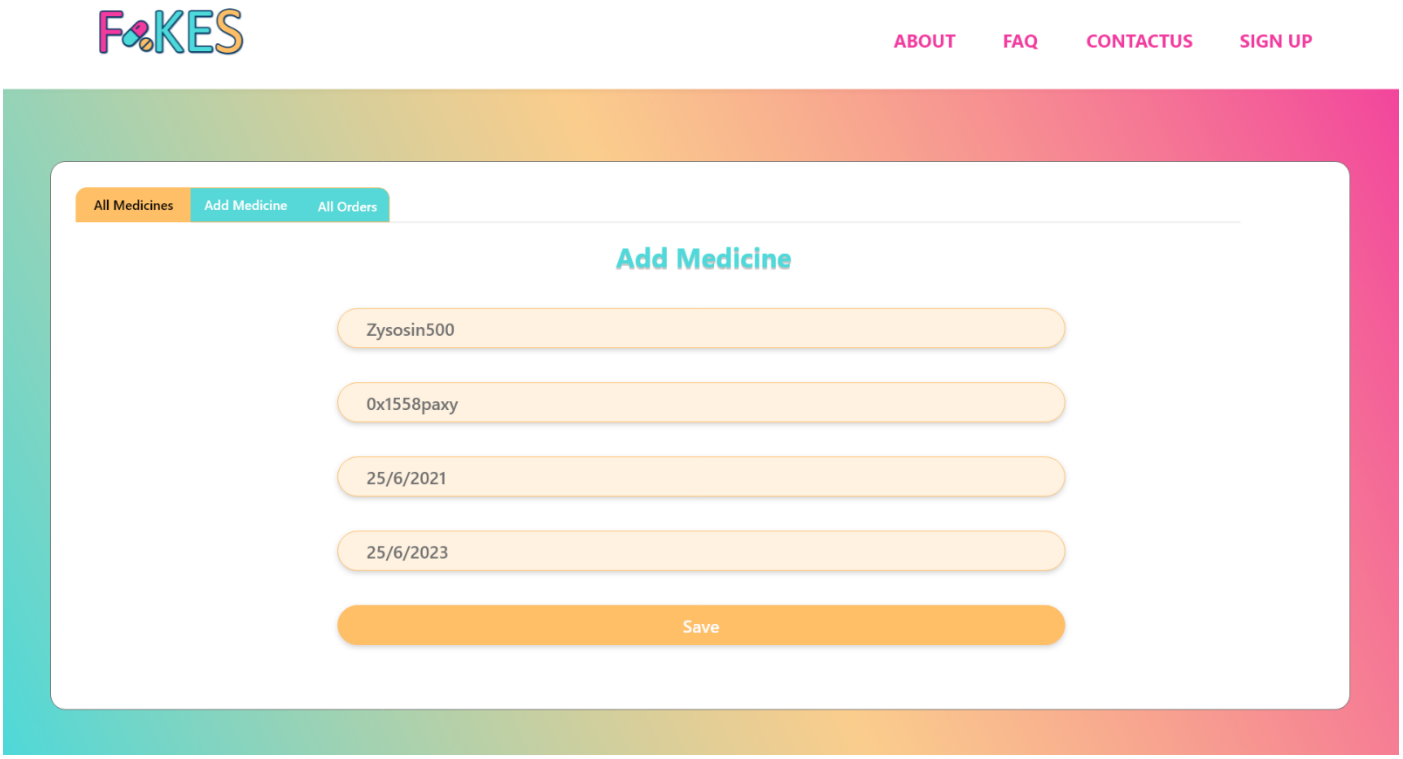

Figure 15 – Manufacture - Add Medicine

b. All Medicines:

i. In this panel, Manufacture user can view all medicines that are recorded in his manufacture profile in the system.

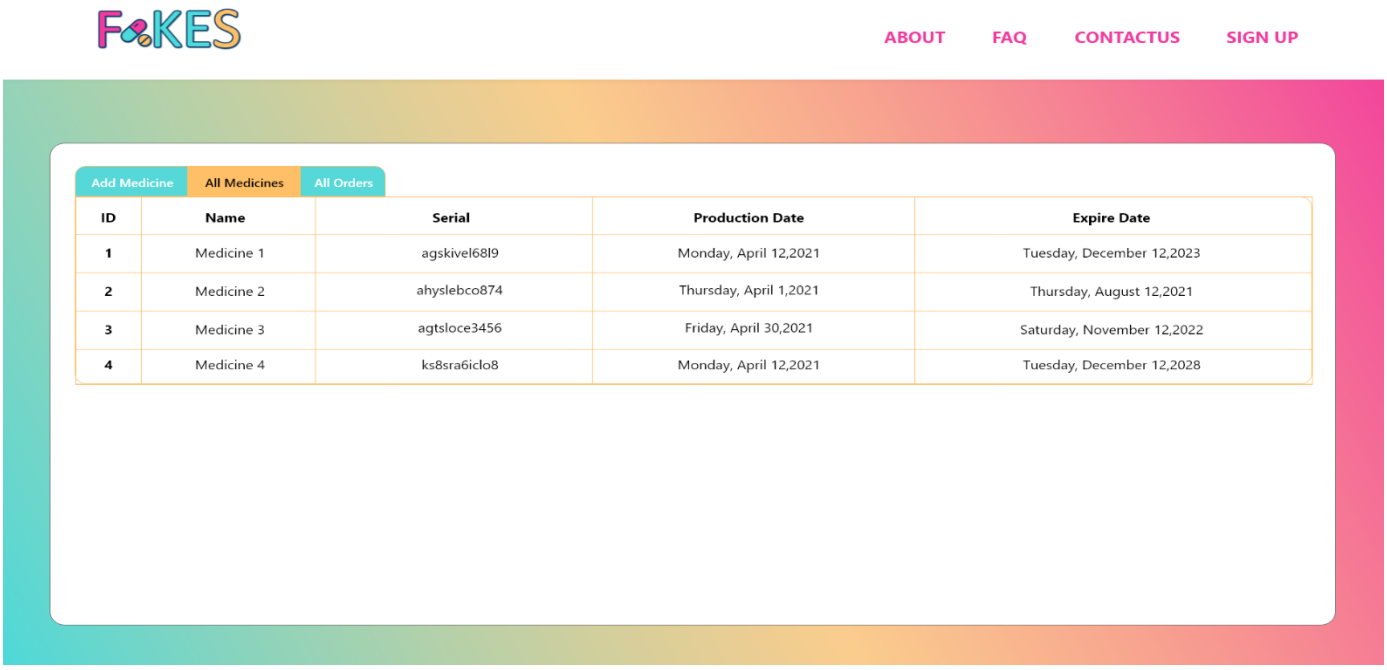

Figure 16 – Manufacture - All Medicines

c. All Orders:

i. in which the manufacture user can view all orders that are requested from pharmacies.

ii. The panel shows a table consists of 4 columns:

1. ID
2. Medicine ID
3. Pharmacy ID
4. Action

iii. In Action column, there are a button named "Confirm", pressing this button means that the manufacture accepts the order of the pharmacy.

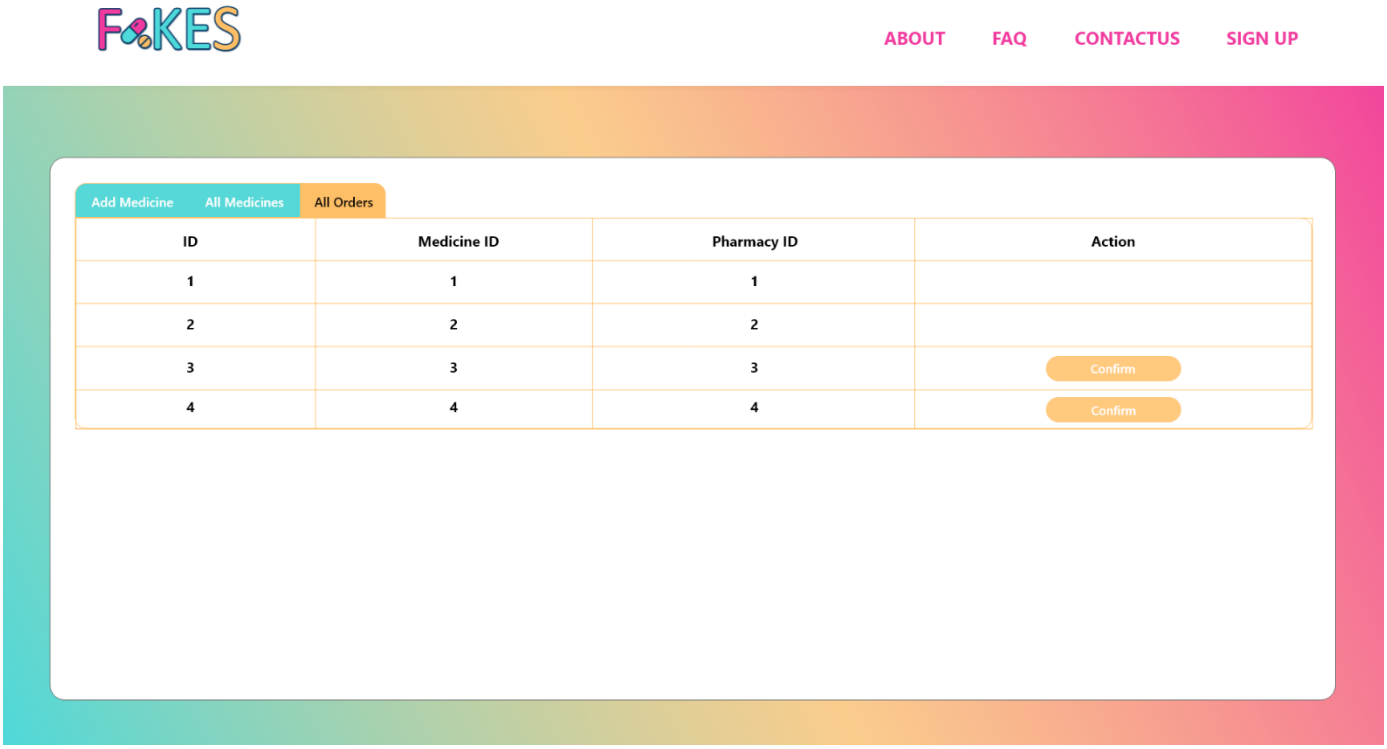

Figure 17 – Manufacture- All Orders

6.4. Pharmacy Panel:

When a user login as a Pharmacy, a panel will open with three options will appear in which.

The three options are: "All Available Medicines", "My Medicines", "All Orders".

a. All Available Medicines:
   i. In which pharmacist can see all medicines that are available to be ordered from manufactures and when pharmacist clicks "**add to card**" button, the order will be sent to the manufacturer.
   ii. information of medicines is:
      1. ID.
      2. Manufacture ID.
      3. Drug Name.
      4. Drug Serial Number.
      5. Drug Production date.
      6. Drug Expire Date.
      7. Action.
   iii. In "Action" column a button named "Add to card", when clicking this button, user request an order of the specific drug from the manufacture which id is shown beside the drug that requested.

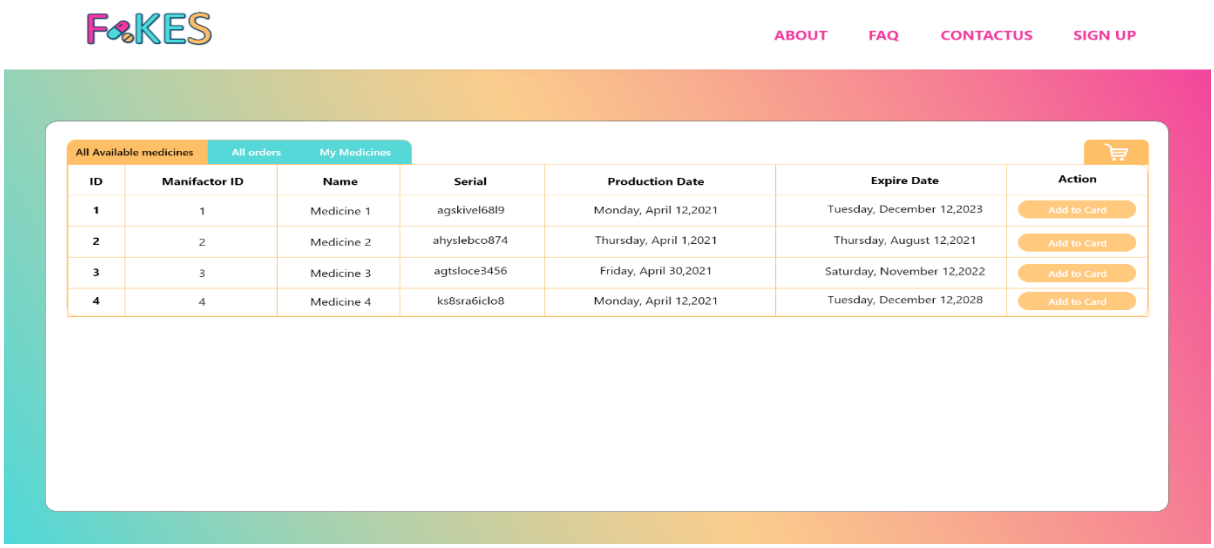

Figure 18 – Pharmacy - All Available medicines

b. All Orders:

i. In which pharmacist can see all medicine's orders which he requested from manufactures, with the status of each order if the request is accepted or not and the action of how to receive the order

ii. Table of this panel consists of 5 columns are:

1. ID.
2. Medicine ID.
3. Manufacture ID.
4. Confirmed Status.
5. Action.

iii. In "Action" column a button named "Receive Order", when clicking this button, Pharmacist is ready to receive the order and track it.

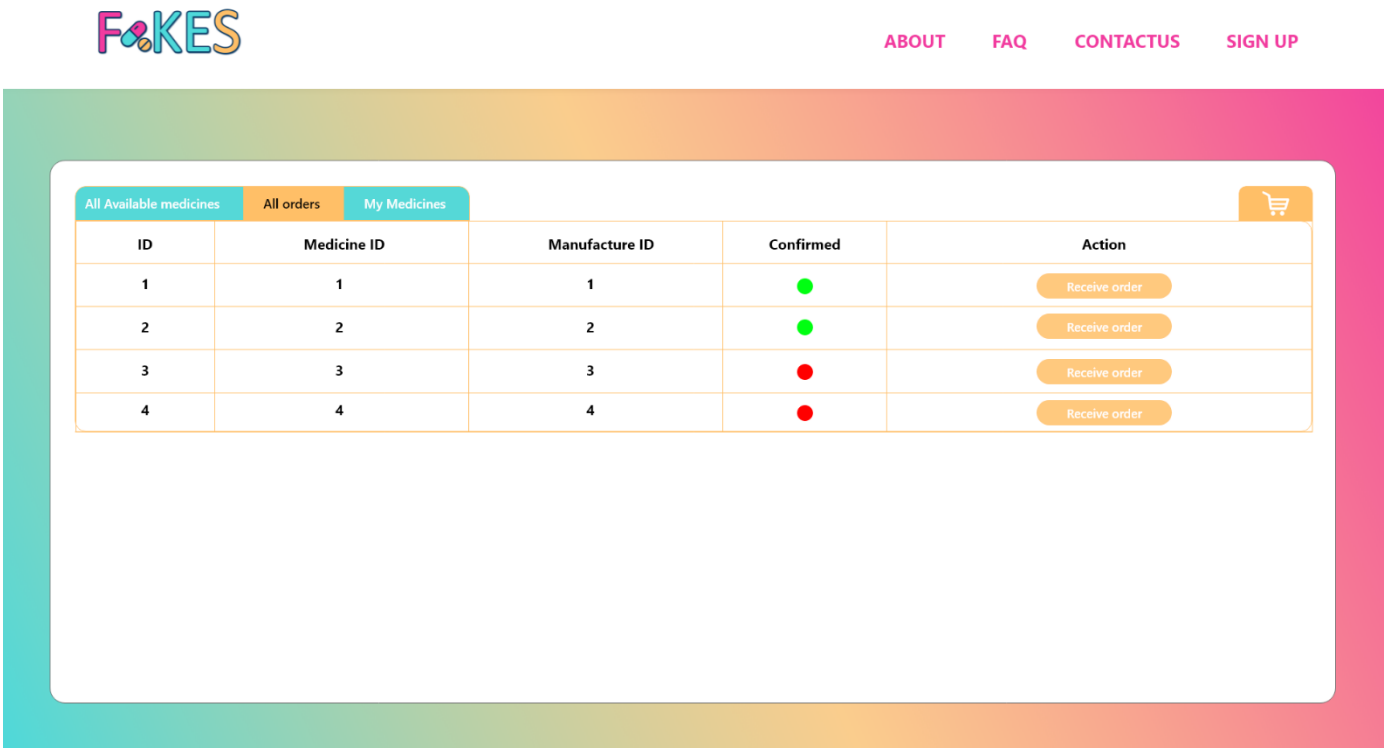

Figure 19 -Pharmacy- All Orders

c. My Medicines:

i. In which pharmacist can see all medicine's which he has in his pharmacy and recorded in the system with all its clearly defined details.

ii. Table of this panel consists of 5 columns are:

1. ID.
2. Manufacture ID.
3. Drug Name.
4. Drug Serial Number.
5. Drug Production Date.
6. Drug Expire Date.

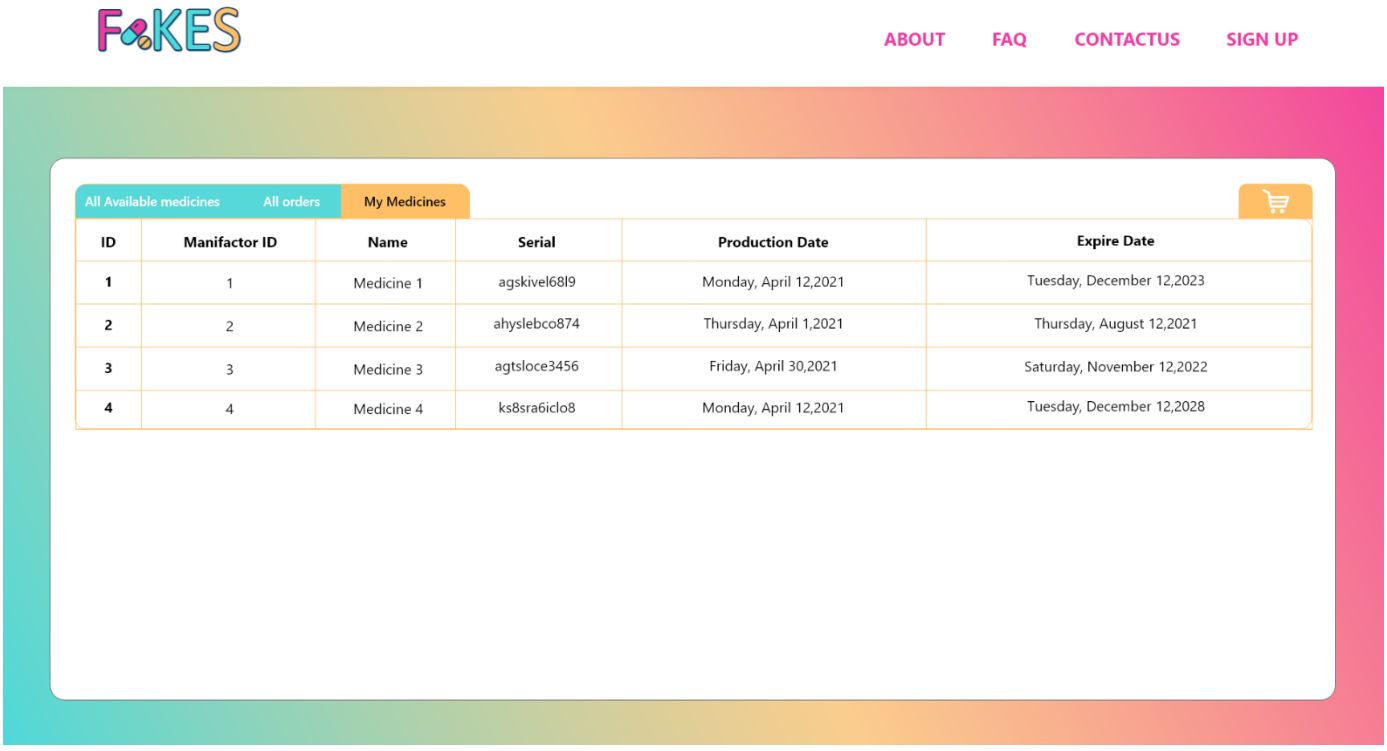

Figure 20 – Pharmacy - My Medicines

Chapter 7

Conclusion and Future Work

7.1. Conclusions:

With the recent advancement in network and Internet technologies, there is an urgent need of improvement in medical health care services. various issues related to drug supply chain management have been discussed. This work also discusses how blockchain can prevent the issues in a transparent and secure manner. Blockchain can be used to add traceability and visibility to the drug supply chain to overcome the issues of drug counterfeiting. A model of decentralized blockchain architecture has also been presented with a shared ledger system, which will not only prevent drug counterfeiting but also will make the drug supply more robust, transparent, and trustworthy. Using this proposed model loopholes in our current drug supply chain can be blocked. Moreover, the proposed model of blockchain framework is not only limited to countering the counterfeiting of drugs but also be useful in real-time tracking such as scheduling delivery of products.

7.2. Future Work:

- **Expand our system:**
  - Expand our system to be use in all Egyptian ports and airports, also in pharmacies to detect fake medicine before entering the country.
- **Enhancing performance:**
  - Adding distributors and transporter companies to systems
- **Developing website for medicines:**
  - Developing website like amazon that contains all categories of medicine to make it easy for hospitals and pharmacies to order medicines.
- **Developing mobile apps:**
  - Extending our system by building an android and iOS application and desktop application.

Chapter 8

References

1. Salman, T., M. Zolanvari, A. Erbad, R. Jain, and M. Samaka. 2018. Security services using blockchains: A state of the art survey. IEEE Communications Surveys and Tutorials 21 (1): 858–880.

2. Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

3. Zheng, Z., S. Xie, H.-N. Dai, and H. Wang. 2016. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services 1: 1–25.

4. Roehrs, A., C.A. da Costa, and R. da Rosa Righi. 2017. Omniphr: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics 71: 70–81.

5. Pharmaceutical industry in India. https://en.wikipedia.org/wiki/Pharmaceutical.

6. Mettler, M. 2016. Blockchain technology in healthcare: The revolution startshere. In 2016 IEEE 18th International conference on e-Health networking, applications and services (Healthcom), 1–3. IEEE.222 M. Sahoo et al.

7. Azaria, A., A. Ekblaw, T. Vieira, and A. Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International conference on open and big data (OBD), 25–30. IEEE.

8. Zhao, H., Y. Zhang, Y. Peng, and R. Xu. 2017. Lightweight backup and efficient recovery scheme for health blockchain keys. In 2017 IEEE 13th international symposium on autonomous decentralized system (ISADS), 229–234. IEEE.

9. Liang, X., J. Zhao, S. Shetty, J. Liu, and D. Li. 2017. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), 1–5. IEEE.

10. "Blockchain may finally disrupt payments from Micropayments to credit cards to SWIFT". dailyfintech.com. 10 February 2018. Archived from the original on 27 September 2018. Retrieved 18 November 2018.

11. K. Kotobi, and S. G. Bilen, "Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access", IEEE Vehicular Technology Magazine, 2018.

12. "The future of blockchain in 8 charts". Raconteur. 27 June 2016. Archived from the original on 2 December 2016. Retrieved 3 December 2016.

13. Ovenden, James. "Blockchain Top Trends In 2017". The Innovation Enterprise. Archived from the original on 30 November 2016. Retrieved 4 December 2016.

14. Brett, Charles (18 April 2018). "EUIPO Blockathon Challenge 2018 - ". Enterprise Times. Retrieved 1 September 2020.

15. Steve Davies (2018). "PwC's Global Blockchain Survey". Financial Website. Source Media. Retrieved 1 February 2021.

16. "Permissioned Blockchains". Explainer. Monax. Archived from the original on 20 November 2016. Retrieved 20 November 2016.

17. Corkery, Michael; Popper, Nathaniel (24 September 2018). "From Farm to Blockchain: Walmart Tracks Its Lettuce". The New York Times. Archived from the original on 5 December 2018. Retrieved 5 December 2018.