COPYRIGHT

ACKNOWLEDGEMENT

The completion of this project and report has been possible due to support, guidance and co-operation of multiple helping hands and it would be unfaithful not to mention them. We are sincerely grateful to IOE, Paschimanchal Campus for this course on a major project and all the teachers and staff of Electronics and Computer Engineering for assisting us in the duration of the project with suggestions, lectures on the context of our project goals.

We are also grateful to our supervisor Mr. Rupesh Kumar Sah for helping us throughout our project and giving us valuable suggestions and clear guidance all the way in this project.

Members of Project

Bhuwan Adhikari (073BCT614)

Jiwan Sapkota (073BCT624)

Paras Khati (073BCT628)

Roshan Rimal (073BCT634)

ABSTRACT

MedicoChain is a decentralized platform where the transactions occurring in the supply chain of the drugs are stored in the Blockchain that cannot be tampered, which unlocks the real power of decentralization and security. The drug counterfeit problem has become global and so huge that it has drawn significant attention from everyone. According to the WHO, the earning from counterfeit drugs is around $32 Billion. Counterfeits are usually manufactured in substandard environments and one of the main reasons behind the drug counterfeiting is imperfect 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 manufacturers. MedicoChain uses Hyperledger Fabric Platform, a framework developed by IBM and Linux Foundation to build a private Blockchain network, where power is distributed among participating parties of the supply chain. Using blockchain technology we have incorporated traceability, visibility and security into the drug supply chain. Thus, MedicoChain tracks the drugs from its origin, the manufacturer to the end, the consumer.

Keywords: ·Decentralized Platform · Drugs supply chain · Security · Traceability · Blockchain · Drug counterfeit · Hyperledger Fabric

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

HTTP:	*HyperText Transfer Protocol*
IBM:	*International Business Machine*
JSON:	*JavaScript Object Notation*
P2P:	*Peer to Peer*
RPC:	*Remote Procedure Call*
NPM:	*Node Package Manager*
Dapps:	*Decentralized Applications*
SH:	*Sexual Health*
HDC:	*Healthcare Data Gateway*
MADA:	*Mobile Application for Drug Authenticating*
NAFDAC:	*National Agency for Food and Drug Administration*
MAI:	*Mobile Authentication Service*
MSP:	*Membership Service Provider*
CA:	*Certificate Authority*
B2B:	*Business to Business*
YAML:	*YAML Ain't Markup Language*
PKI:	*Public Key Infrastructure*
API:	*Application Programming Interface*
SDK:	*Software Development Kit*
RFID:	*Radio Frequency Identifier*

1. INTRODUCTION

1.1 Background

MedicoChain is a blockchain implementation in the drug supply chain in which the drugs are tested for their originality and aid in avoiding their counterfeiting. It is not a distant possibility, and this has become a reality for most developing countries even for some developed countries. Fake medicines have turned into a 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. So, the real-time visibility of drug production and management is necessary. If the drug is replicated by the same name, package or strip, our application can help in reducing such counterfeit acts as the application tracks the path of the drug from manufacturer to the hand of consumer. So, the consumer can verify the genuinity of drugs by seeing the history of drugs stored in the blockchain.

Our project had aimed at implementing the concept of decentralized drug information to eliminate the hindrance caused due to centralized systems and the progress on it has been substantial. This ledger software is capable of monitoring and tracking all parts of the drug delivery process. The Hyperledger fabric can configure multiple world state databases to maintain the set of current values, and, when applied to the pharmaceutical world, it enables medicine to be accurately traced regardless of where it is in the world.

1.2 Motivation

Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises.

Hyperledger Fabric is a framework for permissioned networks, where all participants have known identities. When considering a permissioned network, you should think about

whether your blockchain use case needs to comply with data protection regulations. Many use cases in the financial sector and healthcare industry, in particular, are subject to data protection laws that require knowing who the members of the network are and who is accessing specific data. Hyperledger Fabric is built on a modular architecture that separates transaction processing into three phases: distributed logic processing and agreement ("chaincode"), transaction ordering, and transaction validation and commitment. This separation confers several advantages: Fewer levels of trust and verification are required across node types, and network scalability and performance are optimized. These notions and ecosystem make Hyperledger Fabric a natural fit for MedicoChain.

1.3 Problem Statement

Counterfeit drugs is an expanding serious issue associated with the healthcare industry which causes extreme threats to society. Counterfeit drugs or counterfeit medicines are defined as "one which is deliberately and fraudulently mislabeled with respect to identity and/or source". These are basically the pharmaceutical products which either have the wrong ingredients or may have the correct ingredients but in the wrong quantity. The traceability of the drugs throughout the pharma supply chain is difficult.

Drug counterfeiting is being identified as a serious threat to the users globally. The consumption of these fraudulent products might have serious repercussions ranging from minor deterioration in health to very severe impacts such as death of the patient. Fake and substandard medicines are widely sold in the Nepali market, but regulators, traders and the public don't seem to realise the enormity of the problem. As per the current scenario the number of diseases and patients are continuously increasing and so is the consumption of these fake drugs. One major issue in dealing with the fake drugs is the storage of health records (mainly drug records and transactions) throughout the supply chain. Therefore, in the healthcare industry the maintenance of health records gains utmost importance. The transfer of health data across different organizations faces two major issues- the integrity issue and the privacy of data.

Counterfeiting can apply to both branded and generic products and counterfeit medicines may include the products with correct ingredients but fake packaging, with the wrong

ingredients, without active ingredients, with insufficient active ingredients, with manipulated expiry dates and with fake manufacturers and the identifier.

The main danger of counterfeit medicines is we don't know what's in them and if it came from the legitimate manufacturer or not. Sometimes they contain dangerous toxins that can be harmful if consumed. They can also contain too much of an active medicine, which can be dangerous to your health and may even lead to death. Another concern about taking counterfeit medicines is that we may not be getting the health benefits you expect from the products. For example, a drug we count on to lower your cholesterol level may not actually provide any benefit at all because it doesn't contain the correct ingredient. We might notice that a medicine we are taking has a different taste, consistency, or appearance than usual. We might also notice that we have a different reaction to the drug, or that it's not working the way it usually does.

To overcome these challenges Blockchain is being adopted. Recently it is seen that the employment of blockchain technology in the medical and healthcare services is increasing at a rapid rate. In the case of block-chain there is no central point of failure as the data is distributed and is stored in blocks. Blockchain technology helps in overcoming the security problems in healthcare. Features which make blockchain reliable for use in combating counterfeit drugs are:

- Peer-to-Peer Transmission
- Distributed Database
- Computational Logic
- Transparency with Pseudonymity
- Irreversibility of Records

1.4 Objectives

Our project is made with the intent to meet the following objectives

1.4.1 General Objectives

The major general objectives of MedicoChain are:

- To allow consumers to fetch details of their drugs they consume with ease.
- To incorporate traceability, visibility and security into the drug supply chain.

1.4.2 Specific Objectives

The major specific objectives of MedicoChain is:

- To track the path followed by drugs in the supply chain so consumption of counterfeit drugs is reduced by using permissioned blockchain, Hyperledger Fabric.

1.5 Scope and Application

MedicoChain is an open source decentralized blockchain based application which emphasizes medicinal drug supply chain management. Supply management is a crucial issue to safeguard in all sectors, but it has a greater importance in healthcare, due to its increasing complexity. This is because any compromise to the healthcare supply chain affects the wellbeing of a patient. Supply chains are vulnerable, and consist of holes for fraudulent attacks as they involve a number of moving parts and people. MedicoChain provides a safe and secure platform to eliminate this problem and, in some cases, prevent fraud occurrence as well, by introducing higher data transparency and improved product traceability. Since a record in blockchain can only be validated and updated through a smart contract, manipulating the blockchain isn't easy.

The pharmaceutical industry is one of the largest-growing, and is a leading sector at the forefront of healthcare delivery. MedicoChain not only helps in the introduction of new and potential drugs into the market, but also assists in ensuring the safety and validity of medical products and drugs sold to the end consumer. Besides, it also aids in evaluation

and processing of safe drugs, which assist ultimately in quicker patient recovery. In the usual cases, drug companies face the challenges of tracking their products timely, which sometimes leads to pose severe risks by allowing counterfeiters to compromise the production, or invade fake drugs into the system.

2. LITERATURE REVIEW

2.1 Overview

According to the research article published by Seyednima Khezri and others, blockchain-based healthcare management applications can transform the traditional healthcare industry with its features which include decentralization, anonymity, persistence, and audibility. The blockchain allows for health records to be time-stamped so that no one can tamper with them after becoming part of the distributor ledger. presented current research on health data management and how blockchain will empower patients and streamline the sharing process of health data[1]. Jasmine and others have studied the innovative blockchain technology, its impact on supply chain performance, and its optimal design. In particular, they have considered a normal firm that orders from its supplier and sells to its tech-savvy customers. From the perspective of both its up-stream supply and down-stream customers, blockchain technology adoption impacts the random supply and demand in a stochastic sense. The firm seeks to maximize the total expected discounted profit, by jointly managing (i) blockchain design, (ii) production and ordering decision, and (iii) dynamic pricing and selling. It has been shown that the deployment of blockchain technology can help firms reduce order quantities, lower selling prices and reduce the target-inventory levels[2].

Blockchains introduced serious disruptions to the traditional business processes since the applications and transactions, which needed centralized architectures or trusted third parties to verify them, can now operate in a decentralized way with the same level of certainty. The inherent characteristics of blockchain architecture and design provide properties like transparency, robustness, auditability, and security [3][4]. A blockchain can be considered a distributed database that is organized as a list of ordered blocks, where the committed blocks are immutable. One can see that this is ideal in the banking sector as banks can cooperate under the same blockchain and push their customers' transactions. This way, beyond transparency, blockchain facilitates transactions' auditing. Companies invest in this technology as they see the potential of making their architectures

decentralized and minimizing their transaction costs as they become inherently safer, transparent and in some cases faster. Therefore, blockchains are not just hype[5].

The Hyperledger blockchain network is permission-based and requires users to sign up to use it. Permissions on the network are controlled using Hyperledger modeling and access control languages. Hyperledger Fabric is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resilience, flexibility and scalability. Medical information is often highly sensitive, in both a social and legal sense, so a closed blockchain such as Hyperledger Fabric helps to retain the necessary privacy required for such an application. Hyperledger Fabric is a better solution for managing access to health records, as it accommodates multiple layers of permission, meaning the owner of a set of data can control which parts of their data is accessed[6].

Ethereum is a digital platform where thousands of powerful computers around the world work in harmony to host the Ethereum network. Ethereum's blockchain represents all accounts and transactions made by its users. Every time you send Ether, the currency of Ethereum, to another user, those computers act as accountants by verifying the validity of the transaction. Once the verification is approved by those "accountants" the money is then transferred to the other user, making transfers secure, transparent and conflict-free. Smart Contracts are code held and executed on the Ethereum blockchain. Anything that can be programmed normally can be programmed within the Ethereum network. Processes that normally require a professional or notary can be automated and validated by Smart Contracts in a wholly transparent and secure way. For example, the average physician spends 3.8 hours weekly on billing and insurance-related activity. Imagine the cost savings if these processes were conducted on Smart Contracts and validated by the Ethereum network[7].

In its early days, the Web was obviously not as useful as it is today with the array of apps and services that do everything under the sun, but it did have a more DIY distributed feel to it. The web was pretty decentralized from the outset. The HTTP protocol connected everyone on the planet with a computing device and an internet connection. In the HTTP protocol guidelines, there are a set of trusted serves that translate the web address you enter into a server address. Furthermore, HTTPS adds another layer of trusted servers and certificate authorities. People would host personal servers for others to connect to and

everyone owned their data. As the HTTP web grew larger, a new protocol was introduced by a developer named Bram Cohen, called BitTorrent. BitTorrent is a protocol created as a solution to the lengthy time to download huge media files via HTTP and as an improvement on some of the P2P proposals before it, like Gnutella, Napster, and Grokster. The problem was that downloading huge files took a very long time and as the Web grew, so did the size of files that were available. Meanwhile, hard-drive space was increasing and more people were connected. BitTorrent tried to solve this problem by making downloaders into uploaders[8].

2.2 Existing Decentralized Healthcare Applications

2.2.1 Medicalchain

Medicalchain uses blockchain technology to create a user-focused electronic health record whilst maintaining a single true version of the user's data. Medicalchain enables the user to give healthcare professionals access to their personal health data. Medicalchain then records interactions with this data in an auditable, transparent and secure way on Medicalchain's distributed ledger. Lastly, Medicalchain is a platform for others to use to build applications that complement and improve user experience. Users will be able to leverage their medical data to power a plethora of applications and services[9].

2.2.2 HashedHealth

Hashed Health is leading a consortium of healthcare companies focused on accelerating meaningful innovation using blockchain and distributed ledger technologies. To empower its consortium members, Hashed Health provides value-added services such as product management, product development, regulatory guidance, and technology support services for blockchain solutions and blockchain networks.

Based in Nashville, Hashed Health's healthcare experts focus on making sure the business problem drives the appropriate technical solution. They help members launch new industry

level solutions more effectively and at a lower cost. They also provide exposure to existing networks who are actively exploring, piloting or using existing solutions[10].

2.2.3 Uthabiti

Uthabiti app connects youths to a network of certified pharmacies that retail safe sexual health (SH) products. Their mission is to fight Counterfeit SH products that put our youths at risk. Through Blockchain technology, they are able to secure and transmit batch numbers of data from manufacturers to consumers. Our app uses batch scanning to verify products helping us achieve sustainable development through healthy living and wellbeing, reduced inequalities, and responsible production and consumption[11].

2.2.4 HDG (Healthcare Data Gateway).

HDG, a smart application that allows a patient to control and manage the sharing of healthcare data, is a blockchain-based application that consists of a gateway and a traditional database. The smart application manages patient medical data in blockchain ledger or a storage system. The HDG-centric healthcare ecosystem is divided into three layers, i.e., the storage layer, data management layer, and data usage layer. The storage layer provides independent storage, which is highly secure and available for healthcare data. The medical data are stored in the private blockchain, which is encrypted with different cryptographic techniques. The data management layer works as a gateway which evaluates all the incoming and outgoing data access. The layer also manages patient data and also authorizes other application data. The data usage layer contains the list of entities that use or access the medical data of the patient[12].

2.2.5 Healthcare

Healthcare is based on many existing systems and is another area that is well suited for disease. One of the main problems in hospitals is that there is no secure platform for storing and analyzing data. The lack of adequate infrastructure might often make it a

victim of hackers. However, in block chain technology, hospitals can safely store data such as medical records and share them with certified authorized experts, doctors, and patients [13]. The enriched features of blockchain technology improve data security and help to enhance the correctness and timeliness of diagnosis. Gem [14] and Tierion[15] are two emerging companies focusing on the current medical data center based on blockchain technology.

2.2.6 Mobile Application for Drug Authenticating (MADA)

MADA is a system that ascertains the validity of drugs using a mobile smartphone. The National Agency for Food and Drug Administration and Control (NAFDAC) already has a Mobile Authentication Service (MAS) that enables consumers to verify drugs with a mobile phone. The current system is faced with usability issues which the proposed system aims to improve on, by validating drugs with ease and a prompt to report invalid drugs. The system is implementable using techniques deployed in the existing system, and also new technologies presenting a more technically robust, user-friendly, cost-effective and portable system. The proposed system requires 30 seconds or less, for a drug to be verified. During a query session the application makes an internet connection with users' data service and connects to the central database containing valid drug data[16].

In the supply chain, block chain technology transactions are recorded permanently and are monitored safely and transparently. This greatly reduces the time required, which minimizes the chances of human errors. Blockchain technology can also be used to monitor cost, labor, as well as waste and emissions at every step of the supply chain [17]. The distributed ledger technology enables the state of a fair-trade product by providing ethnicity and tracking its origin. Many of the blockchain startups working in the industry (i.e., Provenance, Fluent, Skuchain and Blockverify) are using blockchain to improve supply chain networks [18,19].

In the present era, due to a lack of resources and infrastructure crowdfunding, it has become a common technique of fund raising for new startups and projects. There exists a crowdfunding platform which develops a conviction between supporters and project creators, and they charge high fees. Instead of creating trust through traditional approaches,

blockchain smart contracts are used, and online reputation systems are used for crowdfunding. This blockchain crowdfunding removes the need for a middle-man [20]. New projects can raise capital by issuing tokens and be exchanged for products, services, or cash. Several blockchain-based startups like Starbase [21] raised millions of dollars through such token sales.

Today, due to lack of transparency and mistakes in public records, buying and selling real estate is difficult. In the real-estate industry, blockchain technology is also used to keep records secure, transparent, and to speed up the buying and selling process. The decentralized distributed ledger ensures the accuracy of a document, tracking, verifying ownership, and transferring property deeds [22].

Blockchain technology has transformed the entire approach to consulting, forecasting, research, and analysis. Blockchain-based platforms like Augur are a decentralized market for predictions. This Ethereum-based solution is used to monitor and place bets on everything like stocks, election, sports, weather, and even cryptocurrencies in a decentralized manner [23].

Due to the emergence of blockchain technology, the data are secured as they never were before. Although the ledger in blockchain is shared, nevertheless, the data are encrypted and verified using enhanced cryptography algorithms. This cryptography algorithm protects data from theft and also maintains the integrity of data [24].

Blockchain removes the barrier of current banking and payment systems by giving access to financial services. People who do not have access to traditional banking systems use bitcoin, which allows them to send money anywhere across the world instantly, securely and with comparatively lower fees. Several banks around the globe like Barclays espouse blockchain technology to increase business and make their transactions efficient, fast, and secure. According to IBM, 65% of the total recognized banks around the world will start using blockchain by the end of 2019 [25].

As stated above, these blockchain platforms are either not open-source or they are permissionless; therefore, the general user cannot modify them for their own purpose. Furthermore, most of the systems presented in literature reviews are either related to managing electronic medical records or sharing the health records of patients and doctors. Nevertheless, none of these systems will address secure drug delivery combined with

doctor and patient management using Hyperledger Fabric platforms. Moreover, many of the systems discussed above use the inherent cryptocurrency which increases the computational power during the transaction. To the best knowledge of the author, there has been no functional, medical blockchain model for drug supply chain management based on Hyperledger technology built so far.

3. REQUIREMENT ANALYSIS

3.1 Feasibility Study

Feasibility is the determination of whether or not a project is worth doing. Three tests for feasibility study for the decentralized system are as follows:

3.1.1 Economic Feasibility

Blockchain being one the major horizontal innovations of the 21st century, it possesses a huge potential to disrupt several industries amounting Tens of Trillions. Even though the technology is new, the number of companies showing interest in this technology is downpouring. Payment system now consumes a lot of time and extra cost. Blockchain is helping people by reducing the extra cost and saving time with it's a great application, cryptocurrency. Since blockchain-based products can save a lot of effort and cost, a lot of companies have already started to invest in this promising technology.

MedicoChain saves the consumers from the extra expenses that arose because of the problem in the interoperability, counterfeit pharmaceutical drugs. Mining process in blockchain technology costs a lot of power and so a lot of money is taken as one of the major disadvantages of this technology but most of the major blockchain platforms are moving from 'Proof of Work' consensus protocol to 'Proof of Stake' consensus protocol.

Hyperledger Fabric is used as a distributed database.It processes information quickly regardless of network load. It allows each user to make instant payments for goods and services using cryptocurrency. Hyperledger Fabric provides a high degree of privacy: due to competition and laws protecting and regulating personal data privacy, organizations dictate the confidentiality of certain data elements, which can be achieved by dividing data into a blockchain. The channels supported in Hyperledger Fabric allow users to transmit data only to the parties that need to use it. Hyperledger Fabric allows users to interact with each other both within one organization and within several organizations This makes MedicoChain more feasible economically.

3.1.2 Social Feasibility

Social feasibility is the determination of whether a proposed project will be acceptable to the society or not. Several people are dying from toxic ingredients, as in the case of repeated mass casualties due to drugs or because counterfeits are found within a drug category that is financed to a significant degree by development aid. This is causing a negative impact on the health of the people in the society. This project is for the ease for the people to detect the drug counterfeiting and the fake drugs using blockchain as a distributed environment.

Though MedicoChain is totally a digital platform, it can be quite difficult for the society to use easily at first but with the passage of time, it will let them save a huge portion of their earnings and time. It is quite difficult to grow the usage of our proposed system where there are more digitally illiterate people. MedicoChain provides a new paradigm to the people for enjoying their health services with the help of a mobile app powered by blockchain.

3.1.3 Technical Feasibility

Blockchain is a new technology that can bring revolution to every industry that exists. A lot of developers have dived into this field in the last couple of years. Since the blockchain technology is decentralized in nature, it increases the trust to the end users because user data and program running don't depend upon any central entity. It reduces the burden of the centralized system that exists today.

Mining of the block provides big security to the blockchain network. But mining requires high energy usage. At a personal level this drives up bills, while at a more general level this higher energy usage could be an important consideration for sustainability sectors. The overall gain from the blockchain products would need to negate this. Blockchain's main advantage is the fact that it cannot be altered, therefore guaranteeing trust. However, if the input is itself a lie, you are trusting lies. There is a need to remember the people and process element of it – blockchain does not answer this (although it doesn't profess to, it just aims to be immutable). There needs to be a process for guaranteeing truth in the input.

3.2 Functional Requirements

This system will be able to perform the following functionalities:

- Reducement of drug counterfeiting so that the consumer will be able to get more quality and genuine drugs. And it also allows the consumer to have a clear picture of the supply chain of the drug from its origin to the hand of the consumer.
- Allowing the manufacturer to track the drug from its origin to the consumer so that their product cannot be counterfeited and sold. This will allow the manufacturer to get data of its product lifecycle which will help the manufacturer for research and analysis of its production.

3.3 Non Functional Requirements

3.3.1 Scalability

Platform like ours is tied to a blockchain implementation system like Hyperledger Fabric and thus the scalability of our system is also tied to the scalability of the implementation system as well. Several research papers have been published studying and testing the performance capabilities of Hyperledger Fabric. The latest scaled Fabric to 20,000 transactions per second.

3.3.2 Privacy

Hyperledger Fabric, being a permissioned platform, enables confidentiality through its channel architecture and private data feature. In channels, participants on a Fabric network establish a sub-network where every member has visibility to a particular set of transactions. Thus, only those nodes that participate in a channel have access to the smart contract (chaincode) and data transacted, preserving the privacy and confidentiality of both.

3.3.3 Fault tolerance

The system is based on fault tolerant mechanisms already available in hyperledger fabric hence is fault tolerant out of the box. It supports pluggable consensus protocols that enable the platform to be more effectively customized to fit particular use cases and trust models. For instance, when deployed within a single enterprise, or operated by a trusted authority, fully byzantine fault tolerant consensus might be considered unnecessary and an excessive drag on performance and throughput. In situations such as that, a crash fault-tolerant (CFT) consensus protocol might be more than adequate whereas, in a multi-party, decentralized use case, a more traditional byzantine fault tolerant (BFT) consensus protocol might be required.

3.3.4 Extensibility

The system supports modular architecture and components can be plugged according to the use cases and requirements. The ordering of transactions is delegated to a modular component for consensus that is logically decoupled from the peers that execute transactions and maintain the ledger. It also provides pluggable membership service providers which are responsible for associating entities in the network with cryptographic identities. Similarly, smart contracts can be written in various standard programming languages, the ledger can also be configured to support a variety of DBMSs. A pluggable endorsement and validation policy enforcement can be independently configured per application.

4. METHODOLOGY

4.1 System Design

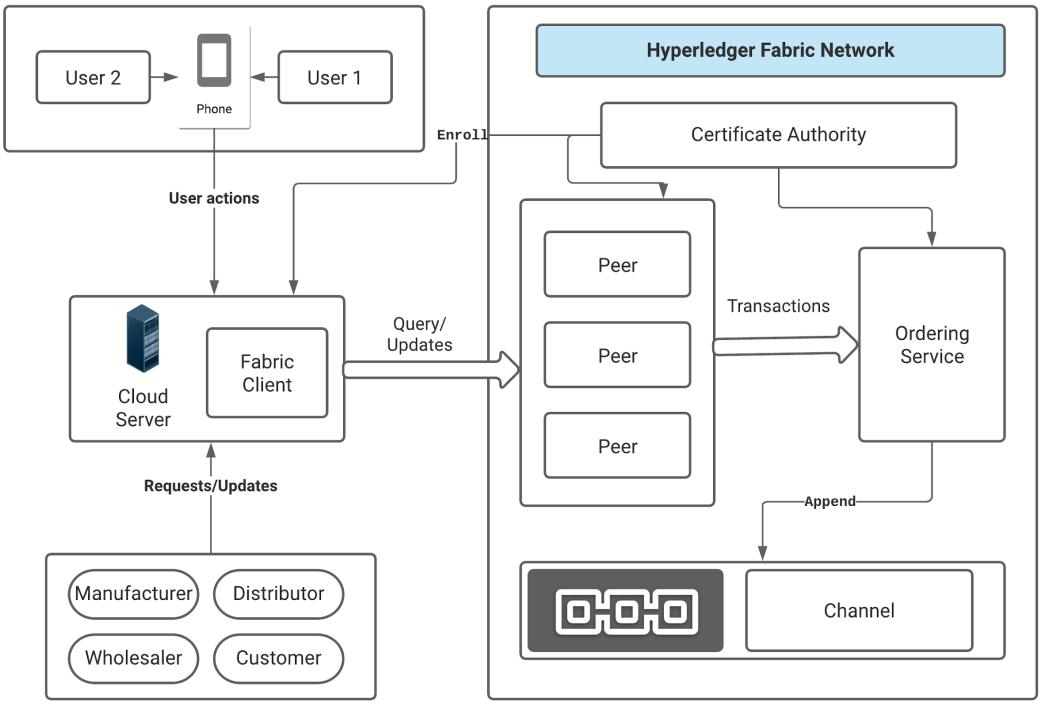

Fig 4.1 : Components of MedicoChain

HyperLedger Fabric forms the core around which MedicoChain is developed. The system's architecture is highly modular where different components interact with each other using REST APIs. The system is organized as shown in the diagram below. The different components are:

1. Mobile Application

   A cross platform mobile application developed using flutter forms the frontend of the entire system and all the end-user interactions take place through this i.e manufacturers, suppliers, distributors all interact with each other and with the

system through this. It is developed using flutter and communicates with the Node.js backend.

2. Node.js Server

   This is a server which communicates with both the blockchain and the mobile application effectively acting as a bridge between the end users and the blockchain. It uses fabric SDK to generate transaction proposals and ledger queries on behalf of the end users and relays the response in the proper format back to the user.

3. Hyperledger Fabric Network

   A network is further composed of sub components which are:

   a) Ledger

   Ledger is the verifiable history of all the successful states and the unsuccessful attempts to change the state occurring during the operation of the system.

   b) Peer Node

   Peers are a fundamental element of the network because they host ledgers and smart contracts. A peer receives ordered state updates in the form of blocks from the ordering service and maintains the state and the ledger.

   c) Ordering Node

   These are the nodes responsible for consensus, ordering transactions and generating new blocks.

   d) Channel

   A Hyperledger Fabric channel is a private “subnet” of communication between two or more specific network members, for the purpose of conducting private and confidential transactions.

e) Chaincode

Chaincode is the 'smart contract' that runs on peers and creates transactions. It has the ability to update the world state of the assets in the distributed ledger.

f) Fabric Certificate Authority

Fabric CA provides features such as: Registration of identities with roles like peer, user or application, or to fetch identities of the mentioned roles. MSP is a Membership Service Provider which defines which certificate authorities(CA's) are allowed to issue certificates.

4.1.1 Communication Diagram

Ledger-query interactions involve a simple three-step dialogue between an application and a peer; ledger-update interactions are a little more involved, and require two extra steps. Applications always connect to peers when they need to access ledgers and chaincodes. The Fabric Software Development Kit (SDK) makes this easy for programmers — its APIs enable applications to connect to peers, invoke chaincodes to generate transactions, submit transactions to the network that will get ordered, validated and committed to the distributed ledger, and receive events when this process is complete.

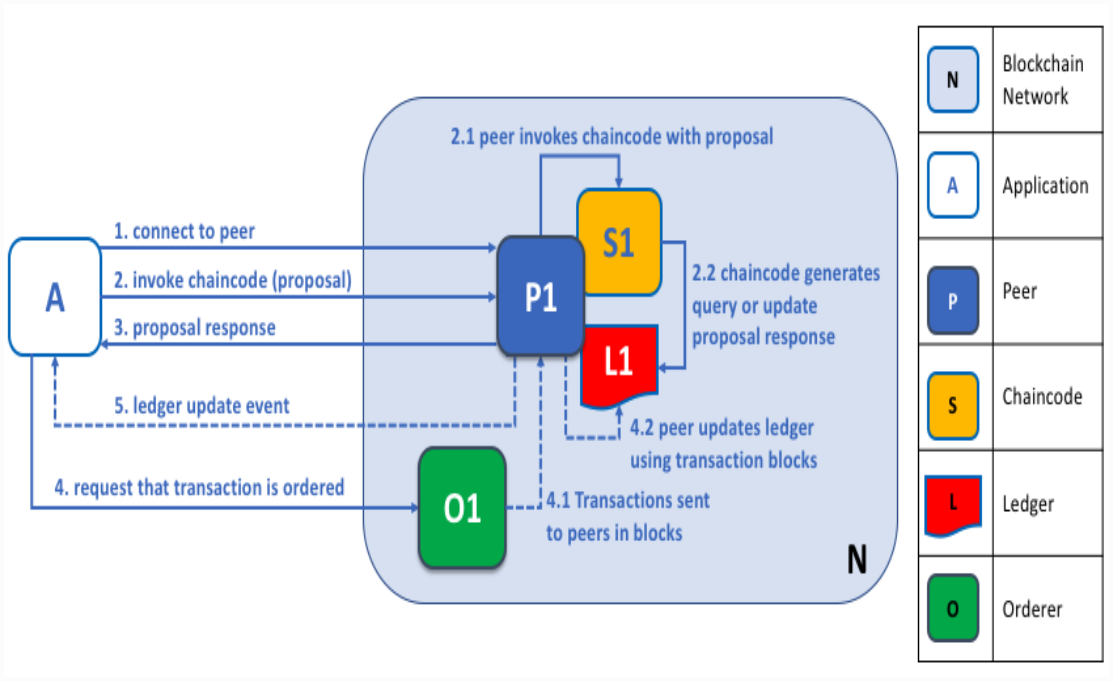

Fig 4.1: Interactions between Application and Blockchain[28]

Through a peer connection, applications can execute chaincodes to query or update a ledger. The result of a ledger query transaction is returned immediately, whereas ledger updates involve a more complex interaction between applications, peers and orders.

Peers, in conjunction with orderers, ensure that the ledger is kept up-to-date on every peer. In this example, application A connects to P1 and invokes chaincode S1 to query or update the ledger L1. P1 invokes S1 to generate a proposal response that contains a query result or a proposed ledger update. Application A receives the proposal response and, for queries, the process is now complete. For updates, A builds a transaction from all of the responses, which it sends to O1 for ordering. O1 collects transactions from across the network into blocks, and distributes these to all peers, including P1. P1 validates the transaction before committing to L1. Once L1 is updated, P1 generates an event, received by A, to signify completion.

A peer can return the results of a query to an application immediately since all of the information required to satisfy the query is in the peer's local copy of the ledger. Peers never consult with other peers in order to respond to a query from an application. Applications can, however, connect to one or more peers to issue a query; for example, to

corroborate a result between multiple peers, or retrieve a more up-to-date result from a different peer if there's a suspicion that information might be out of date. In the diagram, we can see that the ledger query is a simple three-step process.

An update transaction starts in the same way as a query transaction, but has two extra steps. Although ledger-updating applications also connect to peers to invoke a chaincode, unlike with ledger-querying applications, an individual peer cannot perform a ledger update at this time, because other peers must first agree to the change in a process called consensus. Therefore, peers return to the application a proposed update one that this peer would apply subject to other peers' prior agreement. The first extra step four requires that applications send an appropriate set of matching proposed updates to the entire network of peers as a transaction for commitment to their respective ledgers. This is achieved by the application by using an order to package transactions into blocks, and distributing them to the entire network of peers, where they can be verified before being applied to each peer's local copy of the ledger. As this whole ordering processing takes some time to complete (seconds), the application is notified asynchronously, as shown in step five.

4.1.2 Activity Diagram

Medicochain has four organizations as the client organizations which have their own peer nodes running in docker. The user authenticated by the manufacturer-ca can interact with the fabric network. When the drug is produced and packaged, each strip of drug is appended with QR code having the following information:

```
{
    "drugNumber": "00001",
    "manufacturer": "Acadia Pharmaceuticals"
 }
```

When the manufacturer scans the QR code by the mobile application, it queries the node server which then queries the blockchain. As the data of manufactured drugs is not recorded in the blockchain, it returns a null response. So, now the manufacturer is redirected to the form where he/she can do the inputs in the form and is submitted. Submitted data is stored in the decentralized ledger (blockchain).

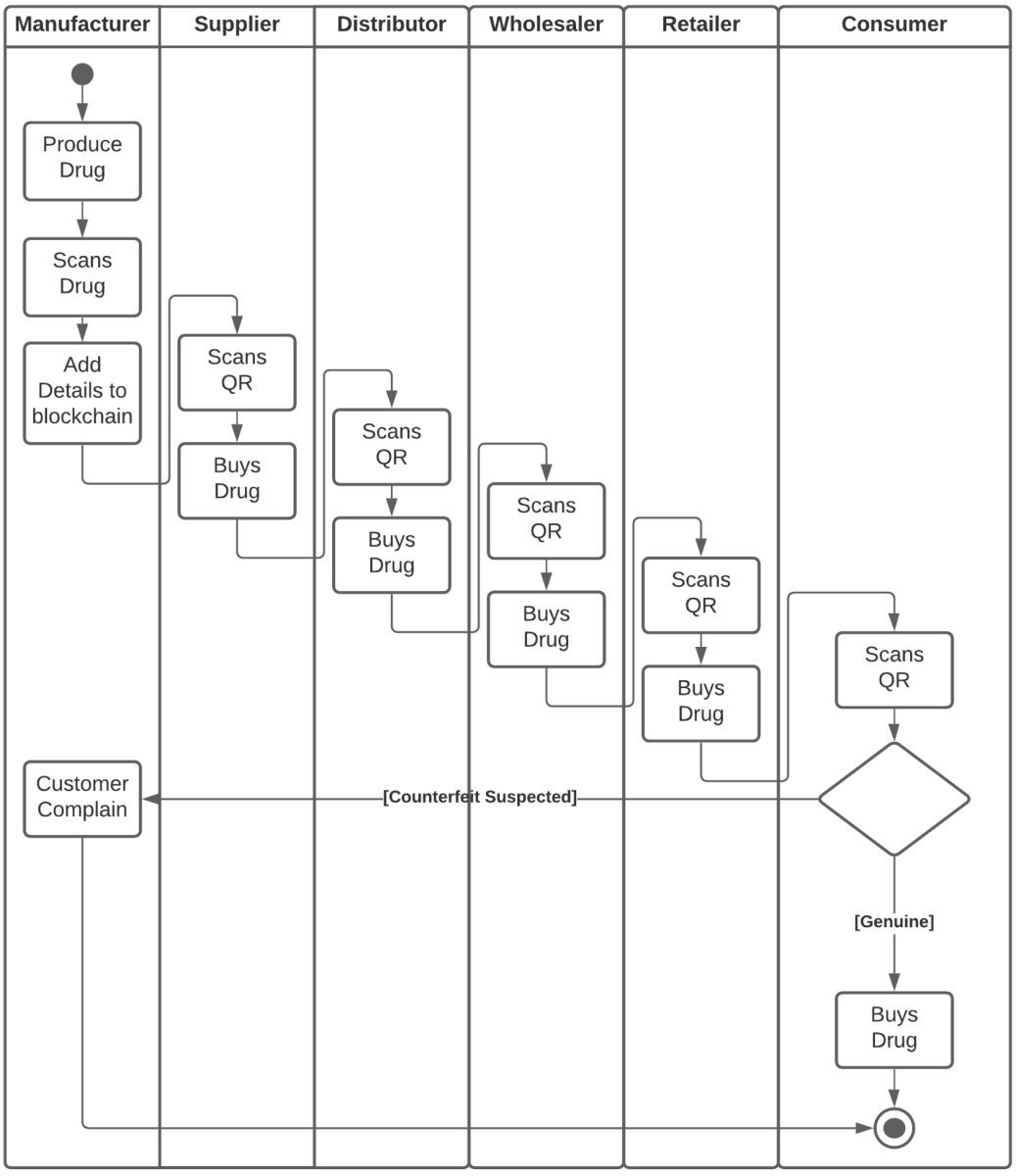

Fig 4.2: Activity Diagram

The structure of data of drug stored in blockchain is:

```
{
    "manufacturer":"<Name of Manufacturer>",
    "manufacturedIn":"<Place of Manufacture>",
    "drugNumber":"<Serial No. of Drug>",
    "mfgDate":"<Date of Manufacture>",
    "expDate":"<Expiry Date of Drug>",
    "dose":"<Dose of drug>",
    "composition":"<Composition of Drug>",
    "name":"<Name of Drug>",
    "bn":"<Batch No. of Drug>",
    "mrp":"<Maximum Retail Price of Drug>",
}
```

When the supplier buys the drug, he can scan the QR code attached on the strip of drug and verify it's genuinity if it's data is stored in blockchain or not. And the transaction of purchase is then stored in blockchain with the ownership transferred to the distributor.

And the wholesaler can scan the QR in the same way and get the drug's genuinity verified. If the drug's data is stored in the blockchain, then we can say it's genuine. The retailer will also buy the drug in the same way and the data about the transaction is stored in blockchain.

When the drug reaches the retailer, consumers can scan the QR code and verify it's genuinity. If the data is stored in the blockchain, we can say the drug is genuine as produced by the drug. The nodes in the supply chain of the drug can replicate the drug and the QR code. When the consumer scans the QR code, the application will show that the drug has already been sold because there is only one original drug which is already sold to the customer. Even in some cases if the consumed drug is found to be counterfeit or replicated, the no. of suspects who are doing fraud in the supply chain can be easily shortlisted and further legal actions can be carried out.

4.1.3 System Workflow

When a drug is manufactured, it is provided with a unique identity which is attached with strips of the drugs which can be scanned by a mobile application to see it's details. The data related to drugs is stored in the distributed ledger after the input transaction triggered by the manufacturer. When the distributor buys the drugs from the manufacturer, the distributor can scan the QR code to see the details of the medicine to be sure that the medicine is genuine.

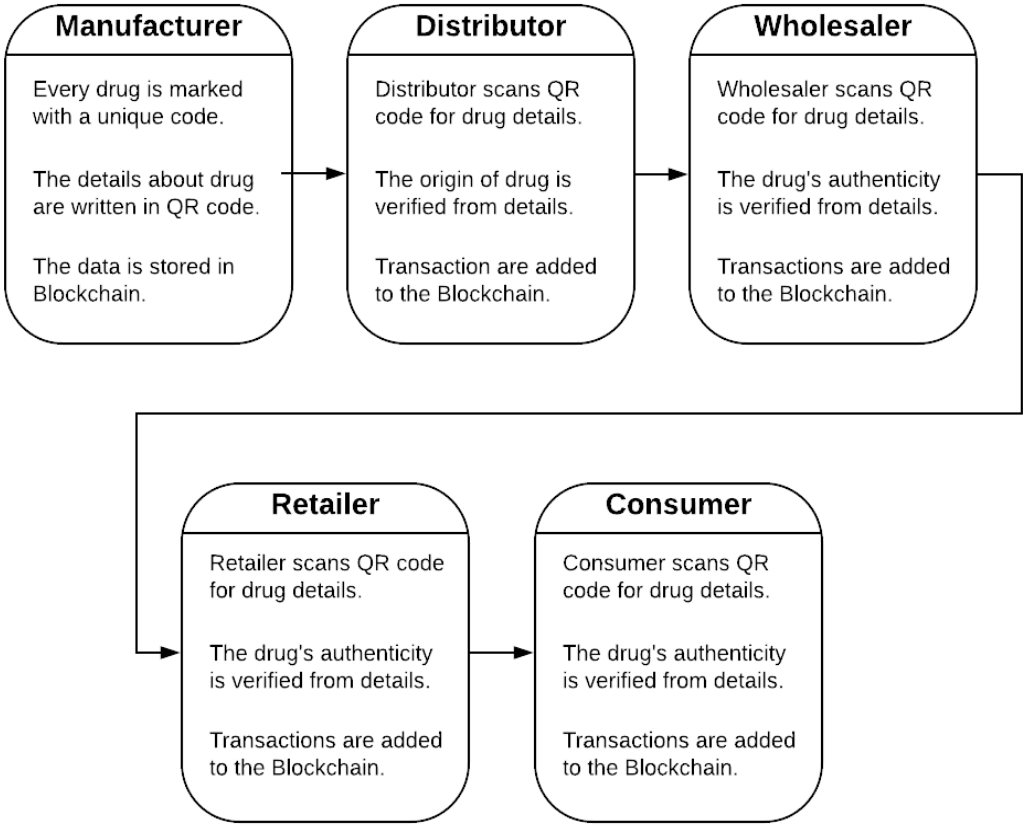

Fig 4.3: System Workflow

When the buying is complete, the transaction data is then stored in the blockchain. In the same way, the wholesaler buys from the distributor and retailer buys from the wholesaler.

Then, consumers can use a mobile app to scan the QR code and verify if it's genuine or not. If the previous transactions are all stored in blockchain, the drug is then genuine as each transaction is signed by the user or peer by which the transaction is triggered. Since, whole transaction data and history is stored in blockchain, a single entity cannot tamper the stored data. This helps in reducing the counterfeiting of drugs.

4.2 Tools and Techniques

Following are the tools used while building the system:

4.2.1 HyperLedger fabric architecture

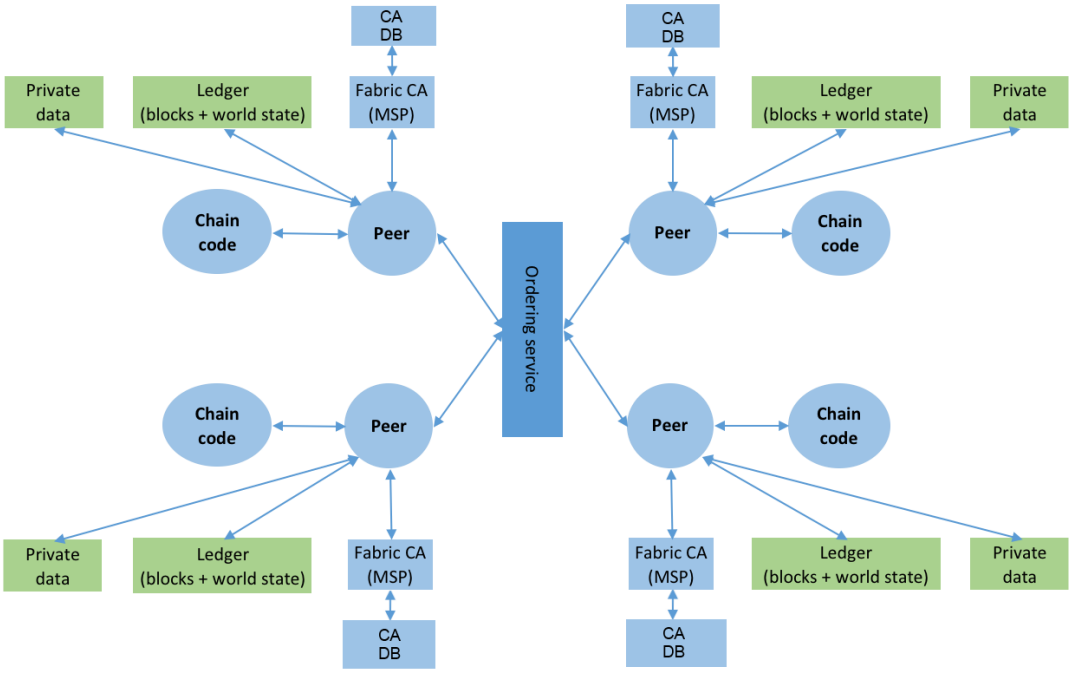

Fig 4.4: Hyperledger Fabric Architecture

The Linux Foundation founded the Hyperledger project in 2015 to advance cross-industry blockchain technologies. Rather than declaring a single blockchain standard, it encourages a collaborative approach to developing blockchain technologies via a community process. Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.

Where Hyperledger Fabric breaks from some other blockchain systems is that it is private and permissioned. Rather than an open permissionless system that allows unknown identities to participate in the network (requiring protocols like "proof of work" to validate transactions and secure the network), the members of a Hyperledger Fabric network enroll through a trusted Membership Service Provider (MSP).

Hyperledger Fabric also offers several pluggable options. Ledger data can be stored in multiple formats, consensus mechanisms can be swapped in and out, and different MSPs are supported.

Hyperledger Fabric also offers the ability to create channels, allowing a group of participants to create a separate ledger of transactions. This is an especially important option for networks where some participants might be competitors and not want every transaction they make a special price they're offering to some participants and not others, for example, known to every participant. If two participants form a channel, then those participants and no others have copies of the ledger for that channel.

Shared Ledger

Hyperledger Fabric has a ledger subsystem comprising two components: the world state and the transaction log. Each participant has a copy of the ledger to every Hyperledger Fabric network they belong to.

The world state component describes the state of the ledger at a given point in time. It's the database of the ledger. The transaction log component records all transactions which have

resulted in the current value of the world state; it's the update history for the world state. The ledger, then, is a combination of the world state database and the transaction log history.

The ledger has a replaceable data store for the world state. By default, this is a LevelDB key-value store database. The transaction log does not need to be pluggable. It simply records the before and after values of the ledger database being used by the blockchain network.

Anchor Peer

A peer node on a channel that all other peers can discover and communicate with. Each Member on a channel has an anchor peer (or multiple anchor peers to prevent single point of failure), allowing for peers belonging to different Members to discover all existing peers on a channel.

Concurrency Control Version Check

Concurrency Control Version Check is a method of keeping ledger state in sync across peers on a channel. Peers execute transactions in parallel, and before committing to the ledger, peers check whether the state read at the time the transaction was executed has been modified. If the data read for the transaction has changed between execution time and commit time, then a Concurrency Control Version Check violation has occurred, and the transaction is marked as invalid on the ledger and values are not updated in the state database.

Assets

Assets can range from the tangible (real estate and hardware) to the intangible (contracts and intellectual property). Hyperledger Fabric provides the ability to modify assets using chaincode transactions.

Endorsement

Refers to the process where specific peer nodes execute a chaincode transaction and return a proposal response to the client application. The proposal response includes the chaincode execution response message, results (read set and write set), and events, as well as a signature to serve as proof of the peer's chaincode execution. Chaincode applications have corresponding endorsement policies, in which the endorsing peers are specified.

Endorsement Policy

The policy that specifies the set organizations on the channel that need to execute the smart contract is referred to as the endorsement policy, which is set for each chaincode as part of the chaincode definition.

Hyperledger Fabric CA

Hyperledger Fabric CA is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate (rootCert) to each member and one enrollment certificate (ECert) to each authorized user.

Leading Peer

Each member can own multiple peers on each channel that it subscribes to. One of peers serves as the leading peer for the channel, in order to communicate with the network ordering service on behalf of the member. The ordering service "delivers" blocks to the leading peer(s) on a channel, who then distribute them to other peers within the same member cluster

Membership Service Provider

The Membership Service Provider (MSP) refers to an abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network. Clients use these credentials to authenticate their transactions, and peers use these credentials to authenticate transaction processing results (endorsements).

Privacy

Depending on the needs of a network, participants in a Business-to-Business (B2B) network might be extremely sensitive about how much information they share. For other networks, privacy will not be a top concern.
Hyperledger Fabric supports networks where privacy (using channels) is a key operational requirement as well as networks that are comparatively open.

Smart Contract

A smart contract is code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the World State via Transaction. In Hyperledger Fabric, smart contracts are packaged as chaincode. Chaincode is installed on peers and then defined and used on one or more channels.

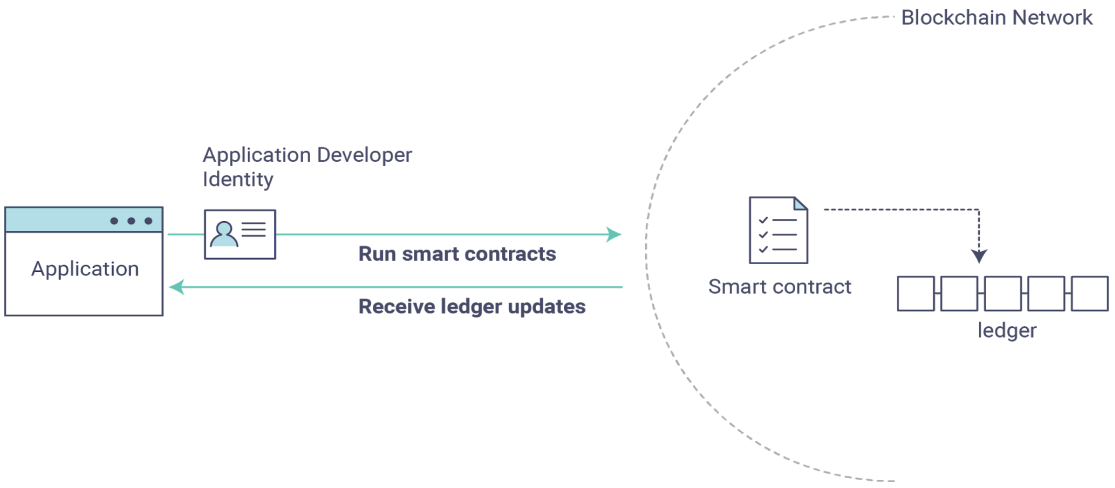

Fig 4.5: Application Invoking Smart Contract[29]

Chaincode

Chaincode is software defining an asset or assets, and the transaction instructions for modifying the asset(s); in other words, it's the business logic. Chaincode enforces the rules for reading or altering key-value pairs or other state database information. Chaincode functions execute against the ledger's current state database and are initiated through a transaction proposal. They are invoked when a network member wants to transfer or change an asset on the ledger. Chaincode execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers.

Consensus

Transactions must be written to the ledger in the order in which they occur, even though they might be between different sets of participants within the network. For this to happen, the order of transactions must be established and a method for rejecting bad transactions that have been inserted into the ledger in error (or maliciously) must be put into place.

Channel

A channel is a private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be authenticated to a channel in order to interact with it. Channels are defined by a Configuration-Block.

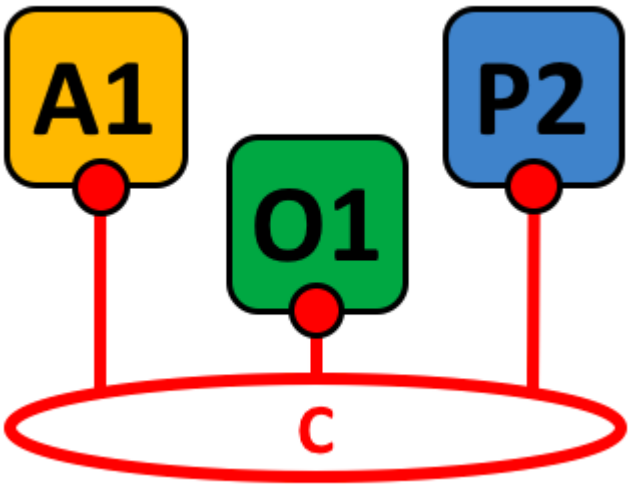

Fig 4.6: Channel connecting Application, peer and Ordering services[30]

A Channel's ledger contains a configuration block defining policies, access control lists, and other pertinent information

Channels contain Membership Service Provider instances allowing for crypto materials to be derived from different certificate authorities.

Security and Membership Services

Hyperledger Fabric underpins a transactional network where all participants have known identities. Public Key Infrastructure is used to generate cryptographic certificates which are tied to organizations, network components, and end users or client applications. As a result, data access control can be manipulated and governed on the broader network and on channel levels. This "permissioned" notion of Hyperledger Fabric, coupled with the existence and capabilities of channels, helps address scenarios where privacy and confidentiality are paramount concerns.

Ledger Operations

The ledger is the sequenced, tamper-resistant record of all state transitions in the fabric. State transitions are a result of chaincode invocations ('transactions') submitted by participating parties. Each transaction results in a set of asset key-value pairs that are

committed to the ledger as it creates, updates, or deletes. The ledger consists of a blockchain (‘chain’) to store the immutable, sequenced record in blocks, as well as a state database to maintain current fabric state. There is one ledger per channel. Each peer maintains a copy of the ledger for each channel of which they are a member.

Yaml

YAML (a recursive acronym for "YAML Ain't Markup Language") is a human-readable data-serialization language. It is commonly used for configuration files and in applications where data is being stored or transmitted. YAML targets many of the same communications applications as Extensible Markup Language (XML).It uses both Python-style indentation to indicate nesting, and a more compact format that uses [...] for lists and {...} for maps so that JSON files are also valid YAML .

X.509

Hyperledger Fabric uses an X.509 standard certificate to represent permissions, roles, and attributes to each user. In other words, a user is able to query or invoke any transaction on any channel based on permissions, roles, and attributes he/she possesses. Client is an application that interacts with the Fabric blockchain network. That is, clients can interact with the Fabric network according to its permissions, roles, and attributes as specified on its certificate derived from its associated organization’s CA server.

Postman

Postman is the only complete API development environment. The comprehensive set of built-in tools support every stage of the API lifecycle so individuals and teams can easily maintain a single source of truth. You can design and mock, debug, test, document, monitor, and publish your APIs from the Postman UI. Postman allows you to manage your APIs on the Postman native apps for MacOS, Windows, and Linux, with Newman, Postman's command line tool, and via the cloud using Postman Monitoring.

PKI

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

A PKI can be viewed as an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision.

Hyperledger Fabric uses public key infrastructure (PKI) to verify the actions of all network participants. Every node, network administrator, and user submitting transactions needs to have a public certificate and private key to verify their identity. These identities need to have a valid root of trust, establishing that the certificates were issued by an organization that is a member of the network. The network setup script creates all of the cryptographic material that is required to deploy and operate the network before it creates the peer and ordering nodes.

The network setup script also provides the option to bring up the network using Certificate Authorities (CAs). In a production network, each organization operates a CA (or multiple intermediate CAs) that creates the identities that belong to their organization. All of the identities created by a CA run by the organization share the same root of trust.

Fabric Application Stack

The Fabric application stack has five layers:

Prerequisite software: The base layer needed to run the software, eg, Docker.

Fabric and Fabric samples: The Fabric executables to run a Fabric network .

Contract APIs: To develop smart contracts executed on a Fabric Network.

Application SDKs: To develop your blockchain application.

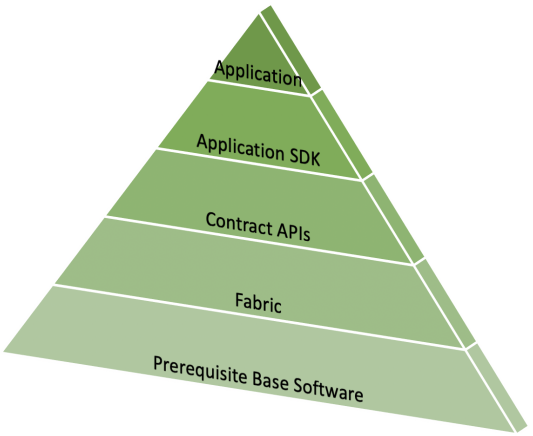

Fig 4.7: FabricApplication Stack[31]

The Application: The Blockchain application will utilize the Application SDKs to call smart contracts running on a Fabric network.

Transaction Flow

The sequence diagram below outlines the transactional mechanics that take place during a standard asset exchange (drug exchange in our case). The scenario includes two clients, A and B, who are buying and selling drugs. They each have a peer on the network through which they send their transactions and interact with the ledger. The application user has registered and enrolled with the organization's Certificate Authority (CA) and received back necessary cryptographic material, which is used to authenticate to the network.

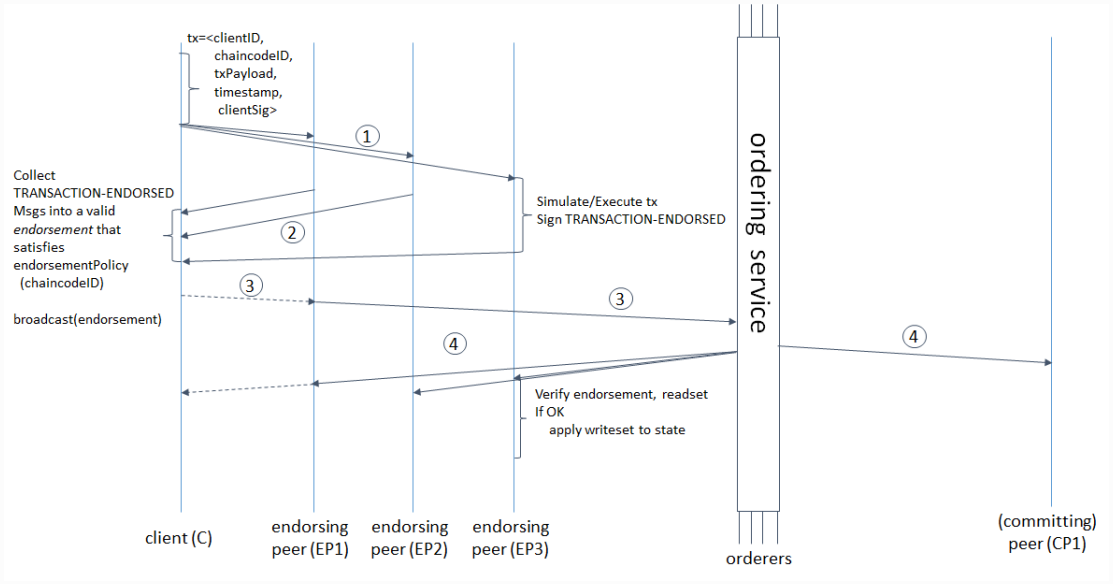

Fig 4.8: Transaction flow[32]

The application user has registered and enrolled with the organization's Certificate Authority (CA) and received back necessary cryptographic material, which is used to authenticate to the network. The chaincode (containing a set of key value pairs representing the initial state of the drug) is installed on the peers and deployed to the channel. The chaincode contains logic defining a set of transaction instructions. An endorsement policy has also been set for the chaincode, stating that both peerA and peerB must endorse any transaction.

1. Client A initiates a transaction:

Client A is sending a request to buy drugs. This request targets peers who are, who are respectively representative of Client A and Client B. The endorsement policy states which peers must endorse any transaction, therefore the request goes to peerA and peerB.

Next, the transaction proposal is constructed. An application leveraging a supported SDK (Node, Java, Python) utilizes one of the available API's to generate a transaction proposal. The proposal is a request to invoke a chaincode function with certain input parameters, with the intent of reading and/or updating the ledger.

2. Endorsing peers verify signature & execute the transaction:

The endorsing peers verify

- that the transaction proposal is well formed,
- it has not been submitted already in the past (replay-attack protection),
- the signature is valid (using the MSP), and
- that the submitter (Client A, in the example) is properly authorized to perform the proposed operation on that channel (namely, each endorsing peer ensures that the submitter satisfies the channel's Writers policy).

The endorsing peers take the transaction proposal inputs as arguments to the invoked chaincode's function. The chaincode is then executed against the current state database to produce transaction results including a response value, read set, and write set (i.e. key/value pairs representing an asset to create or update). No updates are made to the ledger at this point. The set of these values, along with the endorsing peer's signature is passed back as a "proposal response" to the SDK which parses the payload for the application to consume.

3. Proposal responses are inspected:

The application verifies the endorsing peer signatures and compares the proposal responses to determine if the proposal responses are the same. If the chaincode is only querying the ledger, the application would only inspect the query response and would typically not submit the transaction to the ordering service. If the client application intends to submit the transaction to the ordering service to update the ledger, the application determines if the specified endorsement policy has been fulfilled before submitting (i.e. did peerA and peerB both endorse). The architecture is such that even if an application chooses not to inspect responses or otherwise forwards an unendorsed transaction, the endorsement policy will still be enforced by peers and upheld at the commit validation phase.

4. Client assembles endorsements into a transaction:

The application “broadcasts” the transaction proposal and response within a “transaction message” to the ordering service. The transaction will contain the read/write sets, the endorsing peers signatures and the Channel ID. The ordering service does not need to inspect the entire content of a transaction in order to perform its operation, it simply receives transactions from all channels in the network, orders them chronologically by channel, and creates blocks of transactions per channel.

5. Transaction is validated and committed:

The blocks of transactions are “delivered” to all peers on the channel. The transactions within the block are validated to ensure endorsement policy is fulfilled and to ensure that there have been no changes to ledger state for read set variables since the read set was generated by the transaction execution. Transactions in the block are tagged as being valid or invalid.

6. Ledger updated:

Each peer appends the block to the channel’s chain, and for each valid transaction the write sets are committed to the current state database. An event is emitted by each peer to notify the client application that the transaction (invocation) has been immutably appended to the chain, as well as notification of whether the transaction was validated or invalidated.

4.2.2 Flutter

Flutter is an open-source UI software development kit created by Google. It is used to develop applications for Android, iOS, Windows, Mac, Linux, Google Fuchsia and the web. Flutter means faster & more dynamic mobile app development. We can make changes in the code and see them straight away in the app. This is called Hot reload, which usually only takes (milli)seconds and helps teams add features, fix bugs and experiment faster[27].

Flutter includes a modern react-style framework, a 2D rendering engine, ready-made widgets, and development tools. These components work together to help you design, build, test, and debug apps. Everything is organized around a few core principles.

The major components of Flutter include Dart platform, flutter engine, foundation library, design-specific widgets.

4.2.3 Node.js

Node.js makes it possible to write applications in Javascript on the server. It's built on the V8 Javascript runtime and written in C++ - so it's fast. Originally, it was intended as a server environment for applications, but developers started using it to create tools to aid them in local task automation. Since then, a whole net ecosystem of Node-based tools(such as Grunt, Gulp and Webpack) has evolved to transform the face of front-end development.

To make use of tools(or packages) in Node.js we need to be able to install and manage them in a useful way. This is where npm, the Node package manager, comes in. It installs the packages you want to use and provides a useful interfacet to work with them.
NPM is a package manager for the JavaScript programming language. It is the default package manager for the Javascript runtime environment Node.js. It helps in discovering packages of reusable code and assembling them in an effective way[26].

4.2.4 Docker

Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels. Because all of the containers share the services of a single operating system kernel, they use fewer resources than virtual machines.The software that hosts the containers is called Docker Engine.

4.2.5 Docker Compose

Compose is a tool for defining and running multi-container Docker applications. With Compose, we use a YAML file to configure your application's services.Then, with a single command, we create and start all the services from our configuration. To learn more about all the features of Compose, see the list of features. Compose works in all environments: production, staging, development, testing, as well as CI workflows.

We can learn more about each case in Common Use Cases. Using Compose is basically a three-step process:

- Define the app's environment with a Dockerfile so it can be reproduced anywhere.
- Define the services that make up the app in docker-compose.yml so they can be run together in an isolated environment.
- Run docker-compose up and Compose starts and runs the entire app.

4.2.6 Express

Express.js, or simply Express, is a back end web application framework for Node.js, released as free and open-source software under the MIT License. It is designed for building web applications and APIs. It has been called the de facto standard server framework for Node.js.

The original author, TJ Holowaychuk, described it as a Sinatra-inspired server, meaning that it is relatively minimal with many features available as plugins. Express is the back-end component of popular development stacks like the MEAN, MERN or MEVN stack, together with the MongoDB database software and a JavaScript front-end framework or library.

4.2.7 CouchDB

Apache CouchDB is an open-source document-oriented NoSQL database, implemented in Erlang. CouchDB uses multiple formats and protocols to store, transfer, and process its data, it uses JSON to store data, JavaScript as its query language using MapReduce, and HTTP for an API. CouchDB was first released in 2005 and later became an Apache Software Foundation project in 2008.

Unlike a relational database, a CouchDB database does not store data and relationships in tables. Instead, each database is a collection of independent documents. Each document maintains its own data and self-contained schema. An application may access multiple databases, such as one stored on a user's mobile phone and another on a server. Document metadata contains revision information, making it possible to merge any differences that may have occurred while the databases were disconnected.

CouchDB implements a form of multiversion concurrency control (MVCC) so it does not lock the database file during writes. Conflicts are left to the application to resolve. Resolving a conflict generally involves first merging data into one of the documents, then deleting the stale one.

4.2.8 LevelDB

LevelDB is an open-source on-disk key-value store written by Google fellows Jeffrey Dean and Sanjay Ghemawat. Inspired by Bigtable, LevelDB is hosted on GitHub under the New BSD License and has been ported to a variety of Unix-based systems, and macOS, Windows, and Android. LevelDB stores keys and values in arbitrary byte arrays, and data is sorted by key. It supports batching writes, forward and backward iteration, and compression of the data via Google's Snappy compression library.

LevelDB is not a SQL database. Like other NoSQL and dbm stores, it does not have a relational data model and it does not support SQL queries. Also, it has no support for indexes. Applications use LevelDB as a library, as it does not provide a server or command-line interface.

4.2.9 VS Code

Visual Studio Code is a freeware source-code editor made by Microsoft for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add additional functionality.

Visual Studio Code is a source-code editor that can be used with a variety of programming languages, including Java, JavaScript, Go, Node.js, Python and C++. It is based on the Electron framework, which is used to develop Node.js Web applications that run on the Blink layout engine. Visual Studio Code employs the same editor component (codenamed "Monaco") used in Azure DevOps (formerly called Visual Studio Online and Visual Studio Team Services)

4.3 Theoretical Background

4.3.1 Blockchain

In general terms, a Blockchain is an immutable transaction ledger, maintained within a distributed network of peer nodes. These nodes each maintain a copy of the ledger by applying transactions that have been validated by a consensus protocol, grouped into blocks that include a hash that binds each block to the preceding block. Blockchain is a shared, replicated transaction system which is updated via smart contracts and kept consistently synchronized through a collaborative process called consensus.

In addition to being decentralized and collaborative, the information recorded to a blockchain is append-only, using cryptographic techniques that guarantee that once a transaction has been added to the ledger it cannot be modified. This property of “immutability” makes it simple to determine the provenance of information because participants can be sure information has not been changed after the fact. It’s why blockchains are sometimes described as systems of proof.

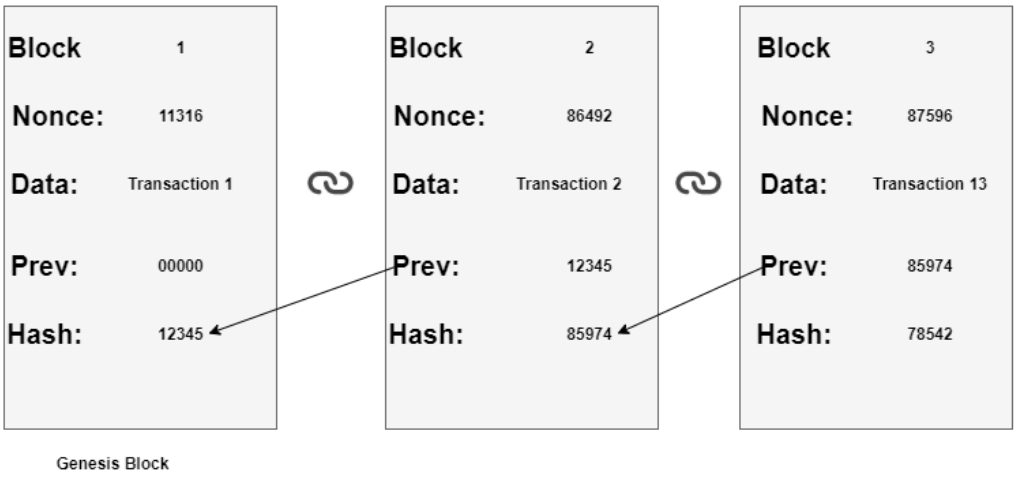

Fig 4.9: Arrangement of blocks in a Blockchain

The first block is called the genesis block and contains arbitrary information. The subsequent blocks are connected to the genesis block by the use of a hash.

Bitcoin and Ethereum fall into a class of blockchain that we would classify as public permissionless blockchain technology. Basically, these are public networks, open to anyone, where participants interact anonymously. However these technologies are currently unable to deliver performance and identity requirements. This is where Hyperledger Fabric comes into picture.

Consensus Mechanism in Fabric: Consensus by definition is 'a general agreement.' So all participating members (peers) that transact with each other on a channel, decide by general agreement on which transactions are valid and can be added to the chain. Fabric is said to have a 'Pluggable' Consensus algorithm.The architecture of Hyperledger Fabric does not provide an individual component for consensus implementation. Rather it builds the consensus infrastructure as a combination of services called Endorsing and Ordering.

Endorsing Peers : Peers can be chosen into a set of 'Endorsers'. These are peers that are the first ones to receive transactions from an initiating client. Endorsers verify the correctness, well formedness, and rule compliances of these transactions. Based on the

copy of ledger available to them locally, the transactions are executed and re results are stored. They produce their results and package them into 'Endorsements'. Endorsements from all endorsing peers are sent back to the client individually.

Endorsing Policies : These are Rules written using Logical Operators to define which transactions are considered valid on the network. Endorsements received back at the client record if individual endorsers see the initiated transaction as valid or not. Identities of Endorsers are also verified by producing valid certificates and keys. If Endorsing Policies are met, the transactions are declared Valid and can be sent ahead to append on to the chain. If not met, transactions are declared invalid. All transactions are immutably recorded in Peer Ledgers before being committed to the (main) Valid Ledger.

5. OUTPUT

This project will have a mobile application which can be used by the consumers and verified users of peer organizations from which the data of the drug can be read and written in the blockchain. The mobile application lets the manufacturer add the data of the drug into the blockchain. In the same way, wholesalers, distributors, retailers can add transactions of buying into the blockchain.

Consumers can use the same mobile app to see the details of drugs stored in the blockchain and and history of the blockchain which show which path it followed through in the supply chain of that drug. So, a consumer can be clear if the drug is counterfeit or not.

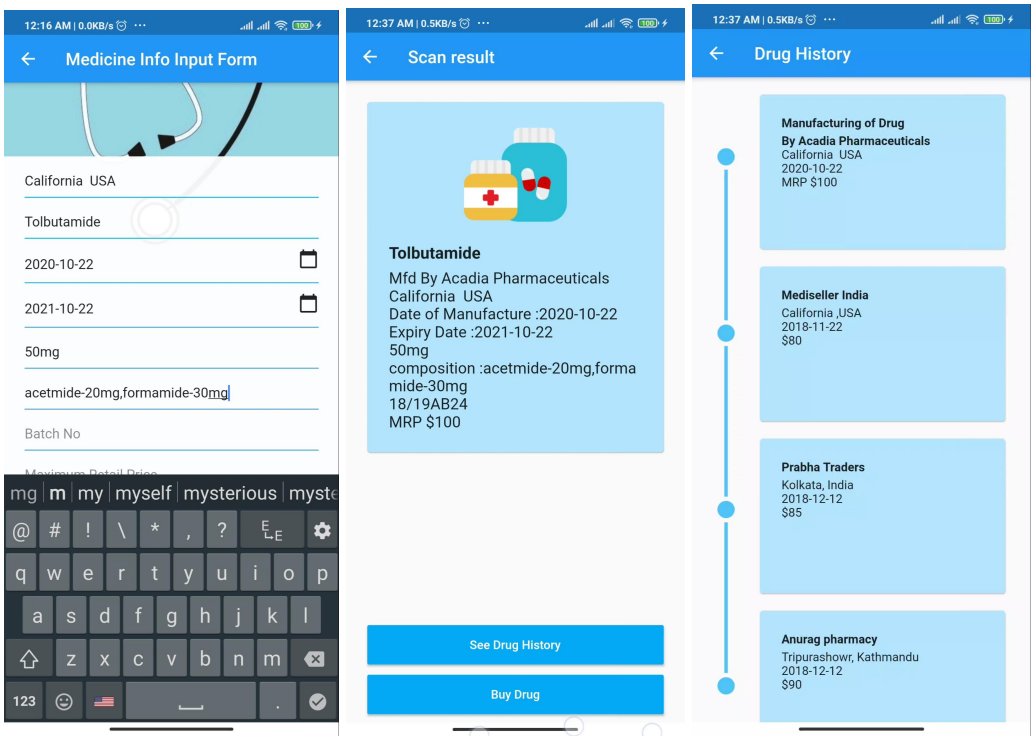

Fig 5.1: User Interaction with Mobile App to Track Drugs

6. FUTURE ENHANCEMENTS

This is only a prototype of blockchain implementation in the supply chain of drugs. This can be further enhanced to make it more efficient and effective. Some of the ways to enhance this project are:

- RFID can be attached with the package of the drug so that the detection and verification will be more secure and effective rather than just QR code.
- Also packages can be attached with simple sensors like humidity, temperature etc so that more data of drugs can be collected and provenance of drugs can be made more effective.
- Similar models of blockchain can be implemented in the supply chain of various other products like clothes, mobile phones, luxury products like jewellery etc.

7. CONCLUSION

MedicoChain is an implementation of blockchain in the drug supply chain in which the drugs are tested for their originality and aid in avoiding their counterfeiting. Counterfeit medicines have turned into a 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. Copies of original drugs by replicating the packages and strips is one of the major counterfeit techniques.

MedicChain has aimed at implementing the concept of decentralized drug information to eliminate the hindrance caused due to centralized systems and the progress on it has been substantial. This ledger software is capable of monitoring and tracking all parts of the drug delivery process. The Hyperledger fabric can configure multiple world state databases to maintain the set of current values, and, when applied to the pharmaceutical world, it enables medicine to be accurately traced regardless of where it is in the world.

8. REFERENCES AND BIBLIOGRAPHY

1. *Seyednima K., ,oniruzzaman A., and Benlamri, R., Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research*
2. *Chang, J., Katehakis M., Melamed, B., Shi, J., Blockchain Design for Supply Chain Management*
3. *Greenspan, G., 2015a. Ending the bitcoin vs blockchain debate, http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate.*
4. *K. Christidis, M. Devetsikiotis Blockchains and smart contracts for the internet of things IEEE Access, 4 (2016), pp. 2292-2303*
5. *Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification, and open issues, Telematics and Informatics, Volume 36, 2019, Pages 55-81, ISSN 0736-5853*
6. *MedicalChain White Paper. Medical Chain. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf*
7. *MedicalChain White Paper. Medical Chain. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf*
8. *Tiwari, K., Poudel, M., Shrestha, N., Tamang, R.2018. Decentralized Payment System.*
9. *MedicalChain White Paper. Medical Chain. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf*
10. *"Hashedhealt," Craft. [Online]. Available: https://craft.co/hashed-health*
11. *"Uthabiti, The Spindle." Accessed 26 Dec. 2019.[Online]. Available: https://thespindle.org/project/uthabiti/.*
12. *Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med Syst.* ***2016****, 40, 218. [Google Scholar] [CrossRef] [PubMed]*

13. *Brennan, B. Gem Health Developing Blockchain Solutions for the Healthcare Ecosystem. 2018. Available online: https://blockchainhealthcarereview.com/gem-health-developing-blockchain-solutions-for-the-healthcare-ecosystem/ (accessed on 20 March 2019).*

14. *Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–3. [Google Scholar]*

15. *Buntinx, J. 'Blockchain Technology Has A Bright Future in Healthcare', Tierion. 2016. Available online: https://btcmanager.com/blockchain-technology-has-a-bright-future-in-healthcare-tierion/?q=/blockchain-technology-has-a-bright-future-in-healthcare-tierion/& (accessed on 20 March 2019).*

16. *Ukaoha, Kingsley & Dim, Chinonye & Daudu, & Odokayor-Ogbomo, F.. (2015). Towards a Mobile Drugs Authentication System for Nigerian Users. Computing, Information systems, Development Informatics and Allied Research Journal..*

17. *Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777. [Google Scholar]*

18. *Allison, I. Skuchain: Here's How Blockchain Will Save Global Trade a Trillion Dollars. Available online: https://www.ibtimes.co.uk/skuchain-heres-how-blockchain-will-save-global-trade-trillion-dollars-1540618 (accessed on 18 March 2019).*

19. *Abeyratne, S.; Monfared, R. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. Int. J. Res. Eng. Technol. **2016**, 5, 1–10. [Google Scholar]*

20. *De Filippi, P. Blockchain-based Crowdfunding: What Impact on Artistic Production and Art Consumption? Available online: https://www.archives-ouvertes.fr/hal-01265211/document (accessed on 12 March 2019).*

21. *Schlegel, M.; Zavolokina, L.; Schwabe, G. Blockchain Technologies from the Consumers' Perspective: What Is There and Why Should Who Care? In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018. [Google Scholar]*

22. *Spielman, A. Blockchain: Digitally Rebuilding the Real Estate Industry. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2016. [Google Scholar]*

23. *Peterson, J.; Krug, J. Augur: A decentralized, open-source platform for prediction markets. arXiv 2015, arXiv:1501.01042. [Google Scholar]*

24. *Singh, S.; Singh, N. Blockchain: Future of financial and cyber security. In Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016; pp. 463–467. [Google Scholar]*

25. *Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. Finance. Innov.* ***2016****, 2, 24. [Google Scholar] [CrossRef]*

26. *NPM.[Online]. Available: https://www.npmjs.com/*

27. *Chris Bracken. "Release v0.0.6: Rev alpha branch version to 0.0.6, flutter 0.0.26 (#10010) · flutter/flutter". GitHub. Retrieved 2018-08-08.*

28. *Hyperledger Fabric official documentation*