

A Blockchain-Driven Framework Designed For Pharmaceutical Community To Secure And Trace The Trail Of Drug Supply Chain

by

Samiha Rahman

17101464

Arif Awasaf Aquib

16201068

Watry Biswas Jyoty

16201069

Moshiur Rahman

21341019

Tamanna Dewan

16201073

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
September 2021

© 2021. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Arif Awasaf Aquib

Arif Awasaf Aquib
16201068

Samiha Rahman

Samiha Rahman
17101464

Watry Biswas Jyoty

Watry Biswas Jyoty
16201069

Tamanna Dewan

Tamanna Dewan
16201073

Moshiur Rahman

Moshiur Rahman
21341019

Approval

The thesis titled “A Blockchain-Driven Framework Designed For Pharmaceutical Community To Secure And Trace The Trail Of Drug Supply Chain” submitted by

1. Samiha Rahman (17101464)
2. Arif Awasaf Aquib (16201068)
3. Watry Biswas Jyoty (16201069)
4. Tamanna Dewan (16201073)
5. Moshiur Rahman (21341019)

Of Summer, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 23, 2021.

Examining Committee:

Supervisor:
(Member)



Muhammad Iqbal Hossain, PhD
Assistant Professor
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Assistant Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Our quality of life relies heavily on health products, which marks our dependence on the pharmaceutical industry. Drug safety is very important to ensure that our life-savers do not turn out to be the cause of our death. Due to the complicated and non-transparent supply-chain management that exists within this industry, we have to face the unfortunate risks of counterfeit drugs. Moreover, drug counterfeiters are taking advantage of people's vulnerabilities during COVID-19 and are making the situation even worse. A blockchain-based platform can make the process of drug development, production and marketing far more efficient and trackable compared to the existing system. Everything can be planned out, recorded and traced by a decentralized and distributed ledger technology. This will give end-consumers the control to monitor the products they receive. Our thesis paper aims to observe the issue with the existing supply-chain of pharmaceutical drugs and create a trustworthy infrastructure which will effectively make the overall process easier, while ensuring drug safety. We have used Hyperledger fabric, an open source enterprise-grade framework under the Hyperledger umbrella, to execute secure and well-planned transactions of drugs.

Keywords: Blockchain; Hyperledger Fabric; Supply-chain; Smart Contract; Chain-code; Hash

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our supervisor Dr. Muhammad Iqbal Hossain sir for his kind support and advice in our work. He helped us whenever we needed help.

And finally to our parents, without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

Declaration	i
Approval	ii
Ethics Statement	iii
Abstract	iii
Dedication	iv
Acknowledgment	iv
Table of Contents	v
List of Figures	vii
List of Tables	viii
Nomenclature	viii
1 Introduction	1
1.1 Motivation	1
1.2 Problem Statement	2
1.3 Research Objective	3
2 Literature Review	4
3 Background Analysis	6
3.1 Blockchain	6
3.1.1 Blockchain Basics	6
3.1.2 Blockchain Structure	7
3.1.3 Types of Blockchain	10
3.1.4 Consensus mechanisms	11
3.1.5 Comparison between Blockchain Platforms	12
3.2 Hyperledger Fabric	13
3.2.1 Core Components of Hyperledger Fabric	13
3.2.2 Features of Hyperledger Fabric	15

4	Proposed Model	17
4.1	Blockchain Based Pharmaceutical Supply-chain Model	17
4.2	System Architecture	20
4.3	Workflow	22
4.3.1	Production Phase	22
4.3.2	Supply Phase	25
5	Implementation	26
5.1	Configuration model	26
5.2	Transaction instance	33
5.3	Scope for performance analysis	36
6	Conclusion and Future Work	38
	Bibliography	41

List of Figures

1.1	Total number of counterfeit incidents concerning pharmaceuticals world-wide (2002-2020)	2
3.1	Use of hashing function to create unique identity [32]	8
3.2	SHA-256 encryption example [33]	8
3.3	A closer look at a block in a blockchain	9
3.4	Blockchain diagram showing how blocks are linked	9
3.5	Blockchain diagram showing the effect of data alteration	10
3.6	Flow of Proof of Work [15]	11
3.7	Flow of Proof of Stake [15]	12
3.8	Peers-Organization-Channel structure [31]	14
3.9	PKI element workflow [21]	15
4.1	Working process of the blockchain in production phase of drugs	18
4.2	Working process of the blockchain in supply chain of drugs	19
4.3	System architecture of the blockchain network	20
4.4	Workflow of production phase- step1	22
4.5	Workflow of production phase- step2	23
4.6	Workflow of production phase- step3	24
4.7	Workflow of supply phase	25
5.1	creating asset	27
5.2	Asset displayed in database	27
5.3	Historian record of assets with timestamp	28
5.4	creating asset	29
5.5	Asset displayed in database	29
5.6	Historian record of assets with timestamp	30
5.7	Model file illustration	31
5.8	ACL for the network	32
5.9	A transaction is submitted	33
5.10	Successful transaction	34
5.11	Historian record of transaction	34
5.12	Drug with previous owner record	35
5.13	Drug with updated owner record	35
5.14	Network with a varying number of endorser[20]	37
5.15	TPS with a varying number of endorser[20]	37

List of Tables

3.1 Blockchain platform comparison	12
--	----

Chapter 1

Introduction

Drug counterfeit, a crime with almost no logical difference with murder, is a devastating globalized occurrence. Drugs we think will save our lives may actually not contain the correct active pharmaceutical ingredient (API), or may even have wrong ingredients that may pose a much higher risk than the actual disease they are meant to cure. On the other hand, the involvement of so many stakeholders (pharmaceutical industries, extraction unit, manufacturer, packagers, distributor, wholesaler) makes the drug supply chain extremely vulnerable to such crimes. For a better common global understanding, the World Health Assembly officially defined sub-standard medical products as “authorized medical products that fail to meet either their quality standards or specifications, or both”, unregistered medical products as “Medical products that have not undergone evaluation and/or approval by the National or Regional Regulatory Authority (NRA) for the market in which they are marketed/distributed or used, subject to permitted conditions under national or regional regulation and legislation” and falsified medical products as “Medical products that deliberately/fraudulently misrepresent their identity, composition or source” [2]

1.1 Motivation

The number of people who fall victim to falsified medicine is significantly higher than the number of people with the slightest idea of how fake drug chains work, and that gives fake drug industries a huge floor to be more creative with counterfeiting. Figure 1.1 [22], the number of worldwide drug counterfeit incidents from 2002 to 2020 give us a clear reason to rethink the existing standard process of drug production and distribution and make it more transparent. There have been incidents where paracetamol syrup, used mostly as a cure for the simplest disease, has killed at least 28 children across Bangladesh in 2009 by causing renal failure as a result of the inclusion of toxic ingredients [1].

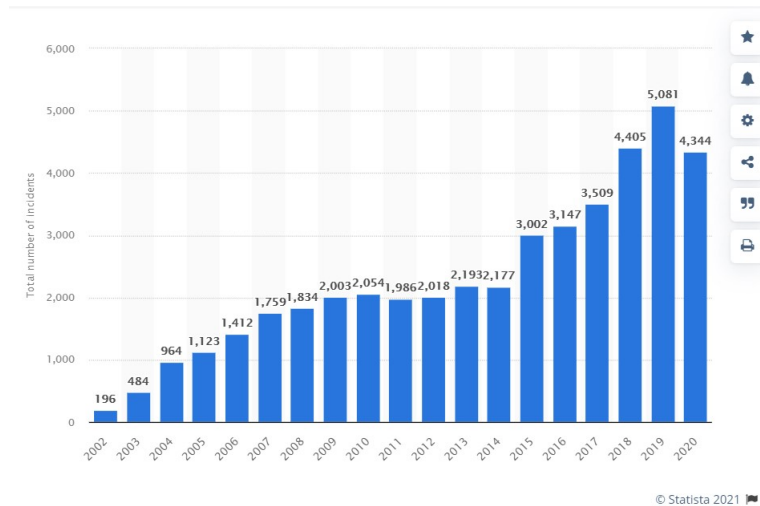


Figure 1.1: Total number of counterfeit incidents concerning pharmaceuticals worldwide (2002-2020)

More than 250,000 children die due to fake drugs that are expected to cure malaria and pneumonia every year, and WHO states the impact of fake and substandard drugs to be difficult to quantify [7]. In 2020, the year ruled by corona-virus, cases of drug counterfeiting have been rampant. Claiming to be a cure for the pandemic, pharmaceuticals worth 14m dollars were seized by Operation Pangea, Interpol’s global pharmaceutical crime fighting unit [17].

1.2 Problem Statement

WHO originated the idea of serialization, global surveillance and establishing monitoring systems to increase the traceability of drug supply, thereby minimizing drug counterfeit. Although the serialization was expected to cover 80% of global drug supply by 2020, the process has proven to be complicated due to the complexity of supply-chains [4][5]. The process of drug supply depends on many stakeholders, which happens to be very centralized. So, we propose a blockchain based system with distributed ledger in this paper which will be decentralized and can save the drugs from being manipulated in any way while going through the complex supply chain. Although blockchain has previously been mentioned as a solution in papers, they were mostly focused on the traceability of the drug’s journey from after it has been produced to the patients. There can be manipulations even before the drug enters the supply chain. In order to counteract this, our paper will focus on maintaining a blockchain based system even in the production stage.

1.3 Research Objective

This paper aims to create a decentralized and two-fold blockchain based system, where we propose a method through which drugs can be tracked from the very beginning of production till it reaches the end consumers. Blockchain is a decentralized technology that can work with sensitive information by the use of encrypted ledger, and so authenticity and accountability is ensured. Digital protocols called smart contracts are used to establish trust between the stakeholders. The complex drug supply-chain, if made decentralized, can be made more transparent and therefore easier to trace back to its root. The idea is to create a private and permissioned blockchain database which will be regulated by the Food and Drug Administration and the Government of the respective countries. When it comes to blockchain implementation, hyperledger frameworks, especially hyperledger fabric, are given the most priority for supply chain management due to its security and scalability. Hyperledger Fabric is said to be a “mature framework”, from which we can expect low latency, high throughput and problem-specific privacy solutions. [29]Therefore our objective is to build a blockchain based framework with hyperledger fabric where all the stakeholders in a drug supply chain can exist within a network but can still be controlled through different permissioned set-up. We use barcode technology, since RFID is not as immune to hackers, to make it possible to scan a specific medicine to its block where all the verified and unaltered information is stored. The background study, framework of the system and the exact working procedure will be discussed in following sections.

Chapter 2

Literature Review

A system was proposed in [10] to track and trace the entire supply-chain of drugs, starting from the extraction of raw materials. Here, a private blockchain database is proposed, which will be controlled by the department of pharmaceutical and the Government through consensus mechanism - proof of authority and certifications will be provided for proper authentication. The blocks will be digitally signed every time it changes hands within the stakeholders. QR code is used so that the information of the block of any specific drug can be reached by scanning, which ensures transparency.

In another research [12], methods were discussed to stop the anticounterfeiting of drugs to prevent millions of deaths around the world by a blockchain based Supply Chain system, where they track the ownership proof of the drug from being manufactured till it is delivered to the customer. The ownership is verified by the certificate signed by the Certificate Authorities. Each owner has a unique hash digital identity for tracking. Customers or any owner can track all the steps and owners of the drug with this digital identity.

A blockchain based tamper proof system [11] was shown where the communication between all the participants is transparent, which provides the traceable system with strong authentication and security. Tracking systems are used in this process, which stores information such as the place of origin of the product and to whom the next supply will go till it reaches retailers. Every core information about the management and movement of the product is tracked and stored by it. Additionally, smart-tags are to be attached to each package, so that customers retrieve the whole history of that product.

A plan was proposed in [19] to eradicate lack of visibility of the manufacturing stages of products to end stage journeys so that the health-care industry can be free of counterfeit drugs. They suggested a solution that presents a blockchain-driven tool that can be used to record and time-stamp the transfer of goods at each point in the pharmaceutical supply chain. Every step of a drug's supply chain, from manufacture, distribution, and its expiry, will be noted and time-stamped. A distributed ledger would be used to ensure the security and safety of the product. The record and time-stamp would also be accessible by various entities by scanning a barcode.

According to [13], Elliptic Curve Digital Signature Algorithm (ECDS) can be used to counteract drug counterfeiting using the blockchain system to ensure forgery-free authentication. The smaller size keys of Elliptic Curve Cryptography ensure an

equal level of cryptography.

A scenario oriented blockchain system for drug traceability and regulation called Drug ledger was demonstrated in [6], which restructures the whole service architecture.

Drug ledger follows several principles:

- The system should truly reflect the practical drug transaction logic of the supply chain, especially the drug package, repackage, unpackage, and order canceling.
- It should guarantee both authenticity and privacy of the stakeholder's traceability information.
- It should be able to counter Sybil attacks.
- The data storage of the blockchain system should not continuously increase without end, which guarantees Scalability.

The framework proposed in [16] focuses on vaccines, and not just the traceability of its supply-chain, but also the production procedure with the help of a double-level blockchain structure. One level is proposed to be private to keep the production record of vaccine enterprises encrypted, the other level will be public and will contain the vaccine information. Cutting mechanism is also implemented so that the used-up batches can be deleted from the database.

A storage system was explained in [8] for a real time blockchain network to tackle counterfeit drug supply-chain. Monitoring systems require stable data storage for rapid analysis and detection performance. Data is transmitted in real time to prevent overloading of monitoring servers in input of Apache Kafka. It stores input data by designating topics by network and data type, and then uses Apache storm to extract the information needed to analyze the data stored in Kafka. Preprocessing data is stored in a database.

Chapter 3

Background Analysis

In this section we will dive into a deeper understanding of the concepts of blockchain and hyperledger fabric which will further assist us to continue our research. The core principles that are needed for our system architecture are discussed here.[24]

3.1 Blockchain

Blockchain is cryptography enabled technology widely known as “a distributed ledger with smart contracts” which assists peer to peer transactions without the need for a representative in between [25].

3.1.1 Blockchain Basics

In general terms, blockchain is a chain of blocks where the block contains data that cannot be manipulated. A shared and immutable ledger is established between organizations, which maintain a record of asset transactions with the help of digital protocols known as smart contracts in a blockchain that are programmed to execute when certain conditions are fulfilled.

Distributed ledger technology: A ledger is distributed between all the participants in a blockchain network. All the participants have the access of the complete ledger and the transactions are recorded just once. Once a transaction is recorded in this shared ledger, it becomes immutable and so cannot be altered [37].

Peer to peer: A game changing feature that blockchain networks hold is that it is a peer to peer network. The exchange of any asset happens between just the participants without any involvement of third party institutions. Trust is built since all peers have the exact copy of transaction records which has never been tampered with.

Cryptographically secured: To ensure the ledger is tamper-proof cryptography is used. Once any information is updated in the blockchain, it should be practically impossible to change that. [14]

Smart Contracts: Smart contracts, in a blockchain, are self-executing programmed rules designed to perform specific tasks depending on some predefined set of condi-

tions. Since this is an automated process, efficiency and accuracy is maximized for any transaction through the blockchain network.[36]

Consensus mechanism: Since there is no specific authoritative figure to ensure safe transactions, some algorithms are followed by the blockchain network to update transaction records securely and they are known as consensus mechanisms. These algorithms establish reliability between distributed networks and enable them to work together.[28]

3.1.2 Blockchain Structure

Hash function

Before we move into how blockchain technology works combining all the key elements mentioned above, we must first understand how hash function in blockchain works. Hashing process takes a transaction as an input and gives an output of specific length with the help of hashing algorithms like SHA-256 (used by bitcoin) and is used to create a unique identity of a block. A cryptographic hash function has the following features that make it suitable for cryptography [3]:

- For one particular input, the hash function should always generate the same output every single time
- For the system to be effective the hash function has to be able to generate the output at a good speed
- The process of tracing back to the original data from its hash output should be “infeasible”. It is not completely impossible to get to the original data using brute-force method, so the function must at least ensure that it takes long enough to make that approach invalid.
- For every output “Y”, if k is chosen from a distribution with high min-entropy it is infeasible to find an input x such that $H(k-x) = Y [g]$, where high min-entropy means the value is chosen from such widely distributed outcomes that the predictability of a random value is very unlikely.

The following examples show hashing for a bitcoin blockchain using SHA-256:

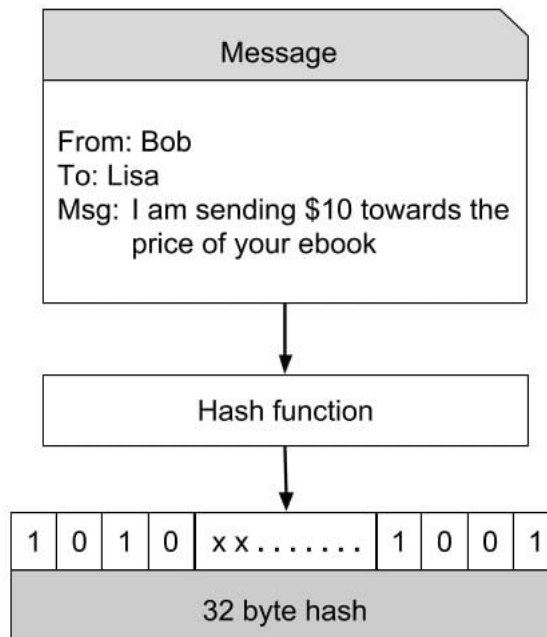


Figure 3.1: Use of hashing function to create unique identity [32]

In the example of Figure 3.1, a transaction happens between Bob and Lisa and that record is saved by encrypting it with a hash function. This 32 byte unique hash will change if any information in this particular record is altered.

```
Sha256(transactions) = 81dc075c3d55230215300137991a25f90be4c243a55580fe2af7538774147bd6  
  
Sha256(Transaction) = eec26ddd9a408449f8e06c622c11d61b94341b04fae5eac8d755c477b8294624
```

Figure 3.2: SHA-256 encryption example [33]

Chaining the Blocks

Just like the name suggests, blockchain is a chain of blocks and we will look into how this mechanism is brought into action. The three fundamental elements we will find are - the data, its unique hash and the hash of the previous function. Figure 3.3 represents the most general form of a block.

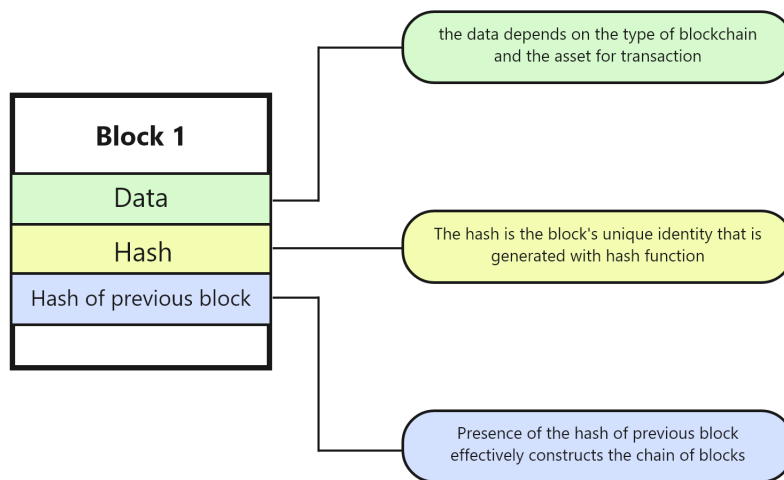


Figure 3.3: A closer look at a block in a blockchain

The first block is called the Genesis block and it does not contain any hash of the previous block since there isn't any. How the blocks are connected in a blockchain network in an immutable manner is demonstrated below in Figure.3.4. The hash values for block n-1, block n and block n+1 are randomly considered just for demonstration.

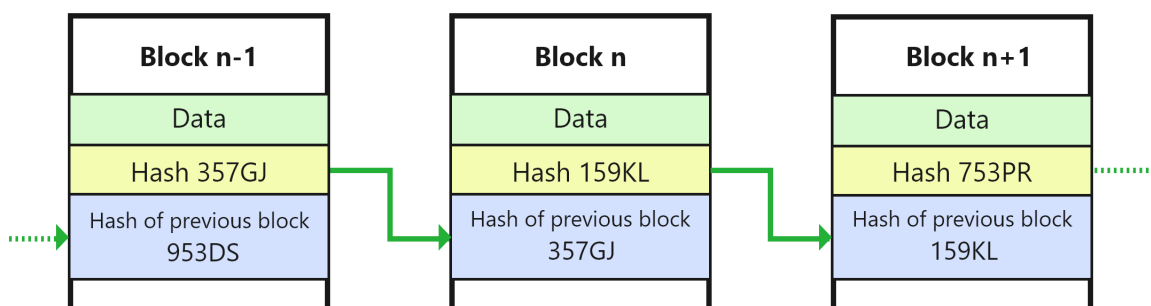


Figure 3.4: Blockchain diagram showing how blocks are linked

Now if we consider someone changed data in Block n-1, the hash of that block is going to change and the new hash is not really saved in Block n. Here the two blocks

(Block n-1 and Block n) are not connected anymore as shown in Figure 3.5. For a single alteration to stay in the chain, all the blocks have to alter their hash which cannot go undetected.

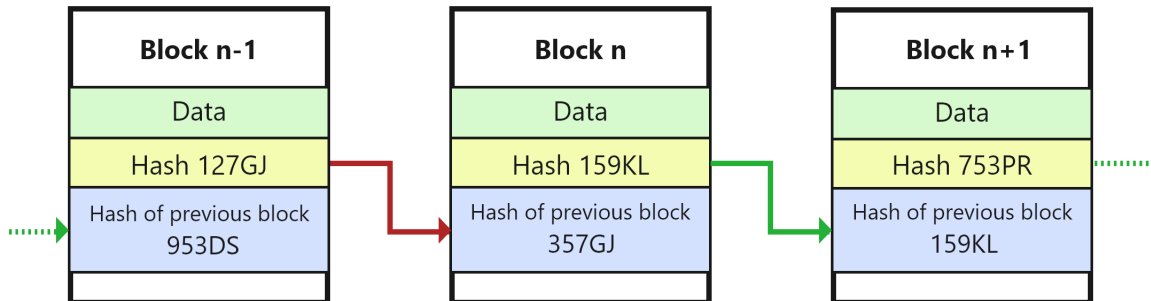


Figure 3.5: Blockchain diagram showing the effect of data alteration

3.1.3 Types of Blockchain

Public blockchain networks

It is an open-sourced, fully decentralized network where anyone is allowed to join and participate. Drawbacks include lack of transaction speed and dissatisfactory scalability. Bitcoin was one of the first public blockchain released. [23]

Private blockchain networks

The level to which one can access the network is controlled by a single organization. We can expect faster output and efficient power consumption from this network. One of the mentionable drawbacks is that it is not completely decentralized which goes against the fundamentals of blockchain technology. [23]

Hybrid blockchain networks

It is a combination between public and private networks where the access permissions are possessed by few pre-determined nodes. It is a good choice if the advantages of both networks are needed, although the process to upgrade to a hybrid network can be burdensome. [23]

Consortium blockchain networks

It is also known as federated blockchain and is managed by more than one organization. Although it provides all the advantages of a private network, it is of

decentralized nature. The speed of transaction is very satisfying since the access control is limited. [23]

3.1.4 Consensus mechanisms

There are different types of consensus mechanisms depending on what type of blockchain is used for the solution.

A logical dilemma termed as Byzantine's General Problem, where a group of generals may face certain communication problems while trying to reach a decision for their next move, is the biggest problem faced while reaching a consensus. In a distributed network, all the nodes will have to agree on the same action to be executed. The ability to resist any failure that can be caused by Byzantine's General Problem and continue to work even if some of the nodes are not reachable is called Byzantine Fault Tolerance. Two highlighted consensus algorithms that can help us build a BFT system are

- Proof of Work
- Proof of Stake

Proof of Work

Although proof of work was introduced long before the existence of bitcoin, Satoshi Nakamoto established a distinctive way to use proof of work as a consensus protocol for bitcoin. In this protocol, miners in a network compete with each other in solving complex computational problems. Miners are responsible for adding new blocks in a blockchain which they will be able to do if they guess a pseudo-random number called nonce. Mining requires a large amount of power making any cost of attack significantly higher than the potential reward and thus providing security to the network. [18]

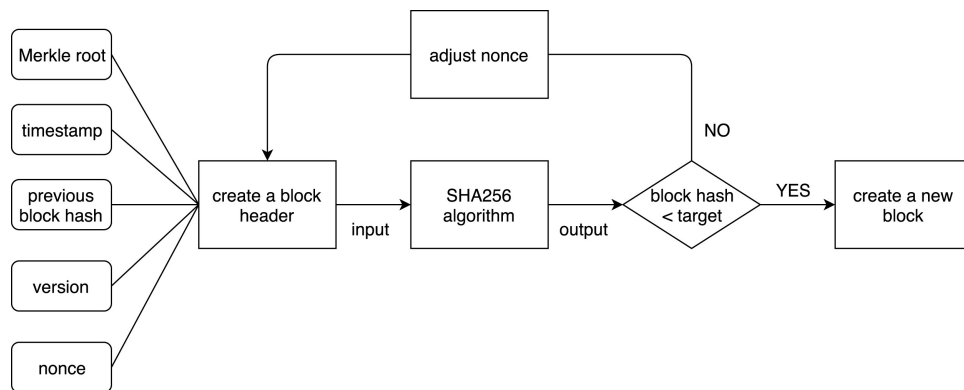


Figure 3.6: Flow of Proof of Work [15]

Proof of Stake

Proof of stake does not include the wasteful process of mining, it has validators who are selected given they have a certain amount of deposit into the network. The chances of a node to be selected as a validator increases with the amount of stake they have in the network and their coin age (amount of stakes * number of days kept). We can trust the validators because they will lose a part of their stake if a suspicious transaction is initiated.

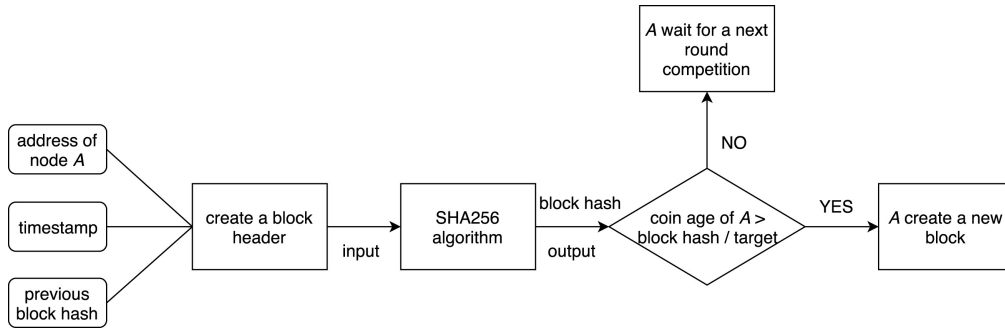


Figure 3.7: Flow of Proof of Stake [15]

3.1.5 Comparison between Blockchain Platforms

	Ethereum	Hyperledger Fabric	R3 Corda
Network Type	Public or Private	Consortium	Permissioned
Security Model	Membership services	Non-encrypted data	Permissioned only
Consensus Mechanism	Proof of Work (requires mining which can be a very expensive process)	Pluggable Mechanism	Notary nodes can run several consensus mechanism
Cryptocurrency	Ether	None, can be made using chaincode	None
Throughput	Roughly 1000 transactions per minute	More than 120,000 transactions per minute	Around 100,000 transactions per minute

Table 3.1: Blockchain platform comparison

3.2 Hyperledger Fabric

Hyperledger fabric, an open source distributed ledger technology platform which can integrate into an infrastructure with minimum complexity, offers some key advantages over other blockchain platforms. Fabric architecture is exceedingly flexible and configurable which can be utilized for the optimization of supply chain management. The key components and features of hyperledger fabric are discussed in this section.

3.2.1 Core Components of Hyperledger Fabric

Assets

Ranging from tangible to intangible, assets are anything that has value. In hyperledger fabric, assets are characterized as a collection of key-value pairs where state changes are recorded as a transaction in the ledger. Assets can be defined and shaped using chaincode transactions. [30]

Smart Contract and Chaincode

Smart contracts and chaincodes are often used interchangeably. Smart contract, defined within a chaincode, is responsible to make the executable business logic of the system which is then further added to the ledger. Chaincodes, on the other hand, are used to group smart contracts for deployment and run in a secured Docker container. Chaincodes can limit the level of trust according to requirements which optimizes the network's performance. [34]

Ledger Features

A ledger consists of - chain which is the transaction log and a state database which is an indexed view into the chain [30]. A ledger is responsible for recording the state and ownership of an asset. **Chains:** Chains consist of blocks that contain sequence of transactions and are cryptographically linked together. The hash of the latest block represents all the transactions made before [30]. **State database:** Stores the latest values of all keys and can describe the state of ledger at any given time [27].

Identity

Every actor (admin, peers, orderer, client application etc) that exist in a blockchain network has a digital identity defined within a digital certificate. For an identity to be verified, it must come from a trusted authority which is controlled by Membership Service Provider [21]. MSP is responsible for managing certificates used to authenticate member identity and roles [27].

Peer Nodes, Channels and Organization

Peers being the host of the ledger and smart contracts, are one of the most fundamental elements of the blockchain network. Peers are owned by different organizations and a logical structure is formed that allows these peers to communicate with each

other within the network. In Figure 3.8 a clear diagram is shown how peers, channels and organizations work together.

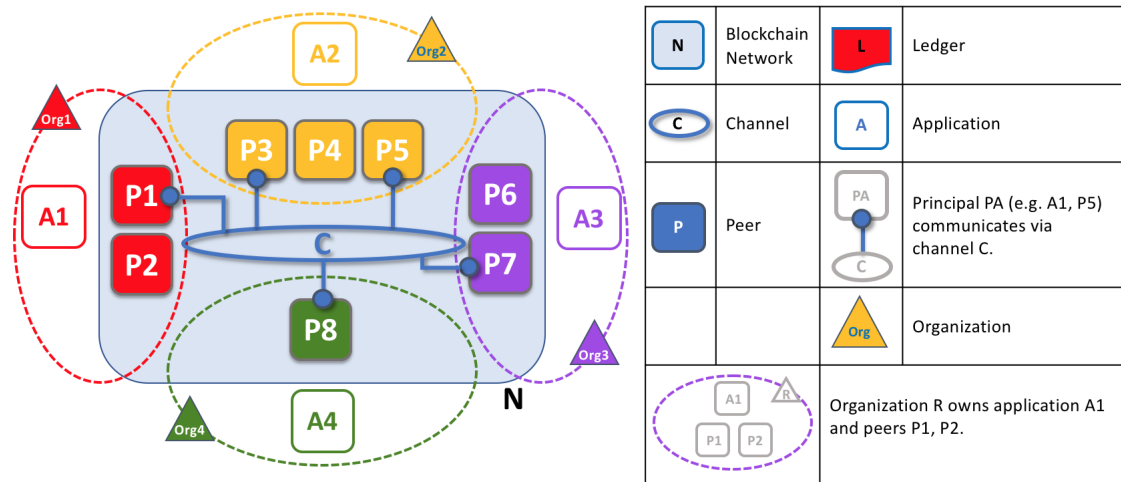


Figure 3.8: Peers-Organization-Channel structure [31]

Peers P1 and P2 are under organization org1, Peers P3, P4 and P5 are under organization org2 Peers P6 and P7 are under organization org3 Peer P8 is under organization org4

Public Key Infrastructure

PKI is a technology that is used to ensure secure communication within the blockchain network. The four element that it is comprised of are:

- Digital Certificates
- Public and Private Keys
- Certificate Authorities
- Certificate Revocation

Digital certificates are issued by CA- Certificate Authorities which hold unique identification details. These certificates can be used to prove the authenticity of the one it belongs to. Certificate Revocation List refers to a list of certificates that are at present invalid. The workflow of these PKI elements are shown in Figure 3.9

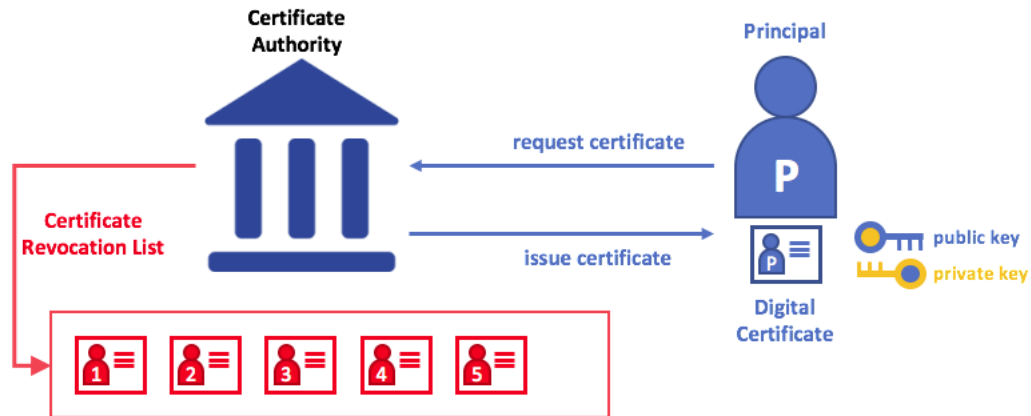


Figure 3.9: PKI element workflow [21]

3.2.2 Features of Hyperledger Fabric

We will be using hyperledger fabric, an open source blockchain technology and the reasons why we decided to go with this blockchain platform are stated below. [26]

Identity management

MSP (Membership Service Provider), a directory structure, is maintained in the hyperledger fabric platform where authentication of participants within the network is maintained. It can contain public or private keys depending on the permission. The types of MSP are: peer MSP, orderer MSP, system channel MSP, application MSP.

Privacy

The concept of channels are introduced in hyperledger fabric through which private transactions can be made between different members within the same network. All the transactions within a specific channel are only visible to the members of that channel. Any other member can exist on the same blockchain network but will not be able to see the data within that channel.

Efficiency

Transaction execution is treated differently than transaction ordering so that they can concurrently work within the system. All the peer nodes can process transactions at the same time as transactions are executed before ordering. The scalability of the hyperledger fabric platform, over 2000 transactions per seconds, is remarkable and makes it so much more efficient than the other blockchain platforms.

Modular architecture

The system is designed in a way that a wide range of implementations are possible.

- Algorithms can be specified for how exactly a business wants to use hyperledger fabric.
- A pluggable MSP uses cryptographic identities to connect entities in the network.
- A peer-to-peer gossip service is available which enables distribution of the output of one block to other peers by ordering service.
- Smart contracts can be programmed using standard programming languages

Chapter 4

Proposed Model

4.1 Blockchain Based Pharmaceutical Supply-chain Model

We aim to prevent data fraud of production records after the certification is given to the drug producers. So the production record will be kept in the blockchain and a hash value will be added to each block according to how all the data is treated. Hash value is generated by an encryption algorithm and it changes if anybody tries to change the data inside the block. A private database is used to protect the privacy of the product records and will be maintained by pharmaceutical regulatory agencies as the primary node and all nodes are connected to it. After the product record is generated, it needs to be in a block with hash, previous hash and timestamp. When it is finally approved as shown in the flowchart, the records can not be altered because that will change the hash and the primary node will be notified. After the drug block gets digitally certified, it moves to the next process mentioned in the following flowchart. (Figure 4.1)

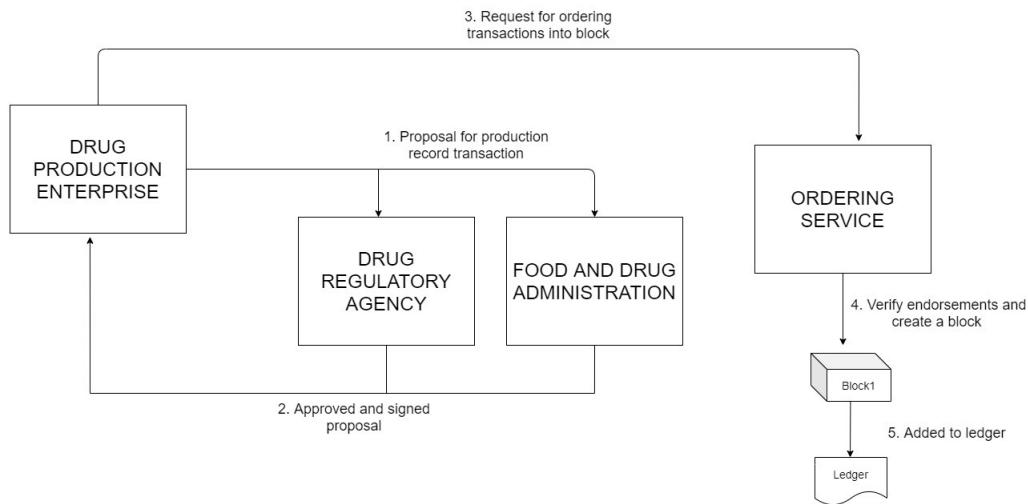


Figure 4.1: Working process of the blockchain in production phase of drugs

After the drug passes the production phase a smart contract is created by the drug administration to avoid the counterfeit of drugs. After being manufactured another smart contract (through chaincode) will run between the distributor and the manufacturing company for every batch of drugs. This smart contract will make sure that the distributor is getting the actual product by the company and the ownership of that batch will be transferred from the company to the distributor. Once again when the distributor distributes the drugs between various transporters, the distributed products ownership will be changed by another smart contract between the wholesaler and distributor. Finally when the whole seller delivers the product to various hospitals and local pharmacies the last smart contract will be will it take place between the local hospital, pharmacies and the wholesalers. By this smart contract the owner of the product will be able to track the previous owner and every step of the development and manufacturing process. When finally the drug is bought by the user they can easily check the credibility of the drug by scanning the barcode which will contain all the details and smart contract of the drug. (Figure 4.2)

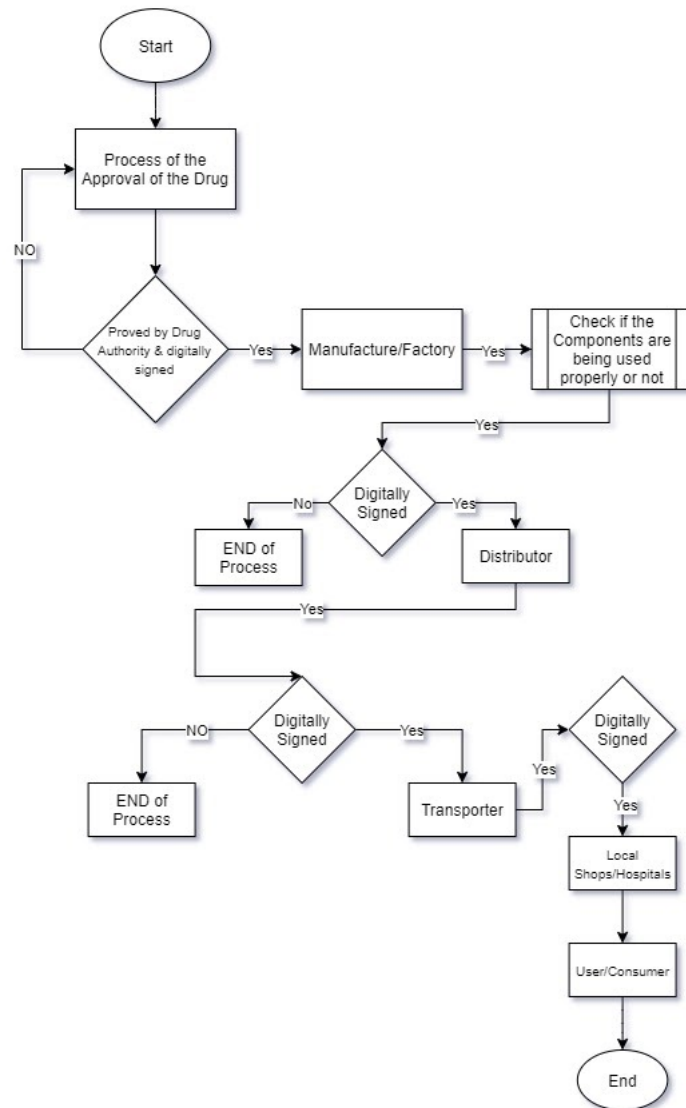


Figure 4.2: Working process of the blockchain in supply chain of drugs

4.2 System Architecture

In Figure 4.3, the way all the organizations (/members) are connected by forming a blockchain network is shown.

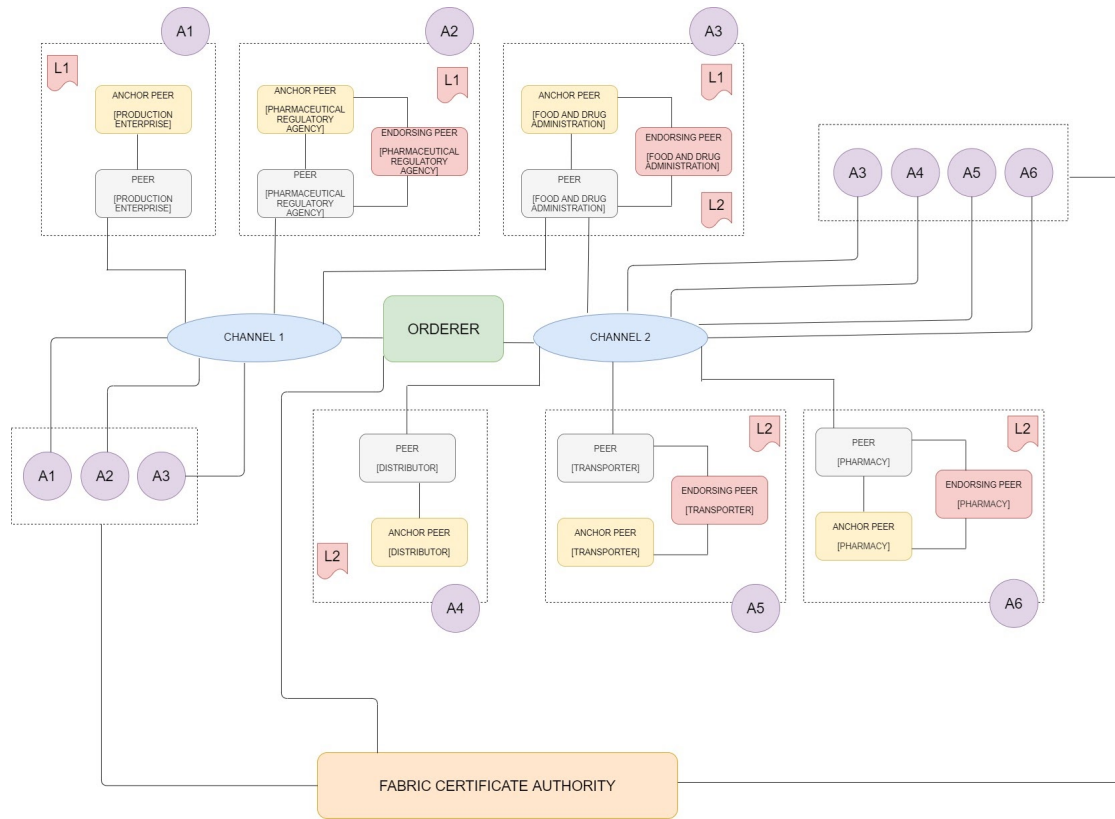


Figure 4.3: System architecture of the blockchain network

Applications

Applications through which the members are going to reach the systems are denoted by A. Applications owned by several members are denoted in the figure as: A1 : Production Enterprise A2 : Pharmaceutical Regulatory Agency A3 : Food and Drug Administration A4 : Distributor A5 : Transporter A6 : Pharmacy

Channels

There are two channels in our blockchain network. Channel 1 is private and owned by Production Enterprise, PRA and FDA. Since we are making a blockchain network which will include the production level, we must ensure the privacy of the production record of the enterprise. Channel 2, on the other hand, is public and owned by FDA, distributor, transporter and pharmacy.

Ledgers

Here L1 and L2 are the two ledgers in the networks which are maintained by channel 1 and channel 2 respectively. The members of only channel 2 do not have the permission to see the data within the L1 ledger.

Ledger L1 contains the production report of the drug

Ledger L2 contains information of drugs once it enters the supply chain

Fabric Certificate Authority

As mentioned in the figure, the managerial rights belong to the government and for any members to get enrolled into this network, a certificate (one root certificate and one enrollment certificate) from fabric CA will be required.

Peers

Endorsing peers: Before a transaction is submitted to the ordering peer, it will require the sign of every (entitled) endorsing peers. For example, in case of channel 1, the endorsing peers (connected to Pharmaceutical Regulatory Agency and Food and Drug Administration) must ensure the production records and production sample batches are consistent.

Anchor peers: Since connecting so many peers together with one another can be a complex process, anchor peers connect the organizations(/members) within the same channel through gossip protocol.

Orderer peers: The orderer peer is the first node created in the network and will be controlled by the government as well. The orderer peer orders all the transactions into a block and sends it to all the peers in a channel so that it can further be included in the blockchain ledger by the peers.

4.3 Workflow

The step by step procedure of how our blockchain network works starting from the production phase of drugs to the consumers and explained below:

4.3.1 Production Phase

Step1:

After producing a batch of drugs, the Production enterprise will generate a production record and hash it with the help of a cryptographic hash function SHA256. Transactions will be proposed towards the agency and FDA for approval. In Fig. 14 we can see how transactions T1, T2, T3 are generated from A1 (production enterprise) and are passed to both DRA and FDA for individual endorsement. Later on, if the production samples and records are approved then the transactions are digitally signed (endorsed) and the endorsed transactions are sent to A1.

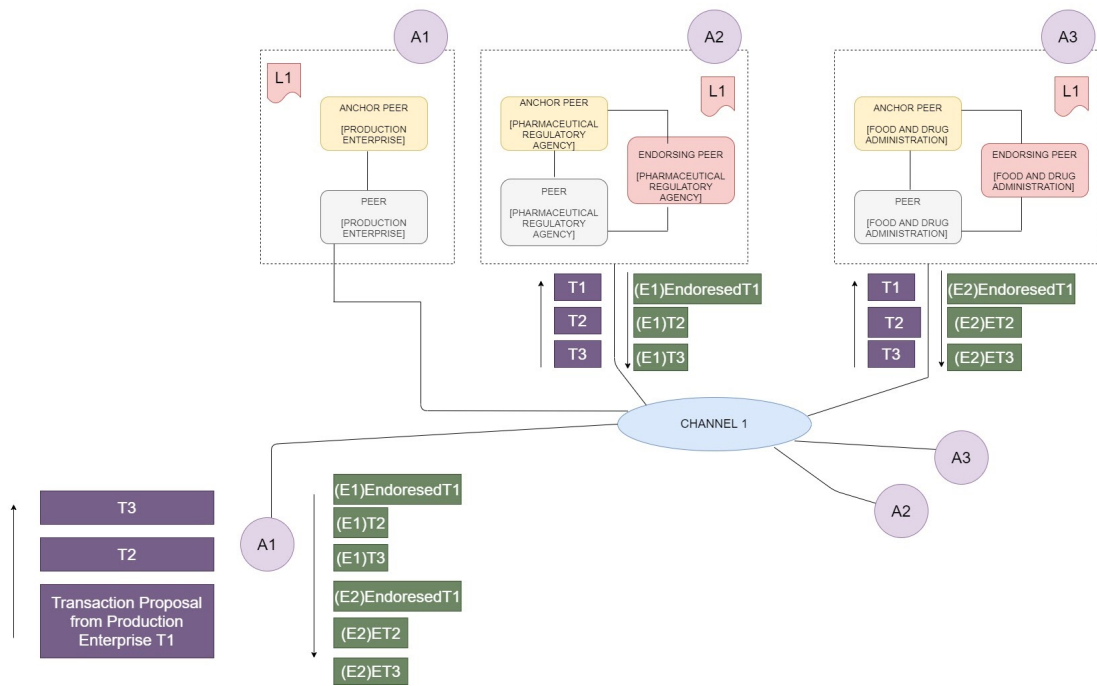


Figure 4.4: Workflow of production phase- step1

Step2:

After the transactions are endorsed and signed by all the required peers, it is further sent to the orderer peer where all the transactions are packaged into a block as shown in Figure 4.5.

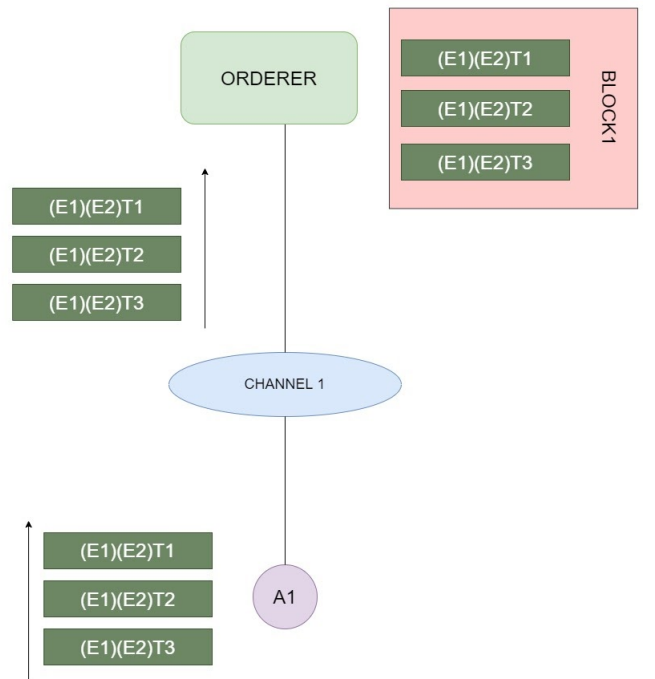


Figure 4.5: Workflow of production phase- step2

Step3:

After the orderer peer, controlled by the managerial authority, creates a block it sends the block to all the peers in the channel for further validations. When all the required digital signs are achieved, the block is then added to the ledger as shown in Figure 4.6. All the members in channel 1 maintain the same copy of ledger L1 and so single point failure is avoided. Once the block is added to the ledger and forms a chain with other blocks (created in the same way), the transaction report becomes immutable and so the trust is ensured.

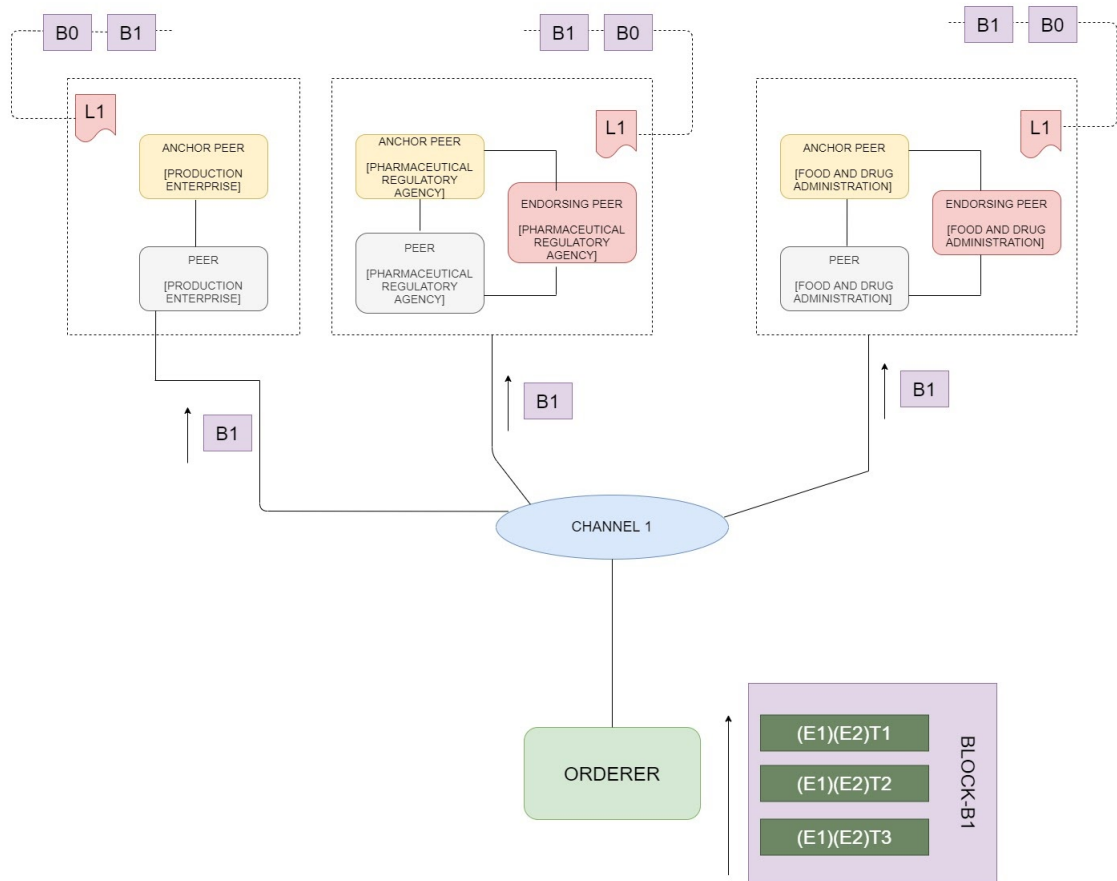


Figure 4.6: Workflow of production phase- step3

4.3.2 Supply Phase

In case of the supply phase which is handled by channel 2, the ledger L2 maintained is public and the data can be viewed by members of channel 1. The members of channel 2, distributor, transporter and the pharmacy will all sign a transaction whenever it changes hands. The data that goes in the blockchain from every member is shown in Figure 4.7.

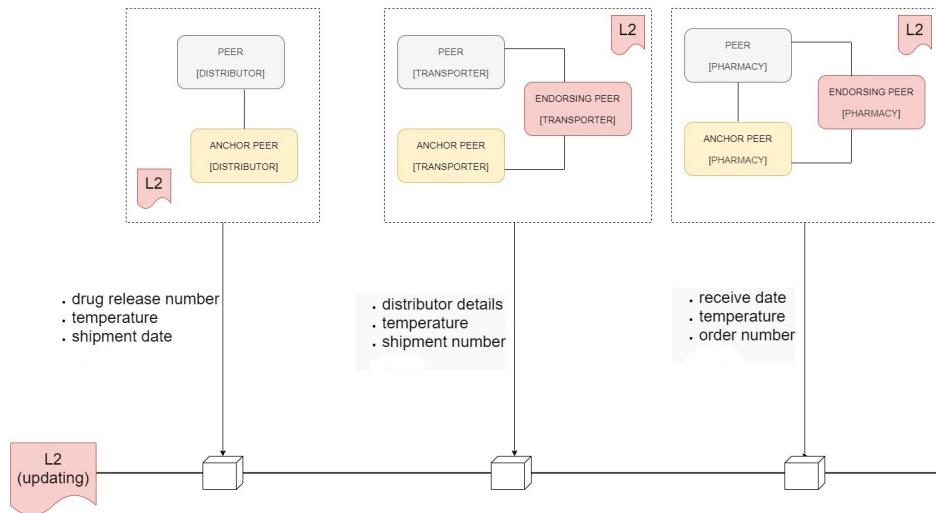


Figure 4.7: Workflow of supply phase

Chapter 5

Implementation

In this paper we worked with Hyperledger Composer which is a comprehensive framework that supports Hyperledger Fabric blockchain foundation and makes it easier to develop applications. Hyperledger composer can ensure the authentication of transactions with the policies that the network participants define, since it supports pluggable consensus algorithms. [35]

5.1 Configuration model

There are four different sources to get started with the configuration [9]:

- Model file
- Transaction scripts
- Access control lists
- Query scripts

Model file

Model file in hyperledger composer is comprised of the fundamental entities of the network:

Assets

In our proposed network model the assets are -

- active pharmaceutical ingredients and the drug itself as the commodity, which are the goods that are to be exchanged and tracked through this network.
- Smart contract for drug enrollment and transaction update

An instance of creating asset in Hyperledger composer is shown in Figure 5.1, Figure 5.2 and Figure 5.3

Create New Asset
✕

In registry: org.example.bc.Commodity

JSON Data Preview

```

1 {
2   "$class": "org.example.bc.Commodity",
3   "Assests": "Drug",
4   "api_Name": "Paracetamol tablet",
5   "details": "Napa Extend",
6   "manufacturer": " X Pharmaceutical Company",
7   "date_of_expiry": "20/12/25",
8   "owner":
9   "resource:org.example.bc.Trader#org.example.bc.TraderPharmaceutical
   Company"
}
```

Optional Properties

Just need quick test data? [Generate Random Data](#)

Cancel

Create New

Figure 5.1: creating asset

ID	Data
Drug	<pre> { "\$class": "org.example.bc.Commodity", "Assests": "Drug", "api_Name": "Paracetamol tablet", "details": "Napa Extend", "manufacturer": " X Pharmaceutical Company", "date_of_expiry": "20/12/25", "owner": "resource:org.example.bc.Trader#org.example.bc.TraderPharmaceuticalCompany" }</pre> <div style="text-align: right; margin-top: 5px;"> Collapse </div>

Figure 5.2: Asset displayed in database

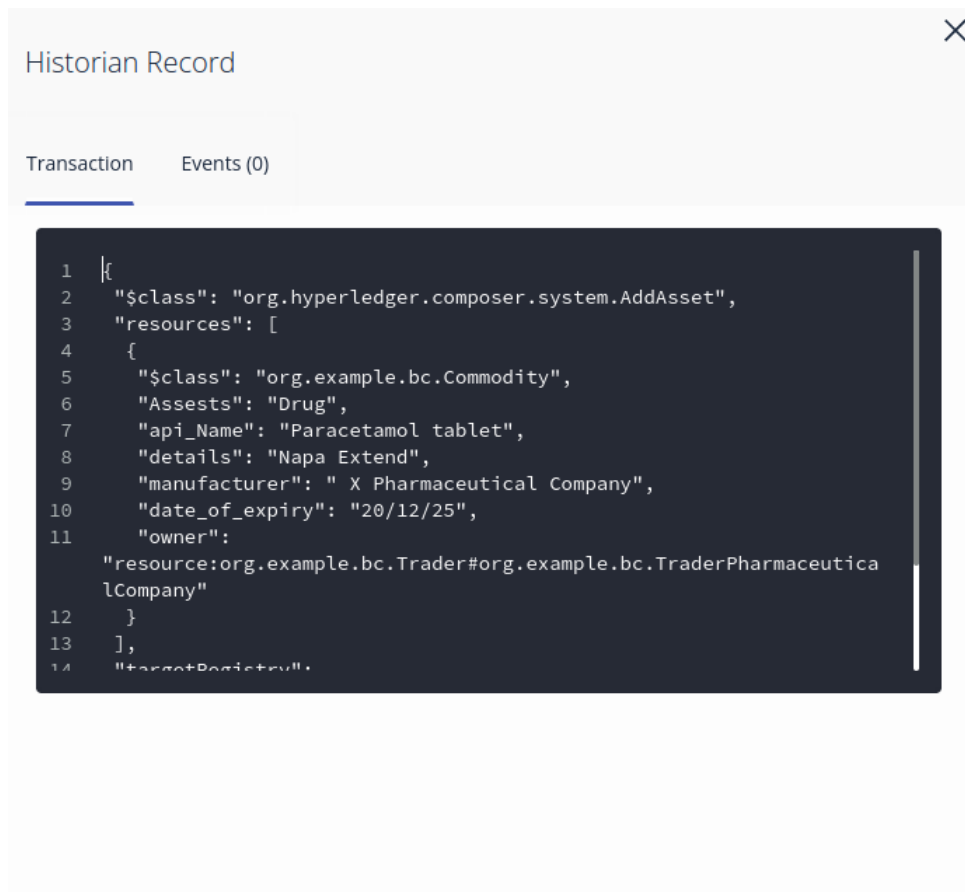


Figure 5.3: Historian record of assets with timestamp

Participants

Participants are the supply chain members: Production Enterprise, Distributor, Transporter, Pharmacy and end Consumer. Regulatory agency and drug admin do not really need to be here because An instance of creating participants in Hyperledger composer is shown in Figure 5.4, Figure 5.5 and Figure 5.6

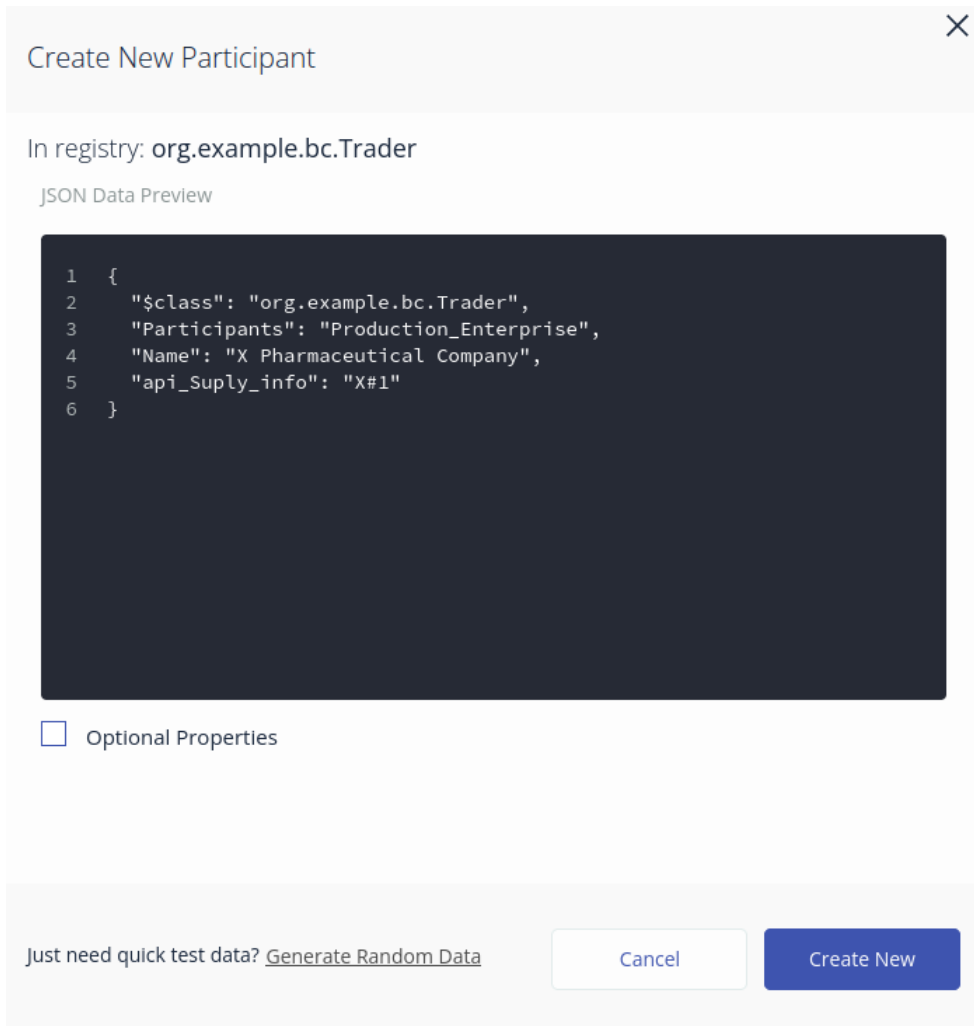


Figure 5.4: creating asset

ID	Data
Production_Enterprise	<pre>{ "\$class": "org.example.bc.Trader", "Participants": "Production_Enterprise", "Name": "X Pharmaceutical Company", "api_Suply_info": "X#1" }</pre>

Figure 5.5: Asset displayed in database

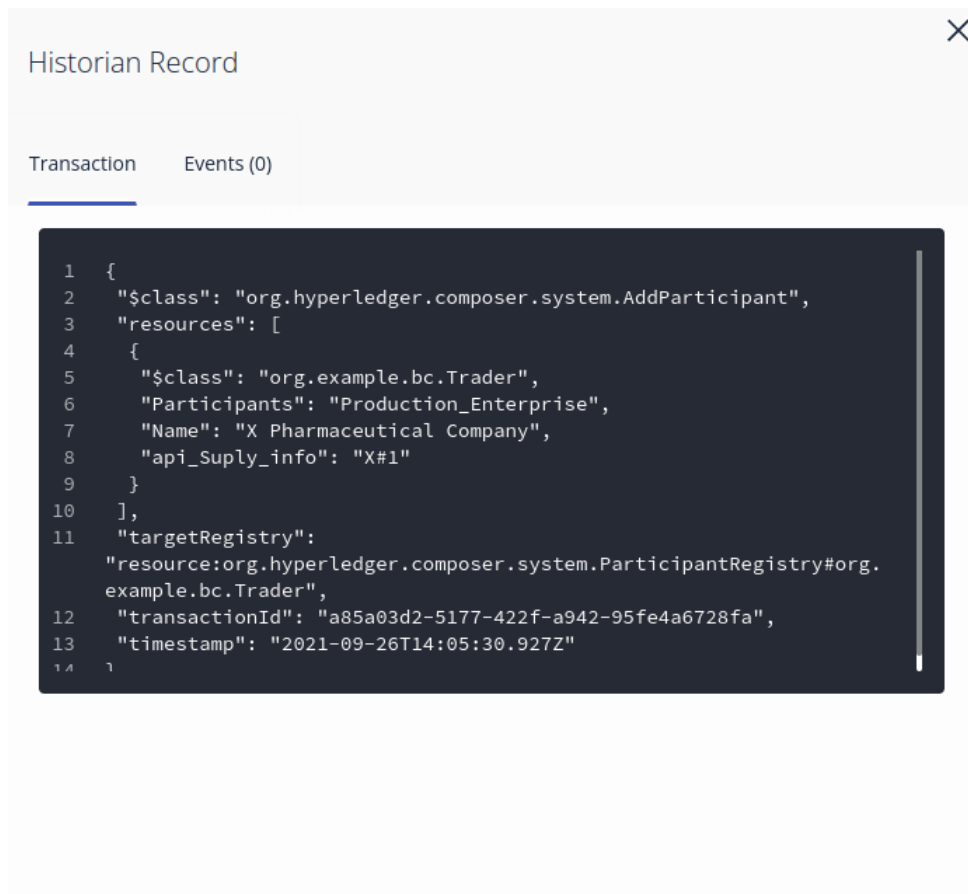


Figure 5.6: Historian record of assets with timestamp

Transaction description

The transaction description will include updated details about active pharmaceutical ingredients, drugs and the updated ownership status. Figure 5.7 is an illustrative representation of model files.

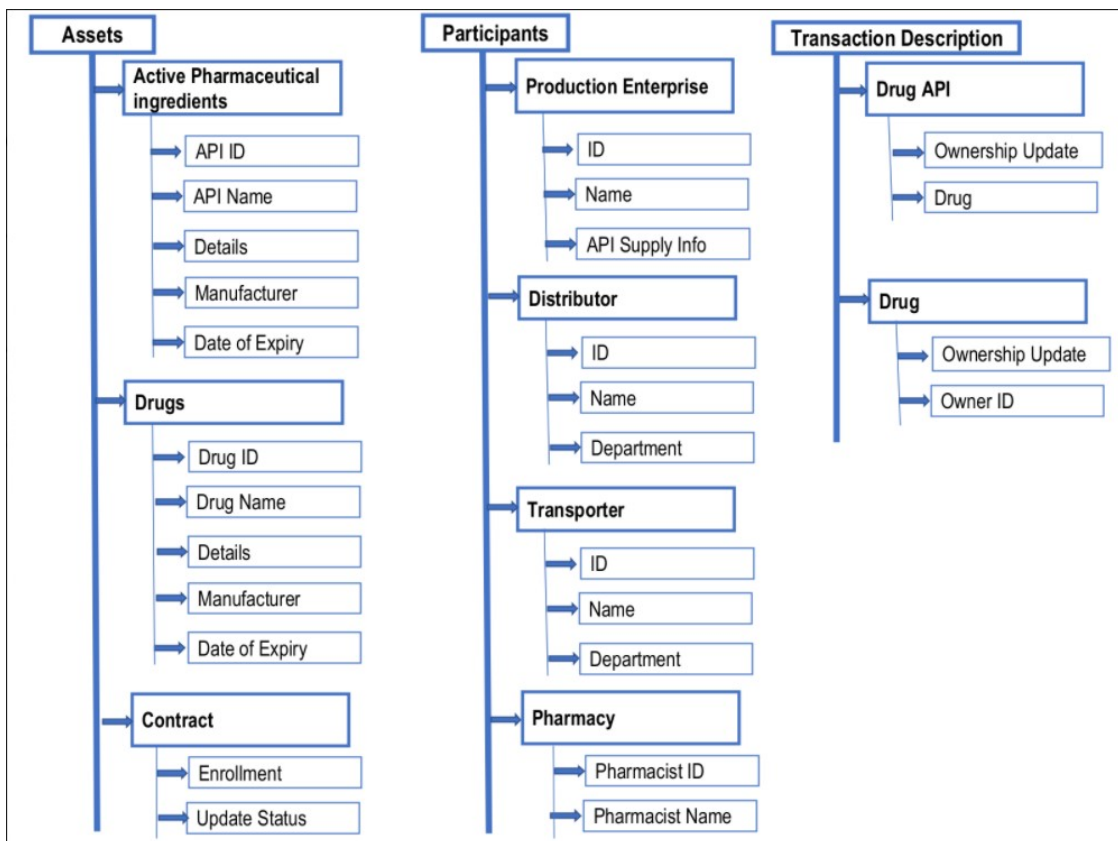


Figure 5.7: Model file illustration

Transaction scripts

Transaction scripts are chaincode that are executed to build and maintain the network. Our proposed model has the following chaincode: addParticipants drugRegistration issueIdentity ownerAPIUpdate ownerDrugUpdate

Access Control List

This where the participants get the access of Creating, Reading, Updating and Deleting asset information according to the right they are given by the administrator. Admin is in control and so has the power to do anything, whereas participants can read anything but other actions are limited to their right.

An instance of ACL for our model is shown in Figure 5.8

```
ACL File permissions.acl
17
18 rule NetworkAdminSystem {
19     description: "Network admin has full access to assets"
20     participant: "composer.system.NetworkAdmin"
21     operation: READ, CREATE, UPDATE
22     resource: "org.example.bc.system.**"
23     action: ALLOW
24 }
25
26 rule productionEnterprise{
27     description: "production enterprise is allowed to update API info"
28     participant: "composer.participant.productionenterprise"
29     operation: READ, UPDATE
30     resource: "org.example.bc.drugAPI.ownerUpdate"
31     action: ALLOW
32 }
33
34 rule distributor{
35     description: "distributor is allowed to update drug status"
36     participant: "composer.participant.distributor"
37     operation: READ, UPDATE
38     resource: "org.example.bc.drug.ownerUpdate"
39     action: ALLOW
40 }
```

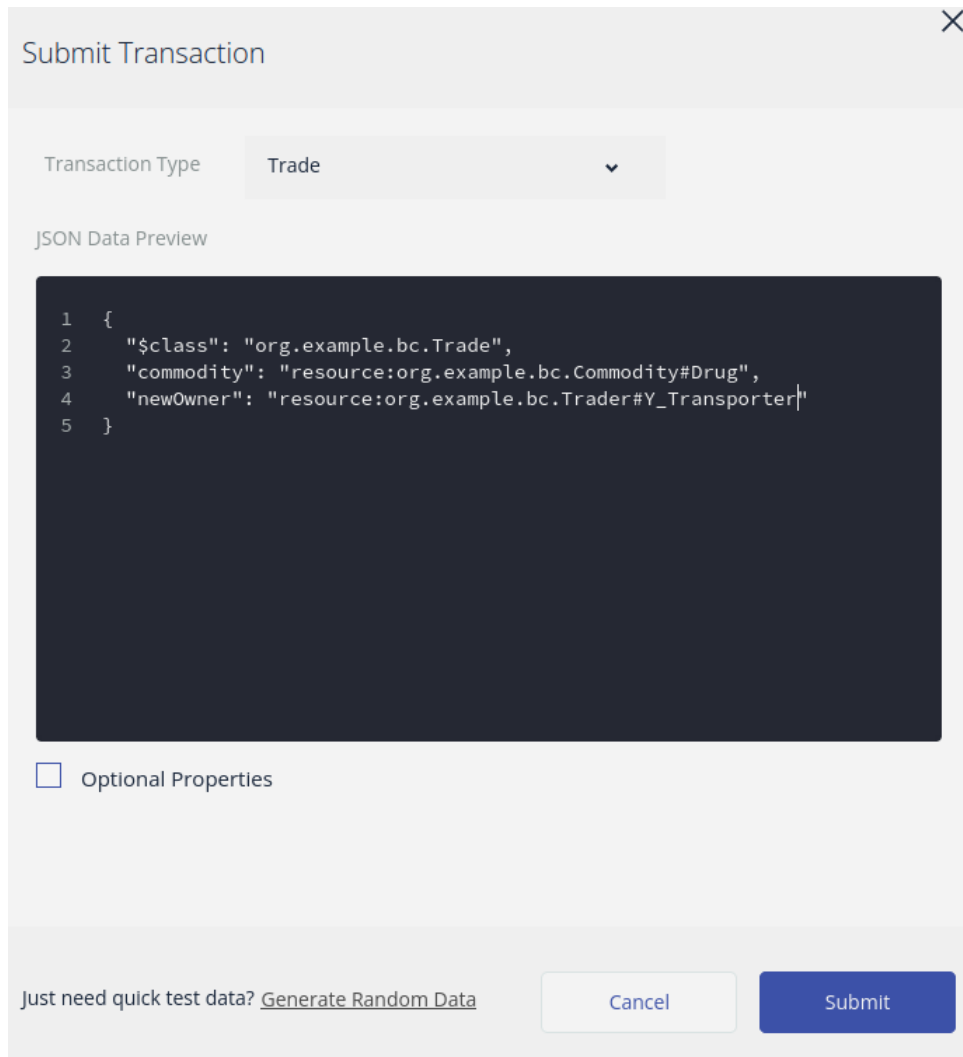
Figure 5.8: ACL for the network

Query Script

This mainly comes into play to show data from blockchain through front-end applications. To query the basic information about participants, assets and transactions, Hyperledger Composer has predefined access points. [9]

5.2 Transaction instance

In the following case, shown in Figure 5.9, a transaction occurs and is submitted. When we update the owner of our asset, an ID is displayed Figure 5.10 with the confirmation that the transaction is submitted successfully. In Figure 5.11 historian record is shown along with the timestamp of when the transaction occurred.



Submit Transaction

Transaction Type Trade

JSON Data Preview

```
1 {
2   "$class": "org.example.bc.Trade",
3   "commodity": "resource:org.example.bc.Commodity#Drug",
4   "newOwner": "resource:org.example.bc.Trader#Y_Transporter"
5 }
```

Optional Properties

Just need quick test data? [Generate Random Data](#) Cancel Submit

Figure 5.9: A transaction is submitted

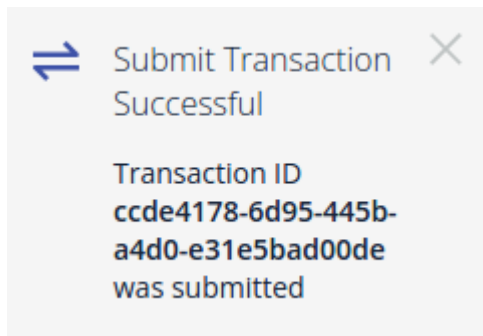


Figure 5.10: Successful transaction



Figure 5.11: Historian record of transaction

In the following Figures we can see that the owner of the drug has changed in the database

ID	Data
Production_Enterprise	<pre>{ "\$class": "org.example.bc.Trader", "Participants": "Production_Enterprise", "Name": "X Pharmaceutical Company", "api_Suply_info": "X#1" }</pre>

Figure 5.12: Drug with previous owner record

ID	Data
Drug	<pre>{ "\$class": "org.example.bc.Commodity", "Assests": "Drug", "api_Name": "Paracetamol tablet", "details": "Napa Extend", "manufacturer": " X Pharmaceutical Company", "date_of_expiry": "20/12/25", "owner": "resource:org.example.bc.Trader#Y_Transporter" }</pre> <p style="text-align: right;">Collapse</p>

Figure 5.13: Drug with updated owner record

5.3 Scope for performance analysis

Scope for performance analysis Since we did not show up to the front-end integration of the network, exact performance analysis could not be portrayed in this paper. Although there are few points we want to discuss about how performance of hyperledger fabric supply chain network may vary depending on various elements. Factors that can play a part in Hyperledger Fabric's performance are [20]:

- Number of endorsing peers
- Number of channels
- Number of endorsements (endorsement policy)
- Ordering service configuration (block size and frequency)
- Number of organizations
- Ledger database used
- Complexity of chaincode/smart contract execution
- Size of transactions
- Use of mutual TLS for all network traffic
- Number of vCPUs
- Memory allocation
- Disk type and speed
- Network speed
- Multiple datacenter deployment
- CPU speed
- Crypto acceleration

An experiment was done using Hyperledger Fabric 1.3.0 in a single Kubernetes cluster running on the IBM Container Service and the following results were obtained comparing average throughput and latency of the network with a varying number of endorser peers.

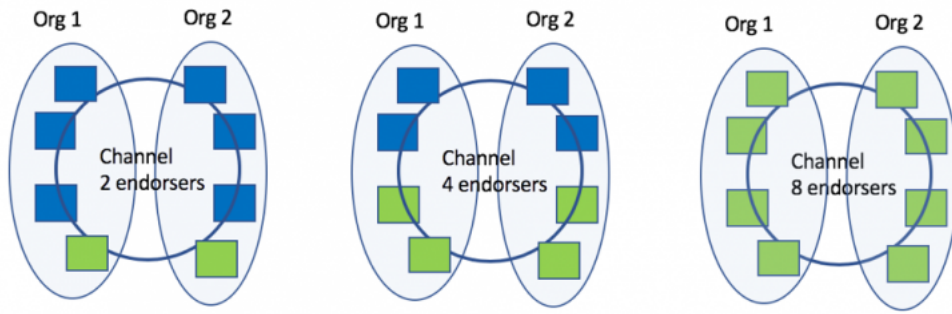


Figure 5.14: Network with a varying number of endorser[20]

# endorsers	2		4		8	
TPS 95% (ms)	785.58	715	948.2	667	1265.5	686

Figure 5.15: TPS with a varying number of endorser[20]

There it is a better idea to arrange more number of endorser to distribute balance and achieve more throughput per second.

Chapter 6

Conclusion and Future Work

This paper works using blockchain technology to secure the supply chain of the pharmaceutical industry from the production processing of drugs. Among all the blockchain platforms there is, hyperledger fabric is the best suited one for the desired implementation since fabric gives a wide range of pluggable options for consensus, provides remarkable performance while dealing with assets like drugs and much more that has been discussed. We extensively discussed about how the technology works and have shown how our blockchain network involving many organizations will be arranged into two channels and the transaction flow within that network. We have also shown how the ledgers will be updated along with the transactions. We further demonstrate the implementation of Hyperledger Composer to create a model of our supply chain network.

Although we have used Hyperledger composer as a tool for our implementation, it holds a status of "end of life" since August 2021 since no developer is maintaining the tool anymore. Thus the best practice is to use Hyperledger Fabric 2 as the platform and build it from scratch. The potential future direction would be to use fabric 2 and integrate couchDB.

Bibliography

- [1] C. C. Halder, *Trial of rid pharma finally starts*, Feb. 2012. [Online]. Available: <https://www.thedailystar.net/news-detail-222513>.
- [2] W. H. Organization *et al.*, “Definitions of substandard and falsified (sf) medical products,” *Seventieth World Health Assembly Update*, vol. 29, 2017.
- [3] A. Rosic, “What is hashing?[step-by-step guide-under hood of blockchain],” *View Online-https://blockgeeks.com/guides/what-ishashing*, 2017.
- [4] Mar. 2018. [Online]. Available: <https://www.drugtrackandtrace.com/solution-for-the-substandard-and-counterfeit-medicin>.
- [5] Apr. 2018. [Online]. Available: [https://www.drugtrackandtrace.com/2018-world-serialization-map/..](https://www.drugtrackandtrace.com/2018-world-serialization-map/)
- [6] Y. Huang, J. Wu, and C. Long, “Drugledger: A practical blockchain system for drug traceability and regulation,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 2018, pp. 1137–1144.
- [7] J. G. B. M. 7, J. G. Breman, A. t. A. R. J. G. Breman @Fogarty_NIH, J. G. Breman @Fogarty_NIH, C. H. O. says: and D. H. C. says: *It’s time to stop murder by counterfeit medicine*, May 2019. [Online]. Available: <https://www.statnews.com/2019/05/07/stopping-murder-counterfeit-medicine/>.
- [8] J. Bang and M.-J. Choi, “Design and implementation of storage system for real-time blockchain network monitoring system,” in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, 2019, pp. 1–4.
- [9] P. Costa, Feb. 2019. [Online]. Available: <https://medium.com/collectiv-stories/implementing-a-blockchain-supply-chain-proof-of-concept-wit%20hyperledger-composer-ee91204f4ef9>.
- [10] A. Kumar, D. Choudhary, M. S. Raju, D. K. Chaudhary, and R. K. Sagar, “Combating counterfeit drugs: A quantitative analysis on cracking down the fake drug industry by using blockchain technology,” in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, 2019, pp. 174–178.
- [11] S. Madumidha, P. S. Ranjani, S. S. Varsinee, and P. Sundari, “Transparency and traceability: In food supply chain system using blockchain technology with internet of things,” in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2019, pp. 983–987.

- [12] R. Raj, N. Rai, and S. Agarwal, “Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership,” in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, IEEE, 2019, pp. 1572–1577.
- [13] M. Sahoo, S. S. Singhar, B. Nayak, and B. K. Mohanta, “A blockchain based framework secured by ecdsa to curb drug counterfeiting,” in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, 2019, pp. 1–6.
- [14] I. Specialist, *How blockchain technology works*, Oct. 2019. [Online]. Available: <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034>.
- [15] S. Zhang and J. Lee, “Analysis of the main consensus protocols of blockchain. ict express (2019),” *Online: https://doi.org/10.1016/j.ictexpress*, vol. 1, 2019.
- [16] S. Peng, X. Hu, J. Zhang, X. Xie, C. Long, Z. Tian, and H. Jiang, “An efficient double-layer blockchain method for vaccine production supervision,” *IEEE Transactions on NanoBioscience*, vol. 19, no. 3, pp. 579–587, 2020.
- [17] S. Piranty, *Coronavirus fuels a surge in fake medicines*, 2020.
- [18] A. Rosic and Blockgeeks, *Proof of work vs proof of stake: Basic mining guide*, Jun. 2020. [Online]. Available: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>.
- [19] N. Saxena, I. Thomas, P. Gope, P. Burnap, and N. Kumar, “Pharmacrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs,” *Computer*, vol. 53, no. 7, pp. 29–44, 2020.
- [20] Feb. 2021. [Online]. Available: <https://www.ibm.com/blogs/blockchain/2019/01/answering-your-questions-on-hyperledger-fabric-performance-and-scale/>.
- [21] M. Glenna and F. Woie, “Blockchain based hospital data management using hyperledger fabric,” B.S. thesis, uis, 2021.
- [22] M. Mikulic, *Pharmaceutical counterfeit incidents worldwide 2002-2020*, Sep. 2021. [Online]. Available: <https://www.statista.com/statistics/253150/counterfeit-incidents-concerning-pharmaceutic>.
- [23] *What are the different types of blockchain technology?* Sep. 2021. [Online]. Available: <https://101blockchains.com/types-of-blockchain/>.
- [24] [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html?fbclid=IwAR0wpkrF>.
- [25] [Online]. Available: <https://www.ibm.com/cloud/architecture/architectures/blockchainArchitecture..>
- [26] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, “Et almbbox. 2018a. hyperledger fabric: A distributed operating system for permissioned blockchains,” in *European Conf. on Computer Systems (EuroSys)*. ACM, vol. 30.
- [27] *Blockchain basics: Hyperledger fabric*. [Online]. Available: <https://developer.ibm.com/articles/blockchain-basics-hyperledger-fabric/>.
- [28] *Consensus mechanisms*. [Online]. Available: <https://ethereum.org/en/developers/docs/consensus-mechanisms/>.

- [29] A. Day, N. Jain, Hyperledger, G. Joseph, and A. Gulley, *Supply chain archives*. [Online]. Available: <https://www.hyperledger.org/tag/supply-chain..>
- [30] *Hyperledger fabric model*. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric_model.html#assets.
- [31] *Peers*. [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html>.
- [32] W. says: *How does blockchain work? - blockchain transaction - intellipaat*. [Online]. Available: <https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/>.
- [33] *Sha256 decrypt encrypt*. [Online]. Available: <https://md5decrypt.net/en/Sha256/#answer..>
- [34] *Smart contracts and chaincode*. [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/smartcontract/smartcontract.html>.
- [35] *Welcome to hyperledger composer*. [Online]. Available: <https://hyperledger.github.io/composer/v0.19/introduction/introduction.html>.
- [36] *What are smart contracts on blockchain?* [Online]. Available: <https://www.ibm.com/topics/smart-contracts>.
- [37] *What is blockchain technology?* [Online]. Available: <https://www.ibm.com/topics/what-is-blockchain>.