Gokaraju Rangaraju Institute of Engineering and Technology

(Autonomous)

Department of Computer Science and Engineering

GR17A4144 - Major Project

IV Year/ II Semester

Academic year 2020-2021

Cryptosystem for medicine supply chain management using Hyperledger-Fabric.

Section : F

Batch No.: 10

Batch Members:

1. 17241A05U2 Abhishek Bhandwalkar
2. 17241A05U7 Srinivas Golla
3. 17241A05Y3 Prashant Sharma
4. 18245A0568 Shaik Asif
5. 18245A0567 G. Bhanu Teja

Project Guide:

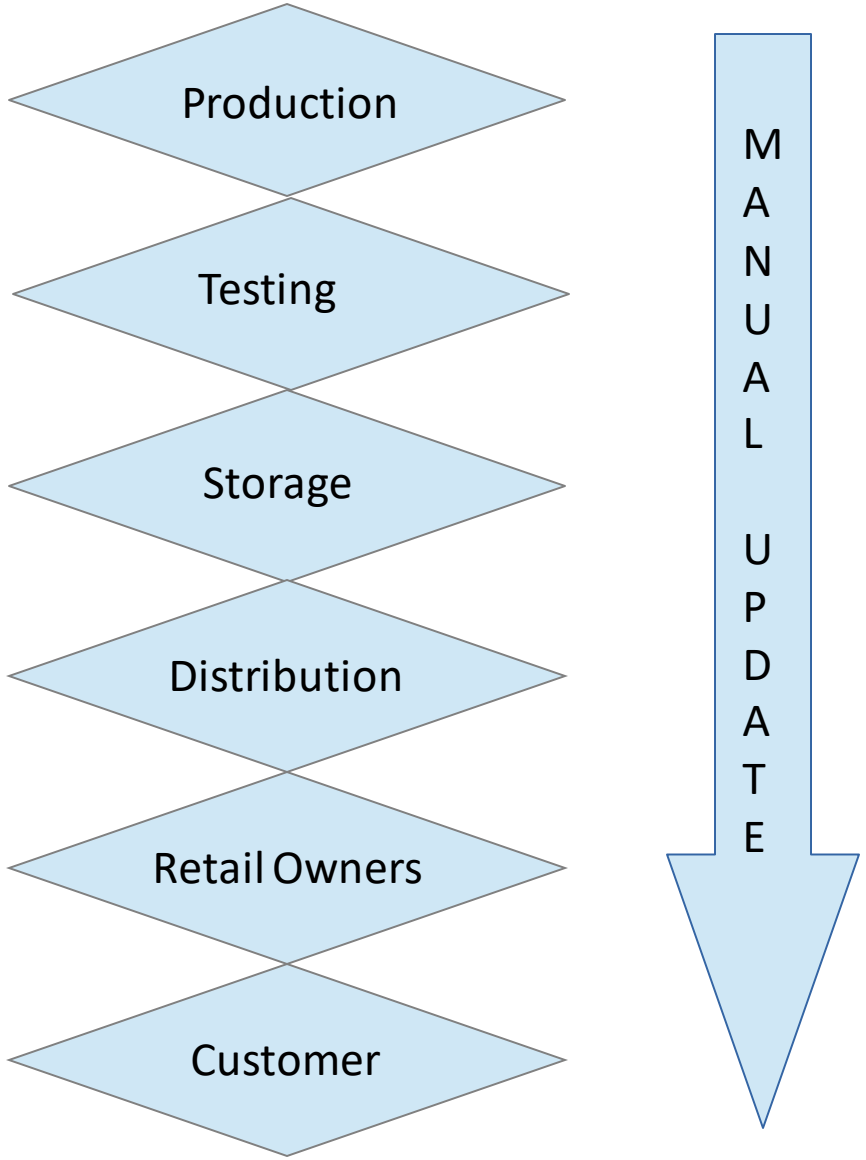
Dr. K. Kavitha

PROBLEM STATEMENT

- In a rapidly developing industrial world. The important aspect of an organization is supply chain management being able to monitor and track the progress of commodities increases the production and transparency in the product manufacturing.

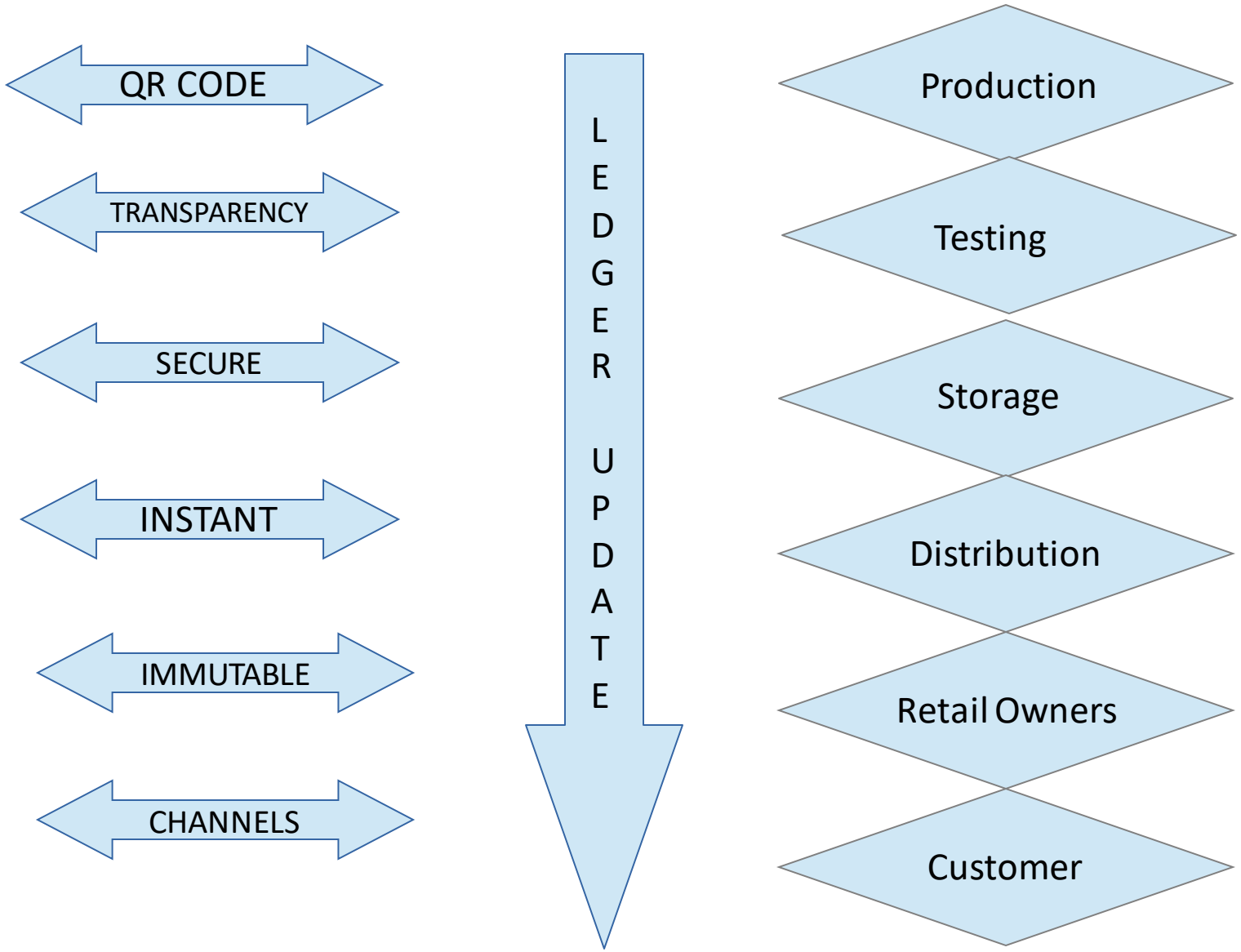
- We have proposed a system specifically dedicated to tracking the progress of medicines from production to the point it reaches the customer. Technologies deployed in the development of this project involve Hyperledger-Fabric, Docker, Frameworks of JavaScript. This project is based on the platform of private blockchain Hyperledger Fabric. Which is a project initiated by the Linux community in 2016 for providing business solutions using blockchain.

EXISTING APPROACH



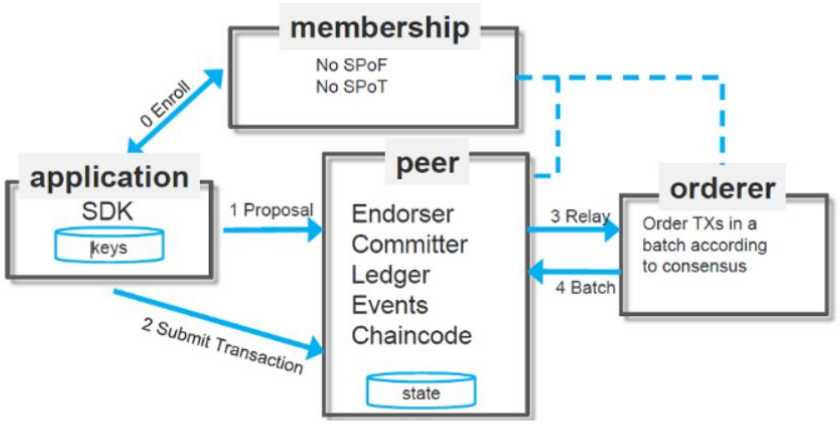
PROPOSED APPROACH

HYPERLEDGER - FABRIC



ARCHITECTURE

• Here when clients submit the transaction proposal through the Fabric SDK, this proposal is sent to all Endorsing Peers. These endorsing peers check the transaction verifies and executes and generate the Read and Write set as output. Now, this response is again sent to the client. The client collects all responses from all endorsing peers, and send them to Orderer. Now, Orderer sees all transactions and orders them in ascending order and form a block. Now, this block is sent to all committers which checks the transaction and add a new block in their own copy of the ledger.



MEMBERSHIP SERVICE PROVIDER (MSP)

- The membership service provider (MSP), is a component that defines the rules in which, identities are validated, authenticated, and allowed access to a network. The MSP manages user IDs and authenticates clients who want to join the network. This includes providing credentials for these clients to propose transactions. The MSP makes use of a *Certificate Authority*, which is a pluggable interface that verifies and revokes user certificates upon confirmed identity. The default interface used for the MSP is the Fabric-CA API.

PEERS

- A node that commits transactions and maintains the state and a copy of the ledger. A peer receives ordered state updates in the form of *blocks* from the ordering service and maintains the state and the ledger. Besides, peers can have a special endorser role. The special function of an *endorsing peer* occurs with respect to a particular chaincode and consists in *endorsing* a transaction before it is committed.

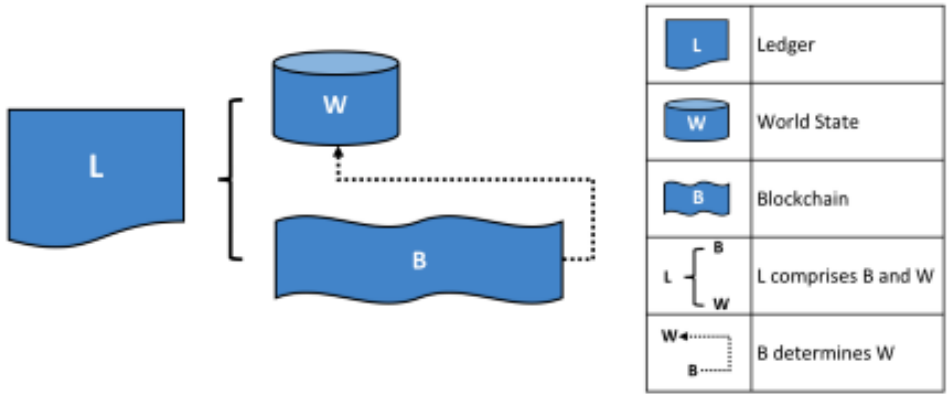
- **Endorser :** A specific peer role, where the Endorser peer is responsible for simulating transactions, and in turn preventing unstable or non-deterministic transactions from passing through the network. A transaction is sent to an endorser in the form of a transaction proposal. All endorsing peers are also committing peers (i.e. they write to the ledger).
- **Committer :** A specific peer role, where the Committing peer appends the validated transactions to the channel-specific ledger. A peer can act as both an endorser and committer, but in more regulated circumstances might only serve as a committer.

CHAINCODE

- A smart contract defines the transaction logic that controls the lifecycle of a business object contained in the world state. It is then packaged into the chaincode which is deployed to the blockchain network. Smart contracts are defined within chaincode. Multiple smart contracts can be defined within a single chaincode. When a chain code is deployed, all smart contracts available within the chaincode is made available to the application. We can see that a smart contract is a domain specific program which relates to specific business processes, whereas a chaincode is a technical container of a group of related smart contracts for installation and instantiation. Every chaincode has endorsement policy attached to it, which applies to every smart contract defined within it. This identifies which organization must sign a transaction generated by Smart contract, in order to consider it valid. So, in short, every smart contract has an endorsement policy attached to it. A smart contract can call other smart contracts within a channel or across different channels.

LEDGER

- It is a current state of the business as a journal of transaction. A ledger consists of two different parts, a **world state,** and a **blockchain**. A ledger is kept at all peers and, optionally, at a subset of orderers.



LEDGER

1.WORLD STATE:

- Each chaincode has its own World state and blockchain. It is a DB that holds the current state of the ledger state. These states are expressed as key-value pairs. It holds the fact of a business object. It can be created, update and delete. When application submits the transaction, and when it comes to committing the valid transaction, it first commits in the World state and then it is updated in ledger.

2.BLOCKCHAIN:

- A transaction log that records all the changes that have resulted in the current world state. Its data structure is different as once written cannot be removed. It is immutable. It is a historical record of facts about how the objects arrived at the current state. It is structured as a sequential log of interlinked blocks, where each block contains a sequence of transactions, each transaction representing a query or update to the world state

ORDERER

- Hyperledger Fabric works differently. It features a node called an **orderer** (it's also known as an "ordering node") that does this transaction ordering, which along with other orderer nodes forms an **ordering service**.
- In addition to their **ordering** role, orderers also maintain the list of organizations that are allowed to create channels. This list of organizations is known as the "consortium", and the list itself is kept in the configuration of the "orderer system channel"
- Orderers also enforce basic access control for channels, restricting who can read and write data to them, and who can configure them.

PROPOSED MODULES

Setting up of networks	Creation of organizations for different departments in medicine production	Creation of peers and order node	Creating users on peers nodes
Generating authentication certificates	Creating first transaction	Checking the status of world state	Updating the ledger for successful transaction
API communication	Connecting API to front end	Development of front end	Testing the application over the front end

- Step-1: A block is created upon the invention of a new medicine or medical care which includes patent protection and a long process of clinical trials. This information is recorded in the digital ledger as a form of transaction.
- Step-2: Once the clinical trial is successful, the patent is sent to the manufacturing plant for test prototype and mass production. Every product has its own unique identity that is integrated with another transaction or block in the blockchain including other relevant information
- Step-3: Once the mass production along with packaging is finished, medicine is gathered in a warehouse for future distribution. Information such as, time, lot number, barcode, expiry date is included in the blockchain

- Step-4: Transportation information is also included in the blockchain which may include time out from one warehouse (IN) to other, mode of transportation, authorized agent, and other information.
- Step-5: A third-party distribution network is normally responsible for distributing drugs and medical supplies to healthcare providers or retailers. A warehouse (OUT) for each third party is used for this purpose from where all distribution endpoints are linked. A separate transaction is also integrated into the blockchain.
- Step-6: Care providers such as hospitals, or clinics need to provide information, for example, batch number, lot number, product owner, expired date to authenticate, and prevent counterfeit.This is also included in the blockchain.
- Step-7: The actions taken by a retailer are similar to Step-6.
- Step-8: Patients are encouraged to determine authenticity throughout the whole process as blockchain supply chain offers transparent information for verification to potential buyers.

IMPLEMENTATION AND TEST CASES

CONCLUSION

- Hyperledger Fabric is the most active of the Hyperledger projects. The community building around the platform is growing steadily, and the innovation delivered with each successive release far out-paces any of the other enterprise blockchain platforms.
- By harnessing the capabilities of Hyperledger we are developing a decentralized application which aims to setup a clear communication in all phases of production of medicines
- So that medicine containers can be tracked in case of false deliveres

- ROBUST MONITORING : One of the key things that the network management team of healthcare needs right now is overseeing, powerful monitoring of all kinds of transactions. The feature that sets Blockchain apart from other healthcare management systems is that it documents all kinds of transactions in the form of a decentralized record. It is precise and transparent to the core that effectively saves time, effort, and cost, thus also saving the hassle of constant management.
- ENHANCED COLLABORATION: A big amount of success of any healthcare initiative depends largely on the people involved like third parties, professionals and researchers. Blockchain technology enhances the collaboration among these participants with the help of its distributed ledger technology through which they can provide deep insights and do group research.

- DATA PROTECTION: the main issue that the healthcare industry is facing is the leakage of significant data and it being used for malicious means and for other vested interests. Another focus area is that the participants and parties involved in the database have access to the most updated and authentic patient data and diagnosis information. Blockchain is made up of the most advanced cryptographic aspects, which makes it immutable. That facilitates data authenticity accompanied by a digital signature, along with foolproof data security stabilizing the issues of security and trust.
- COST-EFFICIENT CURES AND PROCESS SIMPLIFICATION

SCOPE

In the future we would like to extend the project by connecting the database to the cloub by making use of services like AWS or Azure.

Currently we are deploying the project using docker we would like to experiment with other micro services like kubernetes.

Also we would implement the front end in django and use django rest framework for the API deployement

REFERENCES

- https://hyperledger-fabric.readthedocs.io/en/release-2.2/
- https://www.hyperledger.org/learn/research
- https://docs.docker.com/
- L. Foschini, A. Gavagna, G. Martuscelli and R. Montanari, "Hyperledger Fabric Blockchain: Chaincode Performance Analysis," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149080.
- https://blog.clairvoyantsoft.com/hyperledger-fabric-components-and-architecture-b874b36c4af5