DEFINE PROBLEM/ PROBLEM UNDERSTANDING

Business Requirements

Team Id	NM2023TMID04410
Project Name	Project- Drug Traceability

Business Requirements In Drug Traceability :

Blockchain based platform, Hyperledger Fabric and Besu meets essential needs for drug traceability such as privacy, dependability, transparency, security, authorization, authentication, and scalability.

A BLOCKCHAIN-BASED DRUG TRACEABILITY SYSTEM FOR PHARMACEUTICAL SUPPLY CHAINS :

The stakeholders are envisioned to access the smart contract, decentralized storage system and on-chain resources through software devices that have front-end layer denoted by a DApp (Decentralized Application) which is connected to the smart contract, on-chain resources, and decentralized storage system by an application program interface (API) such as Infura, Web3, and JSON RPC.

The stakeholders will interact with the smart contract to initiate pre-authorized function calls and with the decentralized storage systems to access data files. Finally, their interaction with the on-chain resources will be for obtaining information such as logs, IPFS hashes, and transactions. More details on the system components are presented below.

- **Stakeholders** include regulatory agencies such as FDA, manufacturers, distributors, pharmacies, and patients. These stakeholders act as participants in the smart contract and are assigned specific functions based on their role in the supply chain. They are also given access to the on-chain resources such as history and log information to track transactions in supply chain. Further, they are authorized to access information stored on the IPFS such as the drug Lot images, and information leaflets.
- **Decentralized Storage System** (IPFS [42])provides a low-cost off-chain storage to store supply chain transactions data to ensure reliability, accessibility, and integrity of the stored data. The integrity of data is maintained by generating a unique hash for every uploaded file on its server, and the different hashes for the different uploaded files are then stored on the blockchain and accessed through the smart contract, and any change that occurs to any of the uploaded file is reflected in the associated hash.

- **Ethereum Smart Contract** is used to handle the deployment of the supply chain. The smart contract is central and essential for tracking the history of transactions and manages the hashes from the decentralized storage server which allows the participants to access the supply chain information. Moreover, the functions of the different stakeholders in the supply chain are defined within the smart contract and access to these functions is given to the authorized participants by using modifiers. A modifier is basically a way to decorate a function by adding additional features to it or to apply some restrictions. The smart contract also handles the transactions, such as selling drug Lots or boxes.

- **On-chain Resources** are used to store the logs and events that are created by the smart contract allowing track and trace. Moreover, a registration and identity system is used as an on-chain resource to associate the Ethereum address of the different participants to a human readable text which is stored in a decentralized way.

The system components are envisaged to function in an integrated manner to track the history of the drug under consideration to verify its authenticity, and no real-time tracking will be required because the DApp user will only need to use the proposed solution to verify that the drug under consideration is not counterfeit and it came from a trusted manufacturer. If real-time location of a drug Lot is to be tracked, a number of technologies can be implemented to accomplish this task. For example, IoT-enabled smart containers is equipped with sensors that continuously monitor and track the TRU from its starting point to its destination. The IoT sensor includes Global Positioning System (GPS) receiver to locate where the TRU is at, temperature sensor to keep track of the temperature, and pressure sensor to measure the pressure differences that detect any opening or closing of the container [43]

Figure 3 illustrates interaction among different participants of the supply chain within proposed system and can be loosely divided into three phases explained below.

Manufacturing: Typically, a manufacturer will send a request for approval from the FDA to initiate the manufacturing process of a drug Lot. Once the FDA approves the request, the manufacturer initiates the manufacturing process and an event is declared to all participants. The manufacturer will upload images of the drug Lot to the IPFS, and the IPFS will send a hash to the smart contract so that the images can be accessed later by authorized participants. The drug Lot will be delivered to the distributor for packaging concluding the manufacturing process.

Distribution: The next step is the initiation of the distribution process, the distributor will pack the drug Lot, and an image of the package will be uploaded to the IPFS which will send a hash to the smart contract. Once this step is completed, the drug Lot packages will be delivered to pharmacies, and this ends the distribution phase.

Sale/Consumption The last step in the sequence diagram is related to the interaction between the pharmacy and the patients. Here, the pharmacy will initiate the sale of drug Lot box and it will be declared to the participants of the supply chain. Then, an image of the sold drug package will be uploaded to the IPFS, and a hash will be sent by the IPFS to the smart contract. The drug Lot box will be sold to the patient, and this concludes the drug Lot selling phase. This process will ensure that all the transactions are stored and can be accessed later by all the supply chain participants to check the authenticity and validity of the products in the supply chain in the form of a sequence of events.

TABLE 1. Comparison between our proposed solution and the non-blockchain solutions

	Smart-Track	**Data-Matrix Tracking System**	**NFC**
Decentralized	No	No	No
Resilience	No	No	No
Integrity	No	No	No
Tracking and Tracing	Yes	Yes	Yes
Security	No	No	No
Transparency	No	No	No

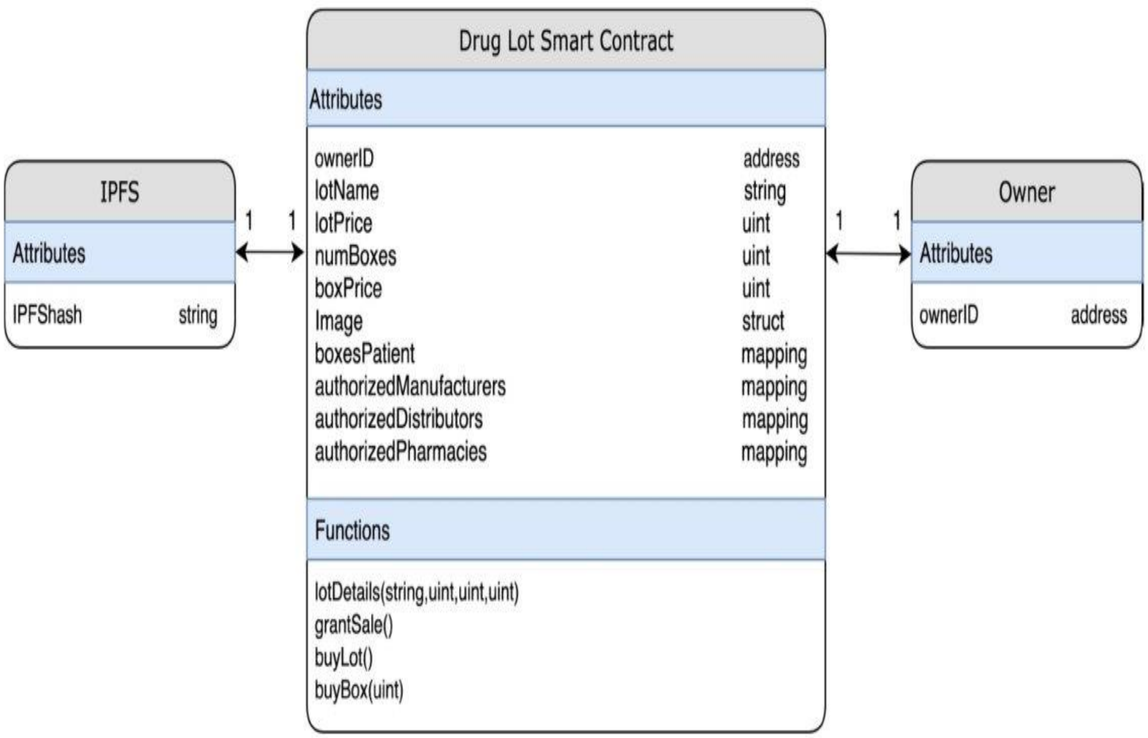
COMPARISON OF PROPOSED SOLUTION WITH EXISTING SOLUTIONS

In this section, we present a comparative analysis of the proposed solution for traceable supply chain for pharmaceutical drugs with relevant existing solutions. A summary of this analysis is presented in Table 1. The proposed solution is decentralized which is an important feature as it prevents any single entity from manipulating or modifying the data. Another important feature of our solution is resilience, since the solution is decentralized, it eliminates single point of failure. Blockchain offers excellent solution for data integrity and security due to its features such as data immutability, therefore once the information is added to the edger it cannot be removed or modified. The security of data is maintained because it's stored in a decentralized way which makes no single entity capable of simultaneous manipulation of data. Transparency of transactions is an important aspect for any supply chain. In our proposed solution, all participants can access and view the verified all transactions in a trusted environment. Finally, all the solutions in Table 1 share one common feature which is the track and trace feature, however other features such as decentralized storage, integrity and transparency are fundamental to achieving a trustworthy track and trace system.

Table 2 compares our proposed solution with other blockchain-based solutions. Our solution uses Ethereum blockchain where as the solution in [34] uses Bitcoin blockchain and the solution in [32] uses Hyperledger-Fabric. Moreover, both our solution and [34] operate in public permissioned mode whereas [32] operates in private permissioned mode which is an inherent feature in Hyperledgerfabric. The payment method in our solution is Ether which is the currency of Ethereum. The solution in [34] uses BTC currency and [32] does not have a currency. Furthermore, in all solutions data is stored on-chain but our solution has an additional feature which allows storing data off-chain as well. Finally, Both our solution and [32] have programmable modules which are the smart contract and docker container respectively. However, the solution in [34] does not provide a programmable module.

TABLE 2. Comparison between our proposed solution and other blockchain-based solutions

	Our Solution	Huang et al [34]	Faisal et al [32]
Blockchain Platform	Ethereum	Bitcoin	Hyperledger-Fabric
Mode of Operation	Public Permissioned	Public Permissioned	Private Permissioned
Currency	Ether	BTC	None
Off-Chain Data Storage	Yes	No	No
Programmable Module	Smart Contract	None	Docker Container



BLOCKCHAIN LIMITATIONS IN HEALTHCARE SUPPLY CHAINS :

Although the proposed system leverages prominent benefits of blockchain technology, there are number of potential limitations which should be highlighted to aid deeper understanding of their potential impact on the proposed system. We present a discussion of such potential limitations of blockchain in healthcare supply chains below.

- **Immutability:** Blockchains are immutable where any information appended to the ledger cannot be altered or removed. While this can be beneficial for data integrity, it presents a major challenge, there is no way to correct inaccuracies on a blockchain because they are immutable. For example, the operators conducting the physical tasks in the drug supply chain can still make errors when recording information to the ledger. Consequently, these errors cannot be corrected even if it's detected. In a healthcare supply chain, this can have unwanted consequences. For example, if the manufacturer inserts wrong details of a drug Lot, it can cause issues later on when it reaches the pharmacy where a pharmacist might incorrectly prescribe a drug to a patient.
- **Data Privacy:** Although immutability is considered one of the main advantages of blockchains, it can be in conflict with emerging laws that address information storage issues. For example, the General Data Protection Regulation (GDPR) in Europe requires that organizations accurately control where and how data is stored because the person it is collected from have the right to modify or delete it any time, and if actions are not taken according to their requests, the organization can be liable to heavy fines [50]. In healthcare supply chains, patients might refuse to have their data stored permanently on the blockchain and they can legally sue the healthcare center.
- **Scalability:** Blockchain requires individual nodes to process every transaction on the entire network which provides security and verifiability to the system, but it limits scalability. However, there is active research to address this challenge. For instance, Sharding and Plasma are two scaling solutions for Ethereum that would eliminate the need for every Ethereum node to process every transaction on the network [51]. In healthcare supply chains, this might not be an issue if the manufacturing is done for small to moderate quantities. However, if a drug is being manufactured in large scale, the process will be difficult and very slow
- **Interoperability**: Blockchain networks other than Ethereum work in their own unique way which leads to interoperability issues where the different blockchains are not able to communicate with each other. If a unified blockchain-based solution is used among healthcare centers, this problem can be avoided. However, if healthcare centers decide to use different blockchainbased solutions with different platforms, it will be very difficult to make them interoperable.
- **Efficiency:** The efficiency of the blockchain solution is highly dependent on the coding of the smart contract and also the consensus algorithm used to verify and confirm a transaction.

The former determines how costly the implementation and execution process will be, and the latter determines the energy consumption level. The healthcare supply chain involves many transactions, therefore it’s very important for the smart contract to be coded properly so that it executes quickly and efficiently.

Drug traceability flow with Hyperledger Fabric

In this section, we describe how transactions in the pharmaceutical supply chain are executed and communicated between different stakeholders using the execute-order-validate transaction processing methodology typical for Hyperledger Fabric. This is shown in Figure 2 The steps taken to complete a transaction processing cycle in this architecture are described in detail and numbered below.

Figure 2. Hyperledger Fabric blockchain architecture.

In the proposed Hyperledger Fabric architecture, initially, an organizational user (client app) from a registered organization such as supplier or manufacturer, submits a transaction proposal (Step 1).

The transaction proposal is a request to invoke a chaincode function with certain parameters, with the intent of reading and/or updating the ledger (Step 2).

This proposal is submitted to all endorsing peers, as determined by the chaincode endorsement policy (Step 3). To clarify, for every chaincode there is an endorsement policy stating which organizations, and by extent which peers, must sign/check every transaction for that chaincode.

The transaction proposal consists of different parameters such as client’s cryptographic credentials (obtained from an MSP), the transaction payload including the name of the chaincode function to be executed with input arguments, and the channel and chaincode identifiers. The client app sends this proposal to a set of endorsing peers to get a consensus that the transaction is valid. This phase is called the *proposal phase*.

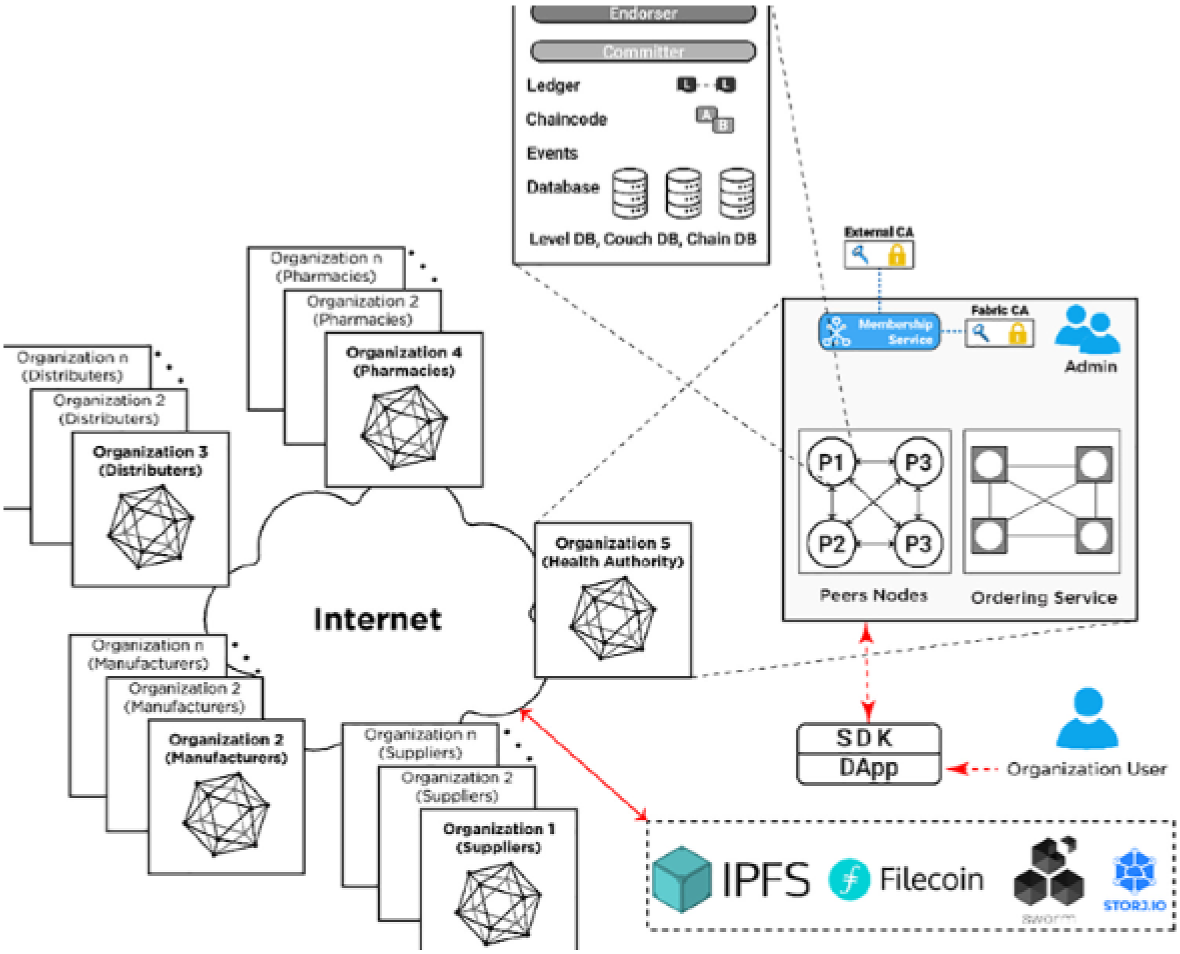
In the proposed Hyperledger Fabric architecture, initially, an organizational user (client app) from a registered organization such as supplier or manufacturer, submits a transaction proposal (Step 1).

The transaction proposal is a request to invoke a chaincode function with certain parameters, with the intent of reading and/or updating the ledger (Step 2).

This proposal is submitted to all endorsing peers, as determined by the chaincode endorsement policy (Step 3). To clarify, for every chaincode there is an endorsement policy sting which organizations, and by extent which peers, must sign/check every transaction for that chaincode.

The transaction proposal consists of different parameters such as client’s cryptographic credentials (obtained from an MSP), the transaction payload including the name of the chaincode function to be executed with input arguments, and the channel and chaincode identifiers.

- The client app sends this proposal to a set of endorsing peers to get a consensus that the transaction is valid. This phase is called the *proposal phase*.



Hyperledger Besu architecture

The proposed Hyperledger Besu drug traceability architecture provides a fully compatible open-source distributed ledger solution for enterprises looking for Ethereum-compatible blockchain architectures. Hyperledger Besu is gaining popularity among enterprises as it supports building networks supporting both private transaction processing and integration with public blockchains (Ethereum), while maintaining architectural flexibility and high transaction throughput. The proposed Hyperledger Besu architecture bridges the gap between private and public blockchains and helps pharmaceutical supply chain organizations to build scalable, high-performance applications on peer-to-peer private networks that fully support data privacy and complex permissioning management. Hyperledger Besu supports business logic through Solidity smart contracts, and can take advantage of using ERC20 tokens and Ether cryptocurrency.

Hyperledger Besu is an open-source Ethereum client. It provides a simple JSON-RPC API for running and managing Hyperledger Besu nodes and executing transactions. The proposed Hyperledger Besu architecture supports storing both private and public drug transaction execution information, which is required to implement an efficient drug traceability across the pharmaceutical supply chain between different stakeholders. The core components of Hyperledger Besu architecture, as shown in , are Ethereum Virtual Machines (EVMs), EtherSign, and Orion nodes. Although it is revolving around a public blockchain, privacy, and permissioning are the two key features of Hyperledger Besu architecture. To create a permissioned private blockchain for the pharmaceutical supply chain, Hyperledger Besu allows creating specific organizations (stakeholders) and their users (nodes) with their associated network accounts (wallets/addresses). Hyperledger Besu uses the inherent Public Key Infrastructure (nodes are issued a private/public key pair) to sign and verify transactions, and the node's address as a unique identifier for the node. To separate business logic from key storage/management procedures, EthSigner is recommended be used in combination with Hyperledger Besu as an external wallet service provider.[36] Upon receiving a transaction, EthSigner will generate a signature using the stored private key, then forward the transaction with the fully valid signature to the Ethereum client for inclusion to the blockchain.