PROJECT DESIGN PHASE

Solution Architecture

Team Id	NM2023TMID01494
Project Name	Project- Drug Traceability

Introduction:

- Counterfeit medications contribute to major public health concern that severely impact human lives and treatment outcomes.
- The World Health Organization (WHO) defines counterfeit medications as products that are deliberately and fraudulently mislabeled with respect to source and/or identity. Counterfeit drugs can contain insufficient, incorrect, erroneous ingredients, falsified information such as wrong labeling, and packaged incorrectly.
- WHO estimates that one out of ten medicines circulating in developing countries are either substandard or falsified, and approximately 1%–2% of all the drugs consumed are counterfeit in the developed nations.
- The global counterfeit drug trade impacts all pharmaceutical stakeholders including hospitals, pharmacies, wholesale distributors, global health programs, and regulatory authorities
- Drug supply chain security act (DSCSA) requires all supply chain stakeholders to implement reliable measures that improve product traceability, the actual implementation of DSCSA will be in a phased manner by the year 2023.
- Blockchain technology is a decentralized, distributed ledger system that provides an efficient and trusted solution for product traceability.
- Blockchain technology powers the crypto currencies and has been applied to variety of industries such as banking, supply chain, energy, commodities trading, healthcare and many businesses involving transaction processing.
- To deal with the issue of counterfeit drugs, blockchain technology has the potential to provide pragmatic solution for drug traceability and provenance in a secure and immutable manner.
- Blockchain technology enables the creation of a distributed shared data platform for storing and sharing the transaction data among various supply chain stakeholders ensuring the information remains accessible, immutable, transparent and secure via cryptographic techniques and accessible only to authorized parties.
- Thus, provides a proactive approach to track, detect, and manage counterfeits in pharmaceutical supply chains.

Drug traceability in healthcare:

- A pharmaceutical supply chain follows an end-to-end process from sourcing the active medication ingredients (source) to manufacturing the final product (medication) distributed and delivered to patients (end-users).
- It is the primary responsibility of the supply chain members to distribute authentic and high-quality products at the right time as it directly influences the health and safety of patients.
- The current drug distribution, and delivery systems have grown immensely in scale and complexity.
- In addition, limited data visibility, lack clear ownership structure, diversity of stakeholders makes transaction verification difficult.
- The lack of an integrated view of the entire supply chain often requires centralized third-party solutions to collect and validate information.
- Pharmaceutical supply chain comprises of several stakeholders (supplier, manufacturer, distributor, retailer, pharmacy, and patient), and product distribution often requires intricate packing, unpacking and repacking process, which makes drug provenance and traceability very complicated.

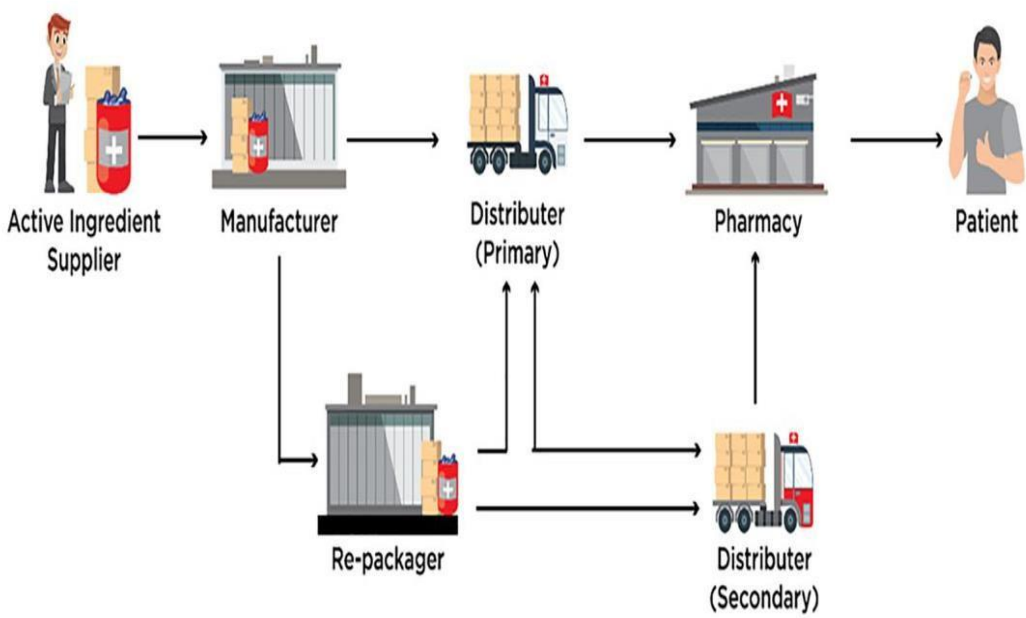

Figure 1. Drug supply chain stakeholders and their relationship

- Blockchain solutions for supply chain and logistics have recently gained enormous acceptance as they provide an immutable and transparent way to record transactions between non-trusting stakeholders.
- The main feature of blockchain technology is the ability to track and trace transactions of an asset using decentralized distributed ledger with cryptographically secured timestamped records, thus enabling the direct digital transfer and storage of transaction records without the involvement of third-party intermediary service providers.

- It enables us to create an immutable ledger for transaction processing among untrusted and physically distributed stakeholders across the pharmaceutical supply chain.
- Blockchain technology has the potential to be integrated with existing anti-counterfeiting solutions including RFID, NFC, QRC, and e-pedigree to provide interoperable and better-integrated solutions.

The wider acceptance of blockchain based solutions in the pharmaceutical industry is evident based on several recent pilot projects involving major stakeholders is shown in table 1.

Table 1. Blockchain based drug traceability pilots.

Product and pilot participants	Type of solution	Platform
IBM, KPMG, Merck, Walmart	Blockchain approach for track and trace	Hyperledger
IDLogiq	Blockchain based authenticated intelligent medication management	Private platform
MediLedger—Amerisource Bergen, McKesson, and drug manufacturers Genentech, Pfizer, Gilead	Blockchain based product verification system for salable returns	Permissioned Enterprise Ethereum
TraceLink—over 22 participants including manufacturers, wholesalers, distributors	Digital recalls and interoperable blockchain network solutions	Hyperledger
Indiana university health and Wakemed health and hospitals	Blockchain based solution to track specialty medicines within and outside the providers network	Private platform
LedgerDomain—University of California Los Angles health	Blockchain based solution for counterfeit detection	Hyperledger
SAP Multichain—Merck, Amerisource Bergen, GSK, Amgen, Boehringer Ingelheim, McKesson, Novo Nordisk	Blockchain based verification of counterfeits and tracking of salable returns	Multichain

Blockchain based architectures for drug traceability:

- In this section, we present and discuss two blockchain-based architectures to fulfil important requirements for drug traceability.

- The proposed architectures are based on two blockchain platforms namely, Hyperledger Fabric and Hyperledger Besu as they provide higher degree of trust, decentralization, transparency, privacy, security, data integrity, deployment, modularity and scalability when compared to other blockchain platforms such as Ethereum, Quorum, BigChain, etc.
- These architectures can be key enablers for creating private permissioned blockchain ecosystems where pharmaceutical stakeholders and their end-users are registered, controlled, and regulated by a regulating authority or a group of authorities/stakeholders.
- The two proposed architectures and their respective transaction flows are described in the following subsections, followed by in-depth technical comparison.
- Hyperledger Fabric is a platform providing distributed ledger solutions, underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability.
- It is an enterprise grade DLT based on blockchain technology that uses smart contracts to enforce trust between multiple parties.

Hyperledger Fabric architecture:

- Hyperledger Fabric eliminates the concept of mining, but still keeps the good properties of a typical cryptocurrency blockchain (such as Bitcoin, Ethereum) like: block immutability, order of events determinism, prevention of double spending, etc.
- Hyperledger Fabric has been confirmed to offer superior transaction throughput, up to several thousand transactions per second.
- These characteristics, among other that will be described below, make Hyperledger Fabric a perfectly suitable candidate for complex supply chain systems with multiple physical and logical processes and parties.
- By using general purpose programing languages (Java, Go, NodeJS) to develop smart contracts, the adoption bar for this technology is lower than for others using dedicated programing languages (e.g. Solidity in Ethereum).
- The proposed blockchain architecture introduces a new modular approach to provide high levels of flexibility, resiliency, scalability, and privacy.

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 Figure2 The steps taken to complete a transaction processing cycle in this architecture are described in detail and numbered below.

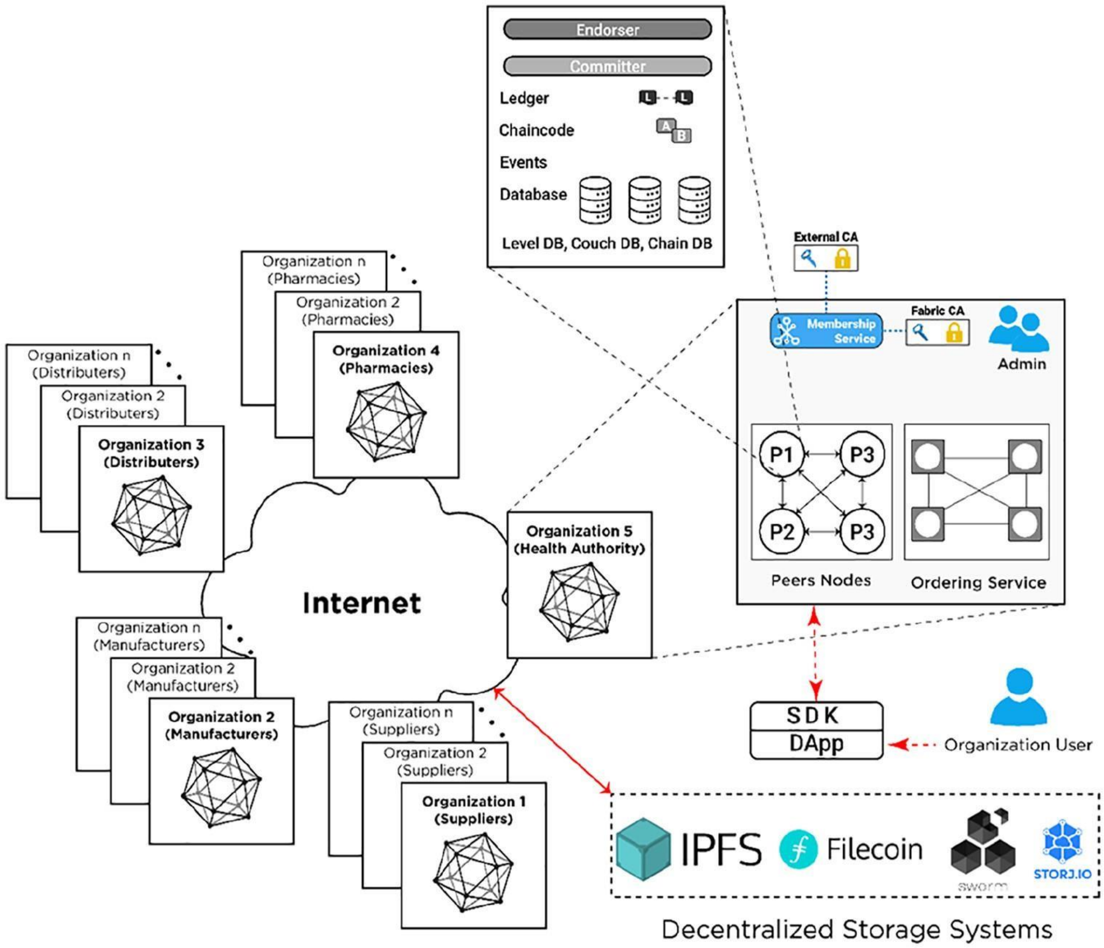

Figure 2. Hyperledger Fabric blockchain architecture.

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 Figure 3.are Ethereum Virtual Machines (EVMs), EtherSign, and Orion nodes.

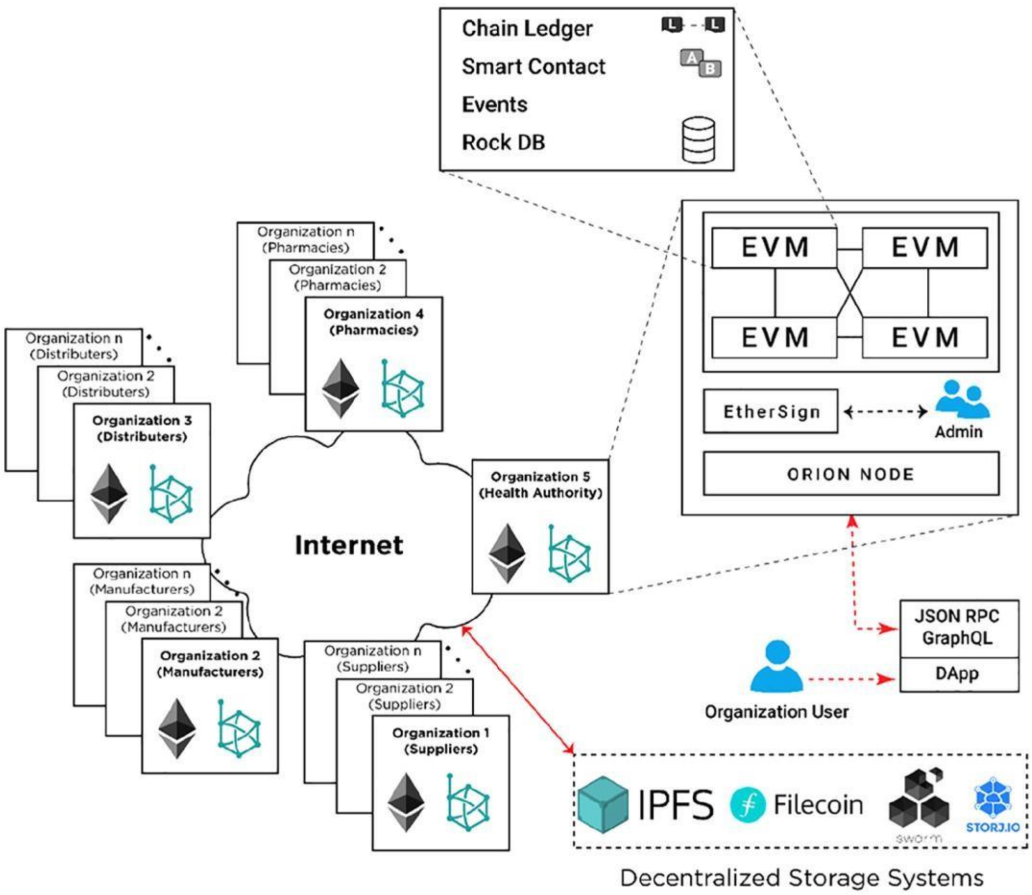

Figure 3. Hyperledger Besu blockchain architecture.

Drug traceability flow with Hyperledger Besu:

- In this section, we describe how medication-related traceability transactions are executed and communicated between different stakeholders on a Hyperledger Besu network.
- In the proposed Hyperledger Besu architecture, when an organizational user (client) wants to perform a transaction (execute a specific smart contract function or transfer (assets), it initially submits a signed private transaction request through a Distributed

- App (DApp) to a Hyperledger Besu EVM node (Step 1). The signed transaction includes the list of recipients' addresses or privacy group ID, sender address, type of transaction (e.g. restricted), etc.
- To clarify, a privacy group is a group of nodes identified by a unique privacy group ID by Orion. Orion stores each private transaction with the privacy group ID.
- The Hyperledger Besu nodes maintain the public world state for the blockchain and a private state for each privacy group. The private states contain data that is not shared in the globally replicated world state. Privacy groups enable access to certain data only to a group of accounts/nodes.
- The DApp user interface uses JSON-RPC to send transactions to Orion (Step 2) through the Private Transaction Handler (PTH). Orion distributes the transactions to other Orion nodes specified by the privacy group ID or recipient addresses (Step 3).
- After receiving the transactions, Orion nodes will store them in the state database, and return the transaction hash value to the PTH (Step 4).
- Alongside private transactions, the PTM creates Privacy Marker Transactions (PMT) which are also mined into blocks and broadcasted (Step 5).
- The Mainnet Transaction Processor on every Hyperledger Besu node will process PMT, and on nodes that contain the corresponding private precompiled smart contract, the transactions are passed to the contract for execution (Step 6).

Technical comparison: Ethereum, Hyperledger Fabric and Hyperledger Besu:

Category	Sub-category	Hyperledger Fabric	Hyperledger Besu	Ethereum
General	Governing bodies	Originally contributed by IBM and Digital. Now governed by Linux Foundation	Originally contributed by ConsenSys (PegaSys). Now governed by Linux Foundation	Ethereum Enterprise Alliance
	Maturity	Announced 2017, ~60 version improvements, high-level maturity	Announced 2019, ~30 version improvements, middle-level maturity	Announced 2015, ~100 Geth client releases, nine hard forks, high-level maturity
	Intended manner of usage	Private, permissioned	Semi-private	Public
	Community of contributors	~200	~60	~450
	Cryptography	Pluggable (ECDSA with secp256r1 and secp384r1 built-in)	secp256k1	secp256k1
		256MB RAM per CouchDB		
		512MB RAM per chaincode container		
		256MB RAM per Ordering Service node (RAFT)		
	Storage options	LevelDBCouchDB	File storage	File storage
Transaction Execution	Transaction consensus	Unique Execute-Order-Validate methodology. Tolerating, instead of eliminating non-determinism	Order-Execute methodology. Every transaction execution must be deterministic	Order-Execute methodology. Every transaction execution must be deterministic
	Applied consensus protocols	Kafka/Raft (Crash Fault Tolerance with trusted leader)	Clique and IBFT 2.0 Proof of Authority (Byzantine Fault Tolerance)	Ethash Proof of Work (Byzantine Fault Tolerance)
	Cost/Fee	Only network running costs exist	Fee is paid in Ether for smart contract deployment or transaction execution. Cost different for different networks Besu nodes are integrated with (public Ethereum, Ropsten, etc.)	Fee is paid in Ether. Higher fee indicates faster mining/confirmation time. $2.71 per transaction for September 24th, 2020

Secure communication	TLS support	Yes	Yes	Yes
Identity and privacy	Data privacy	Private data collections	Privacy groups that can access private transactions	No support
	User and Node Permissioning	Organization level: channels	On-chain through smart contract	No support
		Chaincode level: function caller certificate/MSP attributes	Of-chain through configuration files	
	Identity generation and management	Based on PKI. Organizational identity rather than individual identities used in consensus and permissioning. Management through Certificate Authority Or third party certificate provider	Public keys—distributed, and interoperable between Ethereum based chains. Coupled to PKI via proofs	Public keys—distributed, and interoperable between Ethereum based chains. Coupled to PKI via proofs
Business logic implementation complexity	Client application responsibility	Coordinating with other participants to obtain endorsement, managing optimistic concurrency locking on state, signature, and submission	Sending signed transactions to a single node in the network	Sending signed transactions to a single node in the network
	Smart contract execution engine	Isolated inside Docker container	EVM (sandbox)	EVM (sandbox)
	Smart contract languages	General purpose: Java, Go, NodeJS. Non-determinism is tolerated	Domain specific (Solidity), guaranteed deterministic. Frameworks: Truffle, Embark, OpenZeppelin, etc.	Domain specific (Solidity, Viper), guaranteed deterministic. Frameworks: Truffle, Embark, OpenZeppelin, etc.
	Smart contract lifecycle	Requires installation on peers, instantiation in coordination with Ordering Service. Stored off-chain	Immutable, easy to deploy, and stored on-chain	Immutable, easy to deploy, and stored on-chain
	Smart contract upgrade	Replacing code via an upgrade transaction (versioning), similar to initial contract deployment	Programing schemes to extend/migrate code and data	Programing schemes to extend/migrate code and data
	Tokenization of digital assets	No native support. FabToken token management system in Hyperledger Fabric 2.0	Native feature with several token standards (ERC20, ERC721, ERC777 etc.)	Native feature with several token standards (ERC20, ERC721, ERC777 etc.)
Integration with Third party services	Services interaction	Service interacts with an SDK (NodeJS, Java, Python, Golang)	Distributed Apps (DApps) interact with nodes. JSON-RPC over HTTP or WebSockets	Distributed Apps (DApps) interact with nodes. Web3.js Ethereum JavaScript API. HTTP or IPC connection

Table 2. Comparison of Blockchain Platforms.

- Compared to Ethereum, both Hyperledger Fabric and Besu are aimed to be used as private, permissioned Business-2-Business networks.
- Ethereum is rather Business-2-Customer oriented, with no inherent support for privacy groups or private data/transactions.
- Hyperledger Fabric and Besu support faster state reconciliation and offer superior transaction execution speed.
- Smart contracts in Hyperledger Fabric might be easier to develop since they use general-purpose programing languages, as opposed to Besu and Ethereum that use a domain-specific language.
- However, Hyperledger Fabric lacks a proper smart contract development framework that is available in both Besu and Ethereum (e.g. Truffle). Network configuration, setup, and deployment complexities are higher for Hyperledger Fabric, however it is easy to manage/update/upgrade since all components are Dockerized.
- Using Hyperledger Fabric also comes with increased client application responsibility, but increases the amount of control on the client side. Hyperledger Fabric is superior to both Besu and Ethereum for identity management and access control by having both physical (channels)

and logical (chaincodes, certificate attributes) enablers to manage them. For the pharmaceutical traceability application both Hyperledger Fabric and Besu provide the best alternatives and features for effective trace and trace solution.

Open challenges:

In this section, we briefly outline notable challenges in adopting blockchain based provenance, track and trace solutions in the pharmaceutical industry.

Stakeholder agreement:

- A blockchain network is a distributed ledger where all pharmaceutical supply chain stakeholders store their core business data and everyone has access to this sensitive private data on the platform. Potential stakeholders might be reluctant to participate in such networks since it could lead to losing their competitive advantage, especially when multiple business competitors exist in the same supply chain.

Interoperability:

- Interoperability is defined as a mass adoption of business software and platforms across multiple organizations to provide efficient integration strategies.
- It serves as a means for users of different platforms and software's to interact and conduct meaningful businesses seamlessly.
- The existing drug traceability solutions such as serialization, bar codes, RFID tags, and e-pedigree as well as blockchain-based solutions and platforms lack full interoperability as there are no standardized solutions to make integration, adaptability and implementation easier.
- Further, different blockchain platforms under the Hyperledger umbrella are coping with issues to provide interoperability, ensure maximum scalability and adaptability for enabling internal and external communication between business organizations.

Implementation cost:

- Designing the perfect blockchain application is not an easy task, since majority of the existing solutions are under development.
- The privacy, scalability, and interoperability challenges also contribute severely toward this issue. Implementation and energy costs are one of the leading challenges faced by majority of enterprises, including the pharmaceutical supply chain.
- The existing platforms and legacy software systems are inefficient and centralized when executing transactions, causing enormous implementation and maintenance costs.
- For example, Hyperledger Fabric can execute more than 3500 transactions per second and its power consumption is significantly reduced compared to Ethereum, due to different consensus protocols.

Attacks and vulnerabilities:

- One of the greatest advantages and selling points of blockchain technology is its resilience against various types of attacks, including cyberattacks.
- A recent cybersecurity report highlights several security risks, such as bad actors and man in the middle attacks, being involved in the blockchain network and exposing the vulnerabilities of the network.

- The current blockchain implementations are leaving inherent vulnerabilities and bugs due to the development of immature processes and systems. Phishing scams, technology vulnerabilities, implementation exploits, and malware, due to lack of standards and procedures, present serious challenges to be addressed in moving forward.

Lack of standardized regulations:

- The role of drug regulatory authorities includes quality checks and monitor the quality, safety, and efficacy and post market surveillance of pharmaceutical products..
- For instance, when a new transaction is executed in the network, it is difficult for these authorities to clearly define the jurisdiction and correct legal obligations of the stakeholders involved.
- Another challenge is to cope with the requirements of upcoming legislations such as FDA DSCSA, sterilization, and GDPR in blockchain networks. Therefore, blockchain technology is still incompatible with recent laws and regulations regarding the pharmaceutical supply chain.

Conclusions:

- ➢ Blockchain technology can be leveraged for drug traceability application in the pharmaceutical supply chain.
- ➢ We proposed two blockchain architectures based on Hyperledger Fabric and Hyperledger Besu. Such architectures provide a shared, trusted, permissioned and decentralized platform for storage and communications among different pharmaceutical supply chain stakeholders, and in a manner that can fulfill key requirements and features that include security, privacy, accessibility, transparency, and scalability.
- ➢ We present a comparison of the two platforms, and outlined a number of implementation challenges that hinder the wide spread adoption of blockchain technology for effective drug traceability.
- ➢ As future work, we plan to develop smart contracts, deploy the overall system components, and build user interface DApps of the proposed architectures.