

DRUG TRACEABILITY USING BLOCKCHAIN

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 mis-labeled 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.³ The Illegal drug market contributes immensely toward producing fake and fraudulent medicines as its actors add contaminated, improperly stored, and falsified ingredients. This is enabled because there is a lack of technical and business solutions that offer adequate traceability and provenance solution. For example, a substandard version of the anti-cancer drug Avastin was purchased and delivered to thousands of cancer patients in the U.S causing potential treatment complications for patients. The Asia Pacific, African, and Latin American regions are most vulnerable to counterfeit drugs with almost 30% of the drugs produced and consumed are counterfeit leading to almost 1.5 million deaths per year. In the European region the number of reported cases of counterfeit drugs have doubled compared to previous years. A recent report by a prominent European research project highlights that the counterfeit medication industry is considered more lucrative and profitable business than selling legal medicines and it estimates a revenue loss equals almost 4.5% in drug sales amounting to €10 billion every year. The increased access to medications via online pharmacies and unauthorized distribution channels makes it difficult to ensure product safety in the supply chain. In addition, limited data visibility about inventory and stock levels across the supply chain presents greater opportunities for counterfeits to enter the

market. Drug traceability is the process of identifying the originality and legitimacy of the product that enables all stakeholders to track and trace the transactions at every stage in the supply chain. Regulations such as the US 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. In this paper, we reflect on the potential and the limitations of blockchain technology for drug traceability. We describe the current blockchain enabled trends and describe two state of the art architectures, provide explanations on how these architectures are robust, secure, and scalable to provide better transaction privacy compared to existing solutions, and discuss potential opportunities for securing the pharmaceutical supply chain. The major contributions of our work are as follows: Uddin et al.

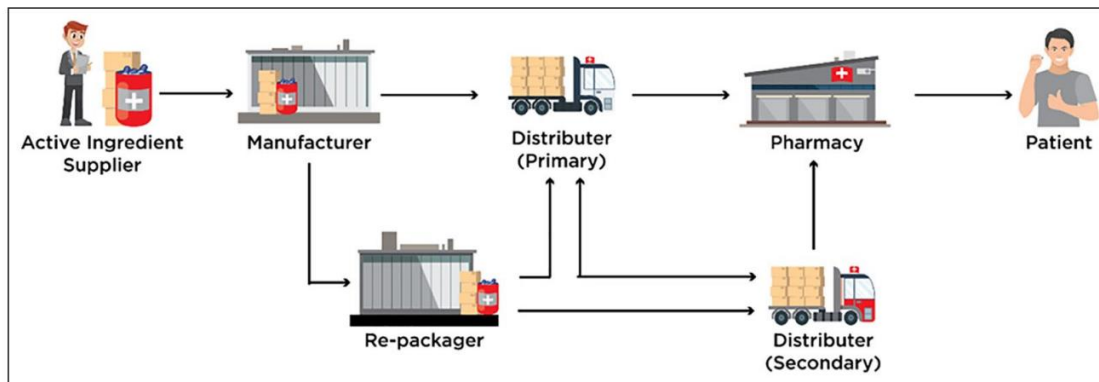
- We discuss the reasons how the pharmaceutical supply chain benefits from a blockchain enabled drug traceability solution.
- We highlight the key benefits of using blockchain solution for drug supply chain compared to existing solutions.
- We present two suitable blockchain architectures for drug traceability, Hyperledger Fabric and Besu private blockchains.
- We identify, enumerate, and discuss several future research challenges that may hinder the successful deployment of blockchain solutions in the drug supply chain.

Overview of drug traceability in healthcare

We highlight potential issues related to drug traceability in the pharmaceutical supply chain with an emphasis on counterfeit drugs. 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. a high-level overview of various stakeholders and their relationship in the pharmaceutical supply chain. There are several factors attributed to the availability of counterfeits in the supply chain, some examples include importing substandard medicines without the approval of regulatory authority, poor manufacturing and storage practices, theft, and infiltration of deficient drugs. Different technology driven approaches such as bar codes, RFID tags, IoT, serialization, and e-pedigree have been adopted to enhance trust among stakeholders to improve product visibility in the supply chains. these solutions are centralized and have serious limitations when it comes to security, interoperability, privacy, and scalability toward preventing counterfeits in the supply chains. 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 ensures an efficient and cost-effective solution that underpins different drug traceability functions and procedures to ascertain proper.

LITERATURE SURVEY



Related Work

We present a critical overview of existing efforts focused at addressing the issue of product traceability in the healthcare supply chain emphasizing solutions proposed for anti-counterfeiting. We have included both blockchain and non-blockchain-based approaches and categorized them accordingly.

Traditional Efforts for Drug Traceability

Traceability is defined as the ability to access any or all information relating to the object under consideration, throughout its life cycle, by means of recorded identifications. The object under consideration is referred to as Traceable Resource Unit (TRU) which is any traceable object within the supply chain. Traceability objectives are twofold; to track the history of transactions, and to track the real-time position of the TRU. In this context, a traceability system requires access to information related to the drug which is the TRU in the supply chain by using different identification techniques to record its identity and distinguish it from other TRUs. The components of a traceability system can be broadly identified by a

mechanism for identifying TRUs, a mechanism for documenting the connections between TRUs, and a mechanism for recording the attributes of the TRUs.

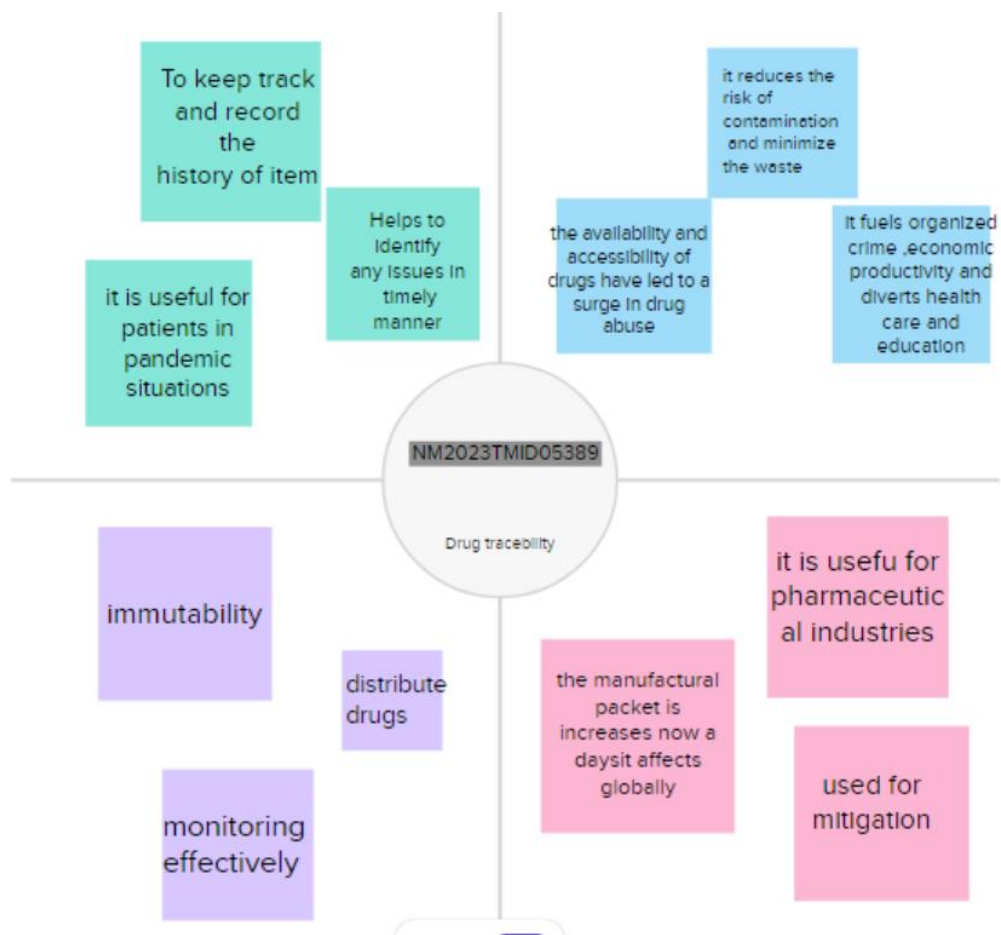
Existing solutions within supply chain management have traditionally used barcodes and RFID tags as identification techniques, Wireless Sensor Networks (WSN) to capture data, and Electronic Product Code (EPC) to identify, capture, and share product information to facilitate tracking of goods through different stages. In this context, Smart-Track utilizes GS1 standards barcodes containing unique serialized product identifier, Lot production and expiration dates. The information contained in the GS1 barcode is captured across various supply chain processes and used to maintain a continuous log of ownership transfers. As each stakeholder records the possession of the product, an end user (patient) can verify authenticity through central data repository maintained as Global Data Synchronization Network (GDSN) by using a smartphone app. In the downstream supply chain at the warehouse, pharmacy and hospital units can scan the barcode to verify the product and its characteristics. Similarly, Data-Matrix tracking system creates a Data-Matrix for each drug which includes the manufacturer ID, Product ID, Unique ID of the package, the authentication code, and an optional meta-data. This allows the patient to verify the origin of the drug by using the attached Data-Matrix.

More recently Near Field Communication (NFC) tags have been proposed to be used to achieve visibility and authenticity across pharmaceutical supply chain. In this respect, presents an effort to develop a NFC-based system which affords visibility throughout different stages of pharmaceutical supply chain. Each drug is registered and authenticated by using a key value and an NFC tag is attached to it. Similar to the previous two solutions, the user or the patient can verify the authenticity or the origin of the drug by scanning the attached NFC tag using a mobile application.

It have proposed solutions for traceability but they use a centralized database which makes tampering goods information relatively easy and difficult to detect. In addition to that, the use of different types of centralized databases can result in the proposed solutions to have lack of interoperability and scalability.

IDEATION & PROPOSED SOLUTION

Empathy Map Canvas



Ideation & Brainstorming



REQUIREMENT ANALYSIS

Security Analysis for the Blockchain-Based Healthcare Supply Chain

We discuss briefly the security analysis of the proposed blockchain-based solution for the healthcare supply chain where integrity, accountability, authorization, availability, and non-repudiation are considered as key security goals. Moreover, we discuss how our solution is resilient against common attacks including Man-In-The Middle (MITM) and Distributed Denial of Service (DDoS).

- Integrity:** The primary objective of the proposed blockchain solution is to keep track of all the transactions that occur within the healthcare supply chain ensuring traceability of the history of the Lots, ownership transfers and their corresponding boxes. This is ensured in the proposed solution because all events and logs are stored in the

immutable blockchain ledger. Moreover, the use of IPFS to store images of the manufactured Lots adds integrity to the proposed solution. This will ensure that every transaction within the healthcare supply chain can be tracked and traced.

- **Accountability:** As demonstrated in section V, each execution of a function has the Ethereum address of the caller stored on the blockchain which means tracing the function caller is always possible. Therefore, all the participants are accountable for their actions. In the healthcare supply chain, the manufacturer will be accountable for any drug Lot he produces using the *lot Details* function and pharmacies will be accountable for any prescription they give to a function because *buy Box* function will show where each patient is getting the drugs from
- **Authorization:** The critical functions in the smart contract can only be executed by authorised participants by using *the modifier*. This ensures protection against unprivileged access and prevention of any unwanted entities from using the implemented functions. This is very important for the healthcare supply chain because the manufacturing of the drug Lot should only be done by a verified manufacturer and the prescription of drugs should be only done by a verified pharmacy.
- **Availability:** Blockchains are decentralized and distributed by nature. Therefore, once the smart contract is deployed on the blockchain, all logs and transactions are accessible to all participants. Contrary to centralized approaches, the transaction data is stored at all participating nodes therefore loss of a node does not result in the loss of transaction data. The blockchain network needs to be up and running all the time for the application of healthcare supply chain to be successful. Any downtime might result in delays that are very costly in the healthcare industry.
- **Non-Repudiation:** As transactions are cryptographically signed by the private key of their initiators, cryptographic properties of PKI guarantee that private keys cannot be deduced from public keys. Therefore, a transaction signed by a specific private key can be

attributed to the owner of the key. This is similar to accountability where the participants of the blockchain-based healthcare supply chain cannot deny their actions since they are already signed by their private key which is associated with their real identity.

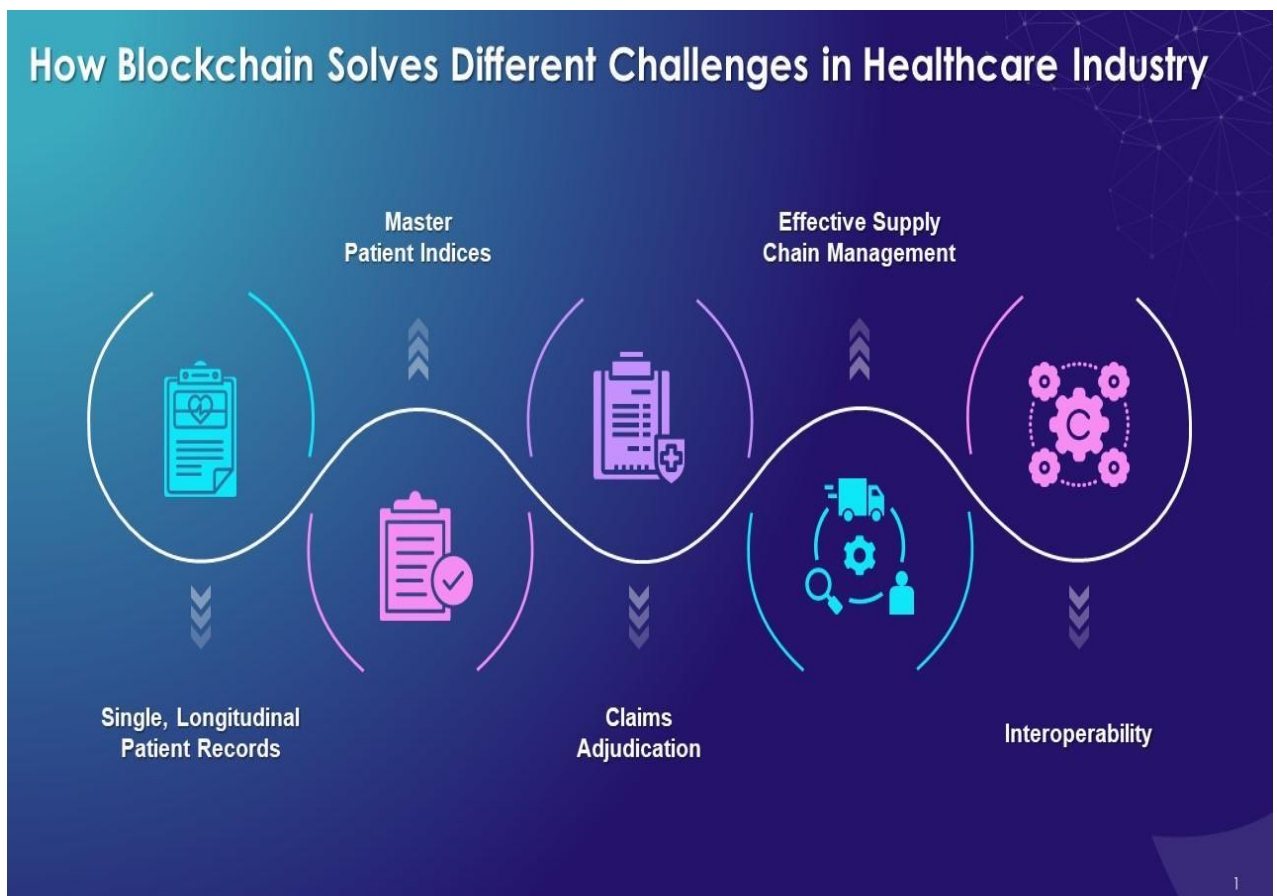
- **MITM Attacks:** Every transaction in the blockchain needs to be signed by its initiator's private key, and therefore if an intruder tries to modify any of the original data and information in the blockchain it will not be confirmed unless it gets signed by the initiator's private key. Therefore, MITM attacks are not possible in the blockchain environment. This feature is indispensable for the application of healthcare supply chain because it ensures that only the verified entities can perform actions within the supply chain, and intruders who illegally try to produce counterfeit drugs in the name of a verified manufacturer will no longer be able to do that.

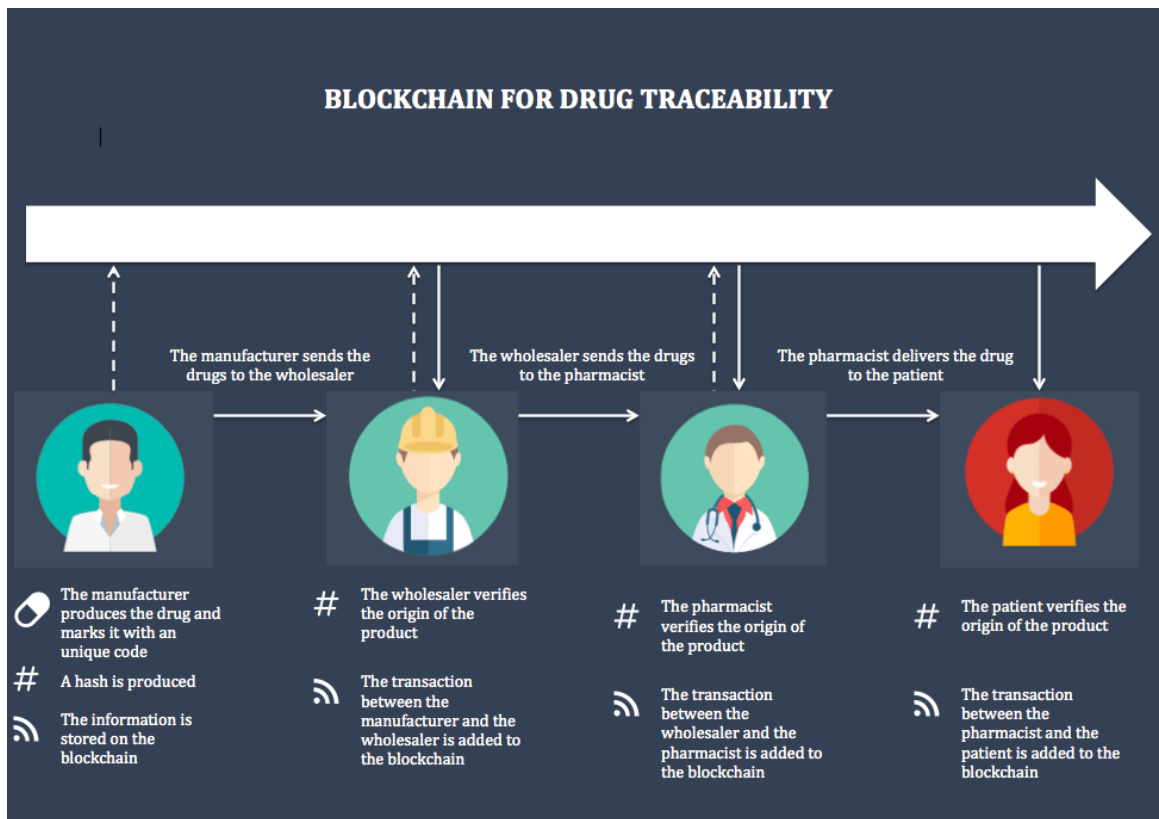
Smart Contract Security Analysis

The developed Ethereum smart contract for drug traceability was analyzed using specialized tools to reveal any code vulnerabilities in addition to the aforementioned security analysis. Those tools were used in code development iterations to improve the reliability of the smart contract. Remix IDE that was used to develop the smart contract provides some code debugging and run-time error warnings. However, they are not sufficient to establish trust in the smart contract robustness. Therefore, SmartCheck was used to detect vulnerabilities in the code at different severity levels. After multiple iterations of smart code modification, the smart code was bug-free as reported by the output. SmartCheck analyzed the smart contract comparing it to its knowledge base and verified that it was free from risks that would make it susceptible to exploitation and cyber-attacks. Oyente tool was also used to explore the smart contract security. Oyente runs on Linux and analyzes the code intensively to rule out any hidden vulnerabilities. It is designed to protect the Ethereum smart contract from known attacks such as callstack depth attack and re-entrancy attacks. After analyzing the smart contract, Oyente generates a result report the code coverage in addition to the availability of some crucial vulnerabilities that can be manipulated for malicious attacks.

PROJECT DESIGN

Data Flow Diagrams





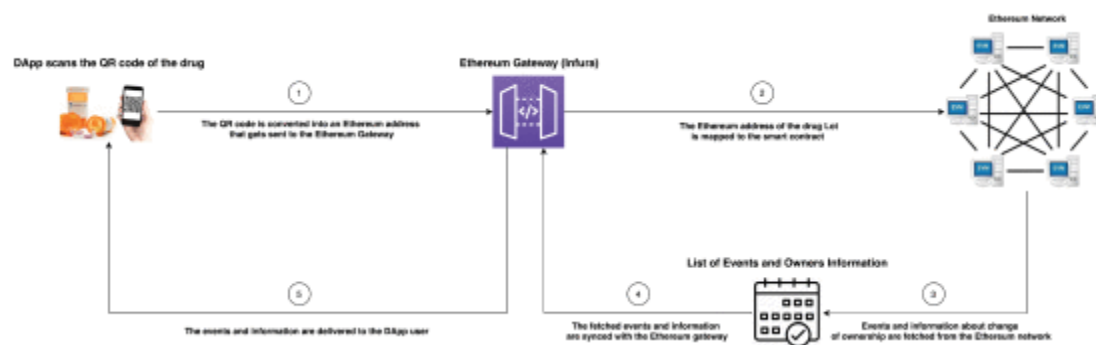
Solution Architecture

Traceability Analysis of the Proposed Solution

In this subsection, the different steps adopted to verify the authenticity of the drug Lot are illustrated. Every drug Lot is manufactured with a smart contract that is specifically designed for it and is responsible for triggering events and logging them on the ledger. A unique Ethereum address is generated for every drug Lot. However, copying Ethereum address of each drug is cumbersome, time consuming, and error prone process. Therefore, a QR code is used which can be easily scanned using smartphones. A QR code is a two-dimensional barcode that is readable by smartphones, and it can allow encoding over 4000 characters in a two-dimensional barcode. Mapping

an Ethereum address to a QR code can be done by using an Ethereum QR code generator in which the Ethereum address is passed and a unique QR code is generated which will exclusively map to that Ethereum address every time it gets scanned. Once the QR code gets attached to the drug Lot, it can be dispensed to patients.

the steps to verify the authenticity of a drug. The first step is scanning the QR code that is attached to the drug by using a DApp which interacts with the Ethereum node (local or remote node) through web3j. To map the QR code to its corresponding Ethereum address, the DApp has to interact with the Ethereum node (Infura for example) through JSON-RPC. The Ethereum node has a replica of the ledger, and it is extremely important for the users because it makes the process smooth and easy by saving them the effort of having to set up their own Ethereum node which takes a lot of time. The gateway (Ethereum node) will map the Ethereum address of the drug Lot to the smart contract which will point to the events of the different functions of the smart contract that are stored in the ledger.



The service user will be able to verify the origin of the drug Lot by utilizing the event filtering feature which is based on the smart contract Ethereum address and the event name. Event filtering allows the service user to access the various events which are already stored on the immutable ledger of the Ethereum blockchain from which the service user can confirm if the drug is

authentic or not. First, the service user can use the *lot-Sold* event to enter the pharmacy Ethereum address to verify the drug Lot was sold to the pharmacy legally. After that, the *lot-Sale* event can be used to fetch information about the drug Lot such as its name, number of boxes, and the price which allows the service user to verify that the pricing of the drug Lot is correct. Next, the *image-uploaded* event can be used to view the image of the manufactured Lot and boxes which shows if the product the service user receives matches the authentic one. Then, the *lot-Manufactured* event can be used to check if the Ethereum address of the manufacturer matches the original one. Finally, the *new-Owner* event is used to view the Ethereum address of the original owner of the smart contract to confirm its authenticity.

The Ethereum network presented the information is distributed among the participating nodes. Each node in the network will have a replica of the ledger that is immutable which will ensure that any information that is fetched from the ledger is authentic and there is no way it has been manipulated with. The requested events and information about change of ownership will be fetched from the Ethereum network and they will be synced with the Ethereum gateway (Infura), and once the syncing is done they will be transferred to the DApp and displayed to the user.

This application use case demonstrates the effectiveness of our proposed solution with respect to effective track and trace of drugs within a pharmaceutical supply chain. It achieves this by automating processes without requiring manual input from the user and utilizing different features of the Ethereum blockchain such as web3j, JSON-RPC, and Infura.

PROJECT PLANNING & SCHEDULING

Blockchain based architectures for drug traceability

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, Big-Chain, 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.

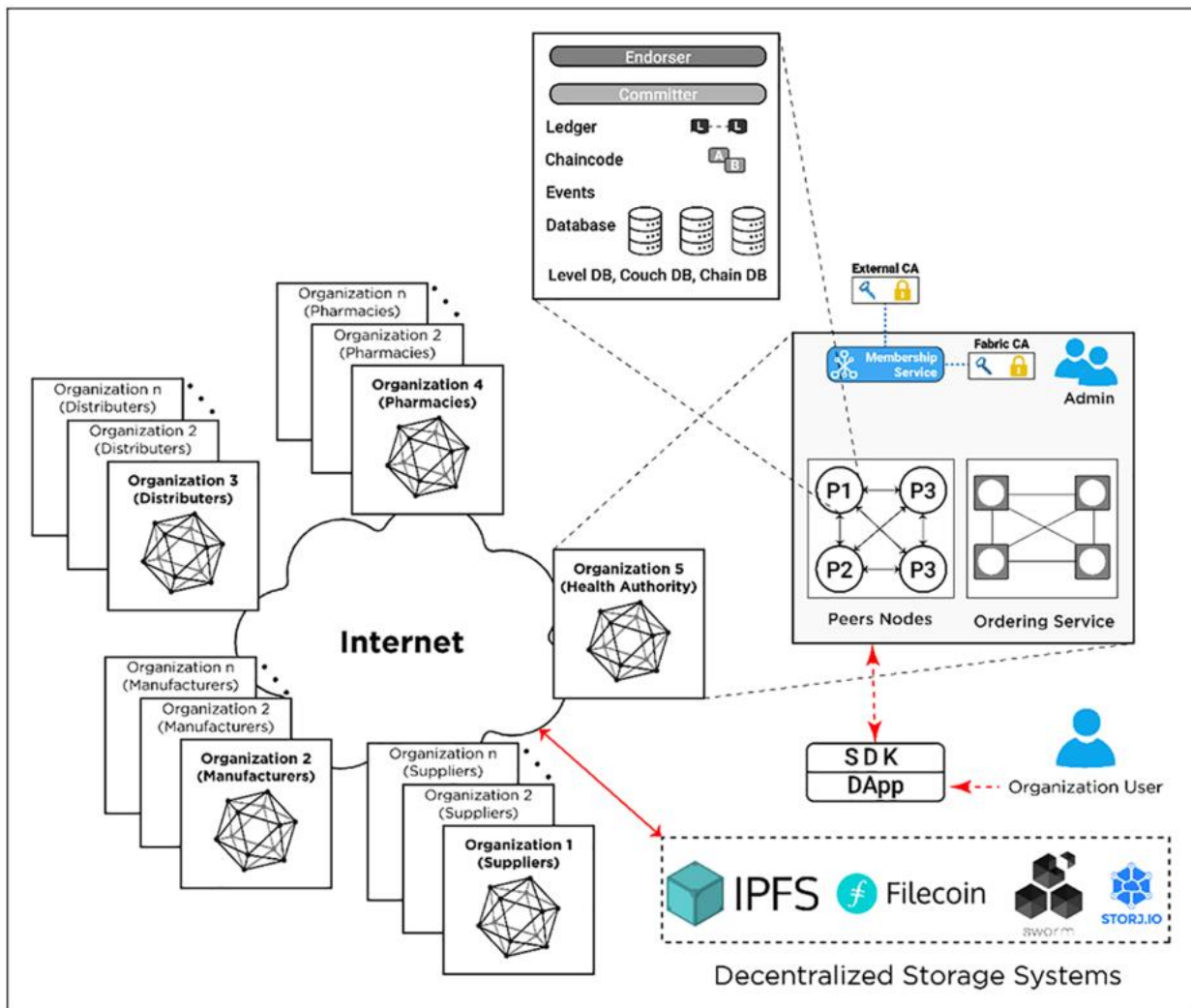
Hyperledger Fabric architecture

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 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 programming languages (Java, Go, NodeJS) to develop smart contracts, the adoption bar for this technology is lower than for others using dedicated programming languages (e.g. Solidity in Ethereum). The Hyperledger Fabric drug traceability architecture proposed in this paper provides an initial design of an enterprise-level blockchain-based supply chain system, where different stakeholders in the pharmaceutical supply chain are identified, their relationships established using different channels to provide maximum privacy, confidentiality, and data security. A concept of channels is unique to Hyperledger Fabric. Channels offer clear separation of business logic and data privacy policies between different stakeholders operating in the same system. By default, Hyperledger Fabric provides a secure and transparent crash –fault tolerant transaction ordering for ensuring deterministic recording of events, secure communication and reliable exchange of medication related transactions amongst a group of untrusted stakeholders. This helps to create a consistent track-and-trace provenance system to ward off counterfeit medications in

PSC. The proposed blockchain architecture introduces a new modular approach to provide high levels of flexibility, resiliency, scalability, and privacy. In the proposed Hyperledger Fabric architecture a permissioned private blockchain network is created where all the participating organizations (pharmaceutical stakeholders) and their end-users are identified and registered by the Health Authority using the membership service provider (MSP) component of Hyperledger Fabric. The MSP component is pluggable—it can be the Certificate 6 Health Informatics Journal 00(0) Authority (CA) offered by Hyperledger Fabric by default (local), or external (e.g. generate and use OpenSSL certificates, integrate with Active Directory, etc.). To create a trusted environment between untrusted participants, Hyperledger Fabric requires usage of an MSP (local or external) that creates rules and regulations by which different stakeholders (identities) are governed, authenticated, validated, and authorized to access blockchain resources. This ensures privacy and confidentiality of every stakeholder throughout the network and enables easy activity tracing (e.g. malicious transaction occurs). The MSP is a comprehensive novel design that revamps the process of non-determinism, resource exhaustion, and performance attacks in the participating stakeholders in the pharmaceutical supply chain by decentralizing identity management. Finally, at the core of the Hyperledger Fabric architecture there are Peer nodes (peers) and the Ordering Service (OS). Peers store ledger copies, execute smart contracts (also referred to as chain-code in Hyperledger Fabric), endorse, and commit transactions. The OS accepts the endorsed transactions from client applications, orders them into blocks with cryptographic signatures of the endorsing peers, and finally broadcasts these blocks to the committing peers in the blockchain network for validations against the endorsement policies. 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. The steps taken to complete a transaction processing cycle in this architecture are described in detail and numbered below. 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. The transaction proposal is a request to invoke a chain-code function with certain parameters, with the intent of reading and/or updating the ledger. This proposal is submitted to all

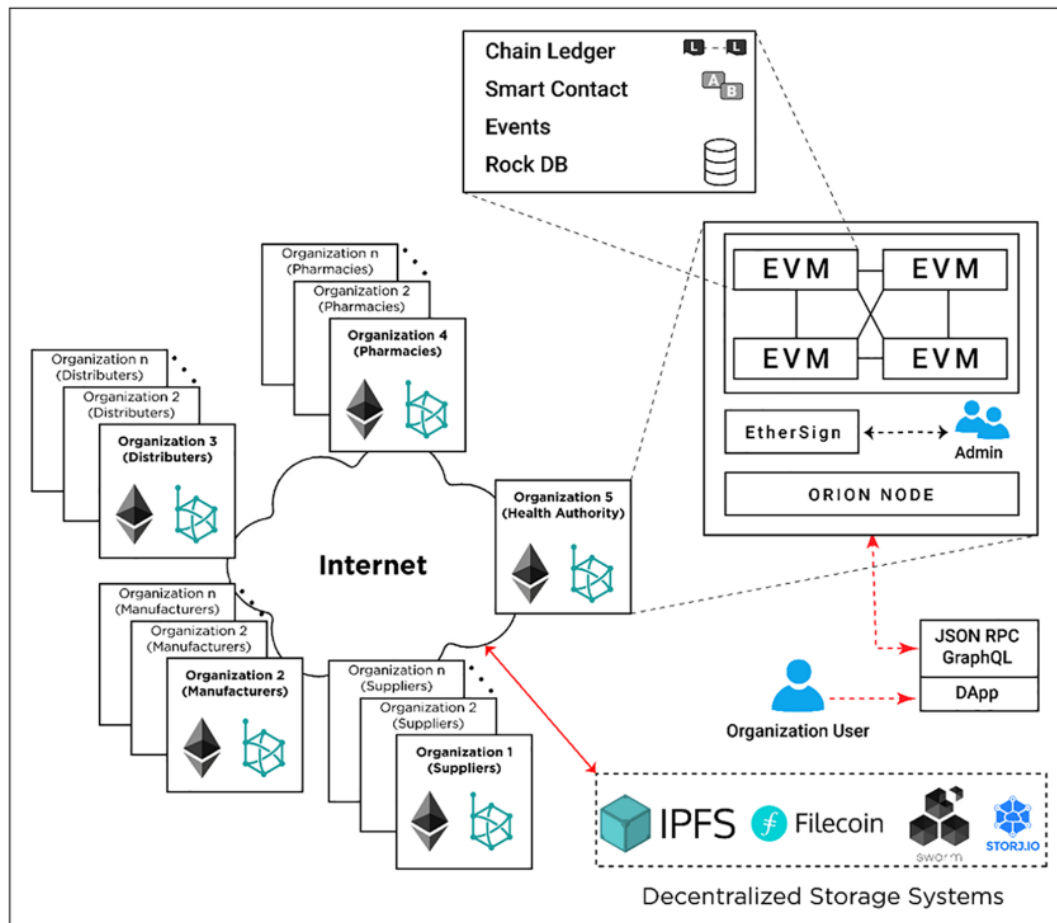
endorsing peers, as determined by the chain-code endorsement policy . To clarify, for every chain-code there is an endorsement policy stating which organizations, and by extent which peers, must sign/check every transaction for that chain-code. The transaction proposal consists of different parameters such as client's cryptographic credentials (obtained from an MSP), the transaction payload including the name of the chain-code function to be executed with input arguments, and the channel and chain-code 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. The transaction proposal is executed by a specific number of endorsing peers determined by the chain-code's endorsement policy . These results (also called endorsements), will be encrypted, and recorded along with endorsing peers' cryptographic signatures and RW sets (readset and writeset), and sent back to the client app, as a response to the transaction proposal submitted . It is important to highlight that the client app continues collect endorsements until it satisfies the chain-code's endorsement policy. No updates are made to the ledger at this point. This phase is called the endorsement phase. When the client app received enough endorsement responses, it inspects them to determine if RW sets are the same, making sure the chain-code ledger was not updated in-between proposal and endorsement phases (Step 6). Next, the client app assembles and broadcasts the transaction proposal and responses within a transaction message to the Ordering Service . This message contains a transaction with RW sets, endorsing peer signatures and channel identifier. The decentralized Ordering Service uses a pluggable consensus protocol to calculate and establish the execution order of all the submitted transactions per channel. Ordering service chronologically orders multiple drug transactions into blocks, chaining the blocks' hashes to previous blocks . This phase is called the ordering phase.

.



The final phase is the execution phase. The OS broadcasts the newly-formed blocks to the leading peers in the Hyperledger Fabric network. The leading peers are then in charge of dis-seminating the blocks to other committing peers within the organization using gossip protocol. Leading peers are elected per organization and they are known to the Ordering Service. Peers check if the endorsements are valid according to the chain-codes' endorsement policies' and verify that the RW sets have not been violated since last checked. If any endorsement is invalid or the RW sets do not match the current world state, the transaction is marked as invalid. Alternately, the ledger is updated and all peers append the transactions to

the channels' ledgers in the predefined order, ensuring determinism. Valid transactions will update the world state. Invalid ones are retained on the ledger but do not update the world state. Finally, the client app that submitted the transaction proposal will be notified by each peer on the network of transaction success. Hyperledger Besu architecture. The proposed Hyperledger Besu drug traceability architecture provides a fully compatible opensource 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, are Ethereum Virtual Machines (EVMs), Ether Sign, 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) . Hyperledger Besu blockchain architecture. Uddin et al. 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. To keep transactions private between involved stakeholders, Hyperledger Besu uses a Private Transaction Manager (PTM) such as Orion. PTMs that conform to the Enterprise Ethereum Alliance (EEA) Client Specification allows shared business logic in smart contracts to be made private to a limited number of participants, thus making all transactions and state associated with those smart contracts private as well. Orion, that is, native to Hyperledger Besu is such a PTM. Configuring a network that supports private transactions requires starting an Orion node for each Hyperledger Besu node. Lastly, to

give access permissions to different organizational users and their accounts, Hyperledger Besu offers both on-chain (via smart contracts) and off-chain permissioning (via configuration files). A permissioned network enables node and account permissioning, making access to the network restricted to only specified nodes and accounts. Alongside, permissioning features of Hyperledger Besu allow real-time account suspension, denying access to broken smart contracts, restricting actions based on organization/account details, etc. This further enables secure and transparent communication on the network by easing the management of access control.

CODING & SOLUTIONING

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Drug{
    address public owner;

    constructor() {
        owner = msg.sender;
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Only the owner can perform this action");
        _;
    }

    struct Drug {
        string drugName;
        string manufacturer;
        uint256 manufacturingDate;
        address trackingHistory;
    }
}
```

```
}
```

```
mapping(uint256 => Drug) public drugs;  
uint256 public drugCount;
```

```
event DrugManufactured(uint256 indexed drugId, string drugName, string  
manufacturer, uint256 manufacturingDate);
```

```
event DrugTransferred(uint256 indexed drugId, address indexed from,  
address indexed to, uint256 transferDate);
```

```
function manufactureDrug(uint256 drugId, string memory _drugName,  
string memory _manufacturer, uint256 _manufacturingDate) external  
onlyOwner {
```

```
    address initialHistory;  
    initialHistory = owner;
```

```
    drugs[drugId] = Drug(_drugName, _manufacturer, _manufacturingDate,  
initialHistory);  
    drugCount++;
```

```
    emit DrugManufactured(drugId, _drugName, _manufacturer,  
_manufacturingDate);  
}
```

```
function transferDrugOwnership(uint256 _drugId, address _to) external {  
    require(_to != address(0), "Invalid address");  
    require(_to != drugs[_drugId].trackingHistory, "Already owned by the  
new address");
```

```
    address from = drugs[_drugId].trackingHistory;  
    drugs[_drugId].trackingHistory = _to;
```

```
    emit DrugTransferred(_drugId, from, _to, block.timestamp);
```

```

    }

    function getDrugDetails(uint256 _drugId) external view returns (string
memory, string memory, uint256, address) {

        Drug memory drug = drugs[_drugId];
        return (drug.drugName, drug.manufacturer, drug.manufacturingDate,
drug.trackingHistory);
    }
}

```

PERFORMANCE TESTING

Testing and Validation

In order to assess the smart contracts developed via Ethereum, Remix IDE in-browser developing and testing environment was used to test and validate different functions. The scenarios involved three different participants and their corresponding Ethereum Addresses as presented.

Ethereum Address	
Participant1	0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c
Participant2	0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C
Participant3	0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB

We further present the transactions and logs of the smart contract's functions below.

- **Lot Details:** In this function, it was tested whether the current owner of the smart contract is able to add the details of a newly manufactured Lot such as the Lot name, Lot price, number of boxes within the Lot, and the price of each box. A successful execution of the function and its corresponding logs and events are displayed.
- **Grant Sale:** The grant Sale function has a simple task yet it's very important, it basically notifies all the entities that the manufactured Lot is currently for sale. A successful execution of the function is given.
- **Buy Lot:** this function is used to buy the Lot from Participant. Participant has specified the correct amount of ether to transfer and the successful execution of the function .
- **Buy Box:** This function deals with transactions related to purchase of specific number of boxes from the Lot (usually happens between a patient and the pharmacy). Figure 11 shows a successful execution of this function where Participant3 purchases 50 boxes from Participant2. The price of the boxes has been selected arbitrarily and they may not be logical but the purpose here is to confirm that the execution of the functions properly.

```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x44c99celec0af6519400dc5641e20fd507c596f90096ffe116181619d7ab1a25",
"event": "lotManufactured",
"args": {
  "0": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
  "manufacturer": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
  "length": 1
}
```

```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x15a51b79663b36aa87b7e256eddbad58070b43d374c4294e41b9e76ad43a4c04",
"event": "lotSale",
"args": {
  "0": "Aspirine",
  "1": "200",
  "2": "10000000000000000000",
  "3": "10000000000000000000",
  "_lotName": "Aspirine",
  "_numBoxes": "200",
  "_lotPrice": "10000000000000000000",
  "_boxPrice": "10000000000000000000",
  "length": 4
}
```

```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0xeb373dc4c684e4ae6135618e7fc15d654b409d8071dc8126b4a5d18ac86590db",
"event": "lotSold",
"args": {
  "0": "0x14723A09ACff6D2A60DcdF7aA4Aff308FDDC160C",
  "newownerID": "0x14723A09ACff6D2A60DcdF7aA4Aff308FDDC160C",
  "length": 1
}
```

```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x82c28ddbad097bd1003a55cdb6788f38fbe3033fa91c813a8a00652716c0d45b",
"event": "boxesSold",
"args": {
  "0": "50",
  "1": "0x14723A09ACff6D2A60DcdF7aA4Aff308FDDC160C",
  "_soldBoxes": "50",
  "newownerID": "0x14723A09ACff6D2A60DcdF7aA4Aff308FDDC160C",
  "length": 2
}
```


Discussion and Evaluation

In this section, we discuss generalization of the proposed Ethereum blockchain-based solution, present cost and security analysis for drug traceability in supply chain, and discuss blockchain limitations in supply chains.

Generalization

The proposed work in this article demonstrates how blockchain technology can be applied for drug traceability in a pharmaceutical supply chain. Although the functions in the smart contract were defined in a way that fits the pharmaceutical supply chain specifically, it can be easily extended to other types of supply chains .

The main difference between the pharmaceutical supply chain and any other supply chain is the products/items that are being shipped, distributed, and sold and the way they are handled throughout the process. For example, some pharmaceutical drugs require very specific conditions like temperature and humidity while they are being transferred from a point to another whereas a spare part supply chain for example would have very different conditions. Since live tracking is out of the scope of this article, tracing the origin of a product/item regardless of its type will be very similar because it only requires the scanning of a unique identification code which is attached to the product/item and the DApp will handle the rest. The only difference might occur in the way unique identifications are generated for the products/items which does not hinder the process.

It can be used as a reference to discuss the generalized application of the proposed solution in a different supply chain. Based on the specific supply chain application, for example, food, spare parts or other application the stakeholders of the supply chain and their role needs modification. Moreover, the use of a decentralized storage system might not be needed in cases where there is no necessity to store and access large data files from off-chain. Finally, the on-chain resources can be modified according to the needs of the proposed application, for example, a reputation system, payment and

funds transfer setup might not be needed. In such cases the on chain storage will be more than adequate to retain the transaction logs amid stakeholders.

The entity relationship diagram can be also modified, for example, if a supply chain has an application that requires the use of more than one parent smart contract then it will have to be added and define its relationship with the other entities. Another possibility is the creation of more than one product at a time which requires an extension to the functions to accommodate the additional products, and this can be achieved by modifying the existing smart contract.

Finally, the defined algorithms follow simple and easy to grasp steps, and similar algorithms are followed in many other supply chains. This fact can be used to adjust the customize the algorithms used in this article to fit the needs of specific supply chain application.

Cost Analysis

This subsection presents cost analysis of the Ethereum smart contract code and the function calls. When a transaction is executed on the Ethereum blockchain, it costs *gas* to send it to the Ethereum blockchain. Remix IDE is a very useful and easy to use tool to estimate the gas costs for the execution and transaction which are the main types of gas costs. The execution cost is the cost of executing different functions in the smart contract whereas the transaction cost deals with several factors such as the deployment of the contract, and any data that gets sent to the blockchain network

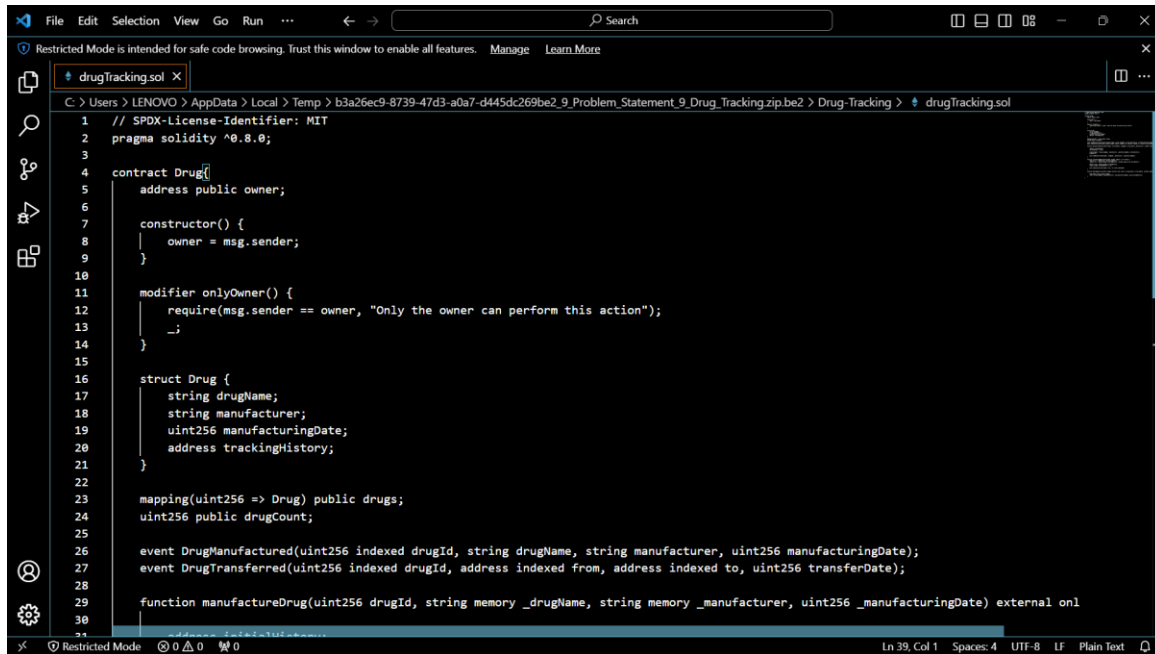
The gas costs of the different functions used in the smart contract, and it also shows the costs converted into fiat currency (USD). An average gas price of 2.8 GWEI was used according to the ETH gas station pricing accessed on Apr 10, 2020. It should be noted that gas prices vary over time and the ones used here will most likely change. However, they have been used in this context to show that the cost of executing these functions is relatively low. Furthermore, a paid oracle service (Chain link for

example) can be used to get the latest price of Ethereum which is then used to convert the transaction and executions costs into USD.

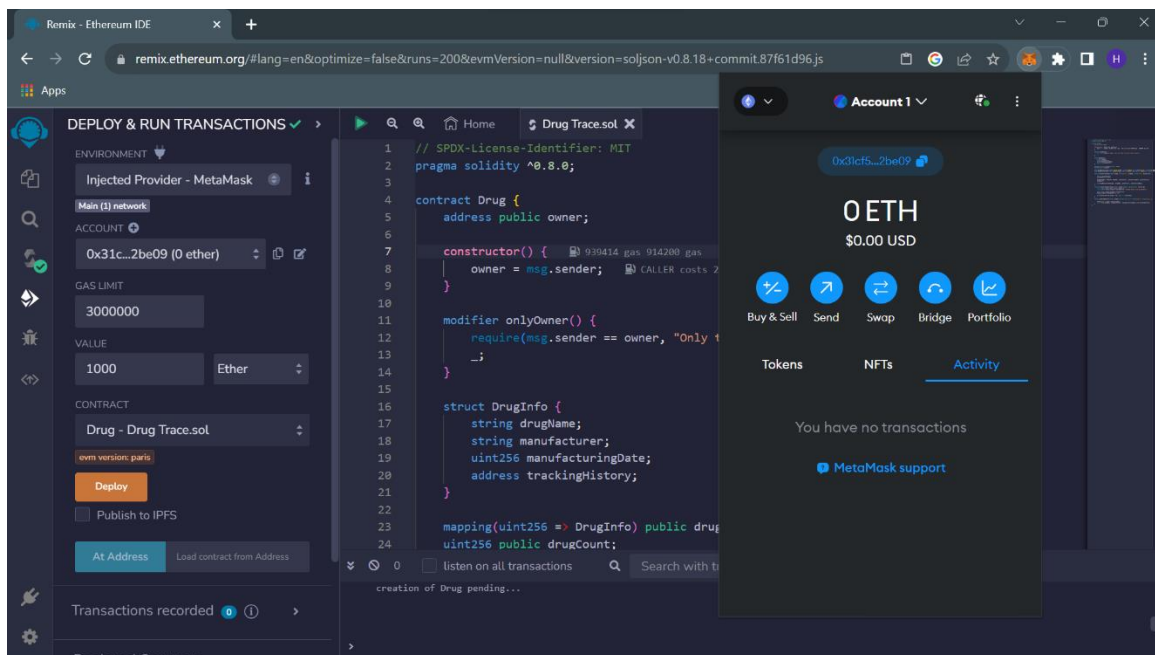
Function Caller	Function Name	Transaction Gas	Execution Gas	Cost in USD
SC Owner	lotDetails	107356	83844	0.04226
SC Owner	grantSale	29745	8473	0.00845
Buyer	buyLot	40845	19573	0.01334
Buyer	buyBox	62305	40841	0.0228

The cost in USD is very minimal for all four functions. The function that costs the most is the *lot Details* which is executed by the smart contract owner (manufacturer). This relatively high cost can be explained due to changes in five different variables in the function which requires storage. On the other hand, *grant Sale* function costs the least, as this function only broadcasts an event to notify the participants that the Lot is available for sale. From the previous observations, it can be concluded that the gas costs are proportional to the number of changes in the state of the smart contract, and it also shows how storage can increase costs dramatically, so it's really important for the user of the smart contract to upload the correct details of the drug Lot because once the function is executed it cannot be reverted and the Gas fees are gone forever.

RESULTS

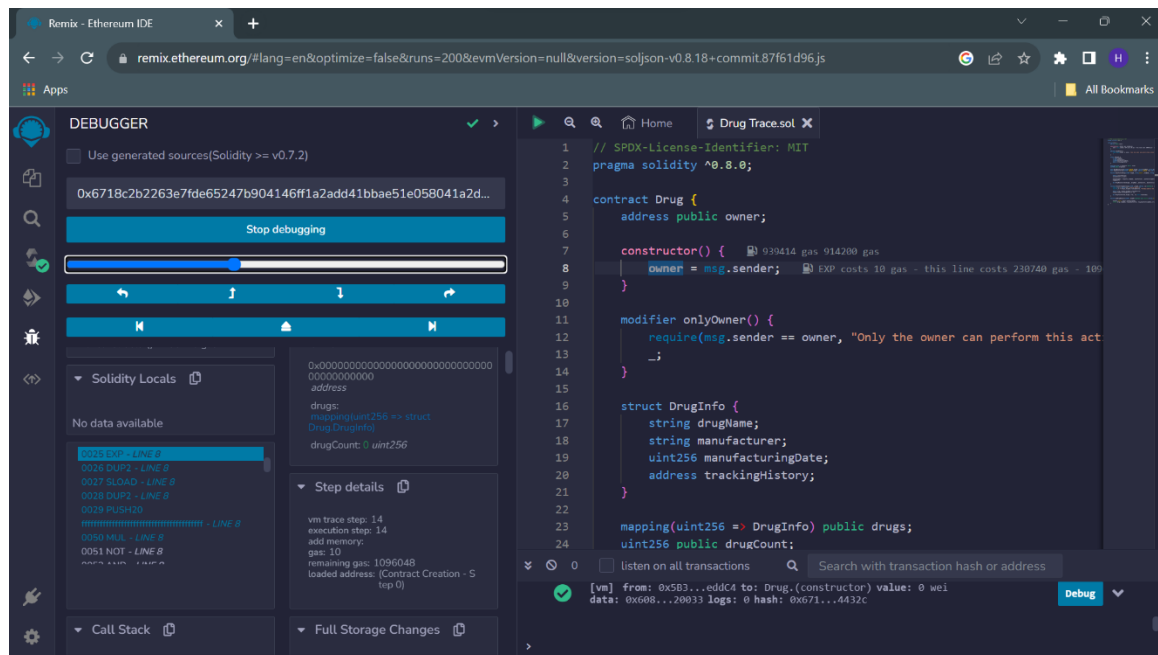


```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
3
4 contract Drug {
5     address public owner;
6
7     constructor() {
8         owner = msg.sender;
9     }
10
11     modifier onlyOwner() {
12         require(msg.sender == owner, "Only the owner can perform this action");
13         _;
14     }
15
16     struct Drug {
17         string drugName;
18         string manufacturer;
19         uint256 manufacturingDate;
20         address trackingHistory;
21     }
22
23     mapping(uint256 => Drug) public drugs;
24     uint256 public drugCount;
25
26     event DrugManufactured(uint256 indexed drugId, string drugName, string manufacturer, uint256 manufacturingDate);
27     event DrugTransferred(uint256 indexed drugId, address indexed from, address indexed to, uint256 transferDate);
28
29     function manufactureDrug(uint256 drugId, string memory _drugName, string memory _manufacturer, uint256 _manufacturingDate) external onl
30
31     function transferDrug(uint256 drugId, address indexed to, uint256 transferDate) external onlyOwner {
32         require(to != address(0), "Invalid address");
33         Drug memory drug = drugs[drugId];
34         drug.trackingHistory = to;
35         drugs[drugId] = drug;
36         emit DrugTransferred(drugId, msg.sender, to, transferDate);
37     }
38 }
```



The screenshot displays the Remix IDE interface with the following components:

- Left Panel (Deploy & Run Transactions):**
 - ENVIRONMENT:** Injected Provider - MetaMask
 - ACCOUNT:** 0x31c...2be09 (0 ether)
 - GAS LIMIT:** 3000000
 - VALUE:** 1000 Ether
 - CONTRACT:** Drug - Drug Trace.sol
 - Buttons:** Deploy, Publish to IPFS, At Address, Load contract from Address
 - Transactions recorded:** 0
- Center Panel (Code Editor):** Displays the Solidity code for DrugTrace.sol, including the constructor, modifier, struct, mapping, and functions.
- Right Panel (Account 1):** Shows the account balance as 0 ETH (\$0.00 USD) and a list of transactions (Buy & Sell, Send, Swap, Bridge, Portfolio). It also displays "You have no transactions" and "MetaMask support".



CONCLUSION

We have investigated the challenge of drug traceability within pharmaceutical supply chains highlighting its significance especially to protect against counterfeit drugs. We have developed and evaluated a blockchain-based solution for the pharmaceutical supply chain to track and trace drugs in a decentralized manner. Specifically, our proposed solution leverages cryptographic fundamentals underlying blockchain technology to achieve tamper-proof logs of events within the supply chain and utilizes smart contracts within Ethereum blockchain to achieve automated recording of events that are accessible to all participating stakeholders.

We have demonstrated that our proposed solution is cost efficient in terms of the amount of gas spent in executing the different functions that are triggered within the smart contract. Moreover, the conducted security analysis has shown that our proposed solution achieves protection against malicious attempts targeting its integrity, availability and non-repudiation of transaction data which is critical in a complex multi-party settings such as the pharmaceutical supply chain.

We continue our efforts to enhance the efficiency of pharmaceutical supply chains and envision to focus on extending the proposed system to achieve end to end transparency and verifiability of drugs use as future work.

APPENDIX

Github link : <https://github.com/HazanaBadhur/NM2023TMID05389>

Demo video link :

https://drive.google.com/file/d/1qhml2agu_42snFHxcXh_ZtBuMGyX0zx7/view?usp=sharing

