DEFINE PROBLEM/ PROBLEM UNDERSTANDING

Specify The Business Problem

Team Id	NM2023TMID04410
Project Name	Project- Drug Traceability

Drug traceability:

. The process of determining the product's authenticity and originality so that all stakeholders can track and trace transactions at every level of the supply chain.

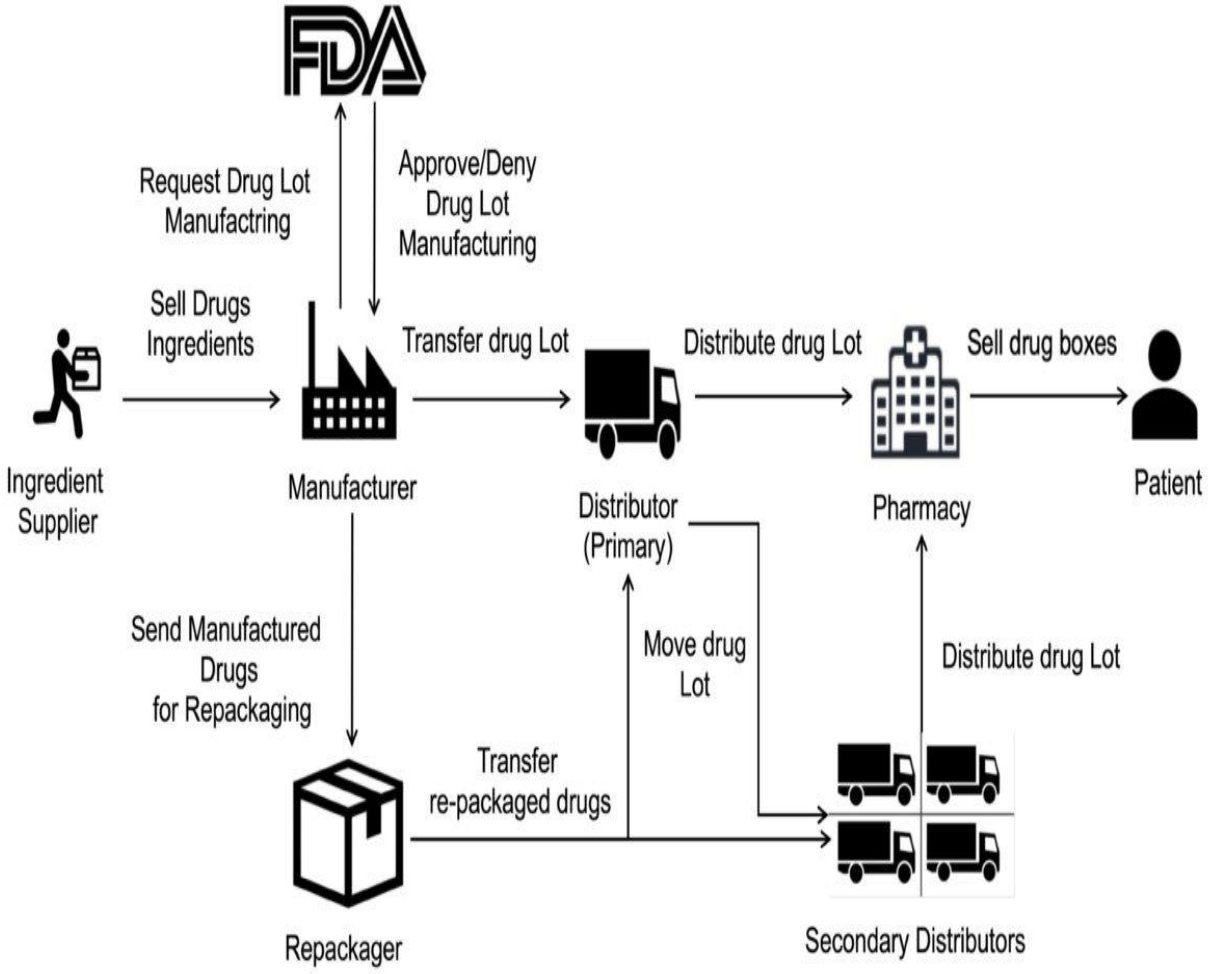


FIGURE 1. Drug supply chain stakeholders and their relationships

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 [21].

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.

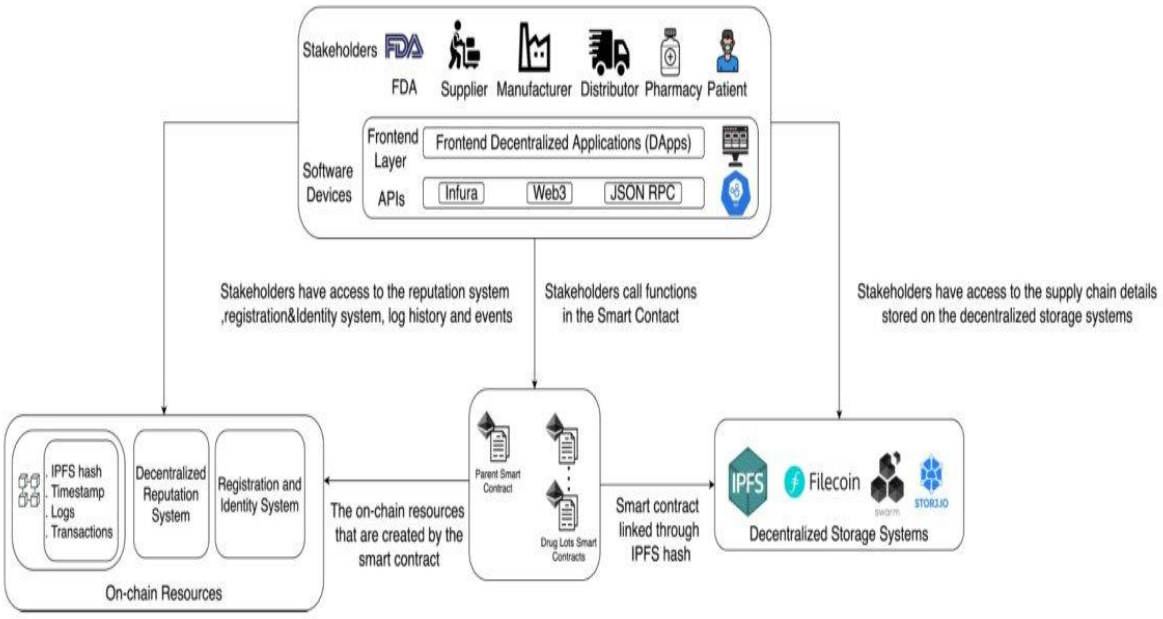
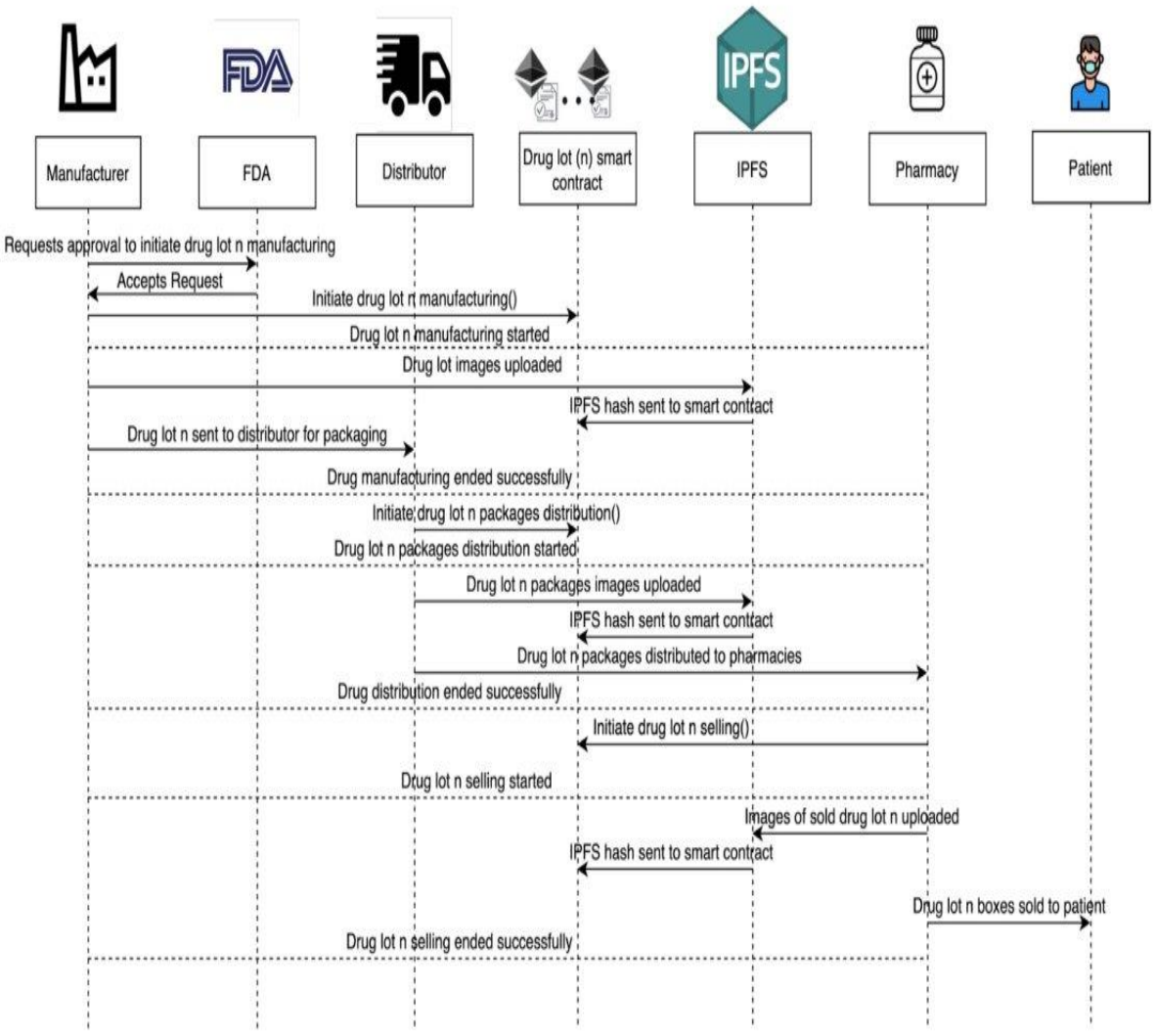


FIGURE 2. A high-level architecture for the proposed blockchain-based system for pharmaceutical supply chain

BLOCKCHAIN-BASED SOLUTIONS FOR DRUG TRACEABILITY :

Traditional solutions to achieve traceability within pharmaceutical supply chain are typically centralized and lack transparency across participants of the supply chain, which allows the central authority to modify information without notifying other stakeholders. On the other hand, a blockchain based solution offers data security, transparency, immutability, provenance and authenticated transaction records. Blockchain is a decentralized, immutable shared ledger that can be applied to a variety of business settings involving transaction processes.



Sequence Diagram showing interactions among the participating entities of the smart contract

In addition to the above, a number of active projects exist which are focused at exploring use of distributed ledger technologies to achieve traceability within pharmaceutical supply chain. For instance, Arsene [39] involves leading companies including IBM, Cisco, Accenture, Intel, Bloomberg, and Block stream where every drug is issued with a timestamp, making it traceable with its origin and manufacturer details. Similarly, MediLedger [40] investigates use of blockchain to provide a solution compliant with the DSCSA regulation to increase interoperability in the industry. Farmatrust project [41] aims to improve traceability in pharmaceutical industry based on Quorum blockchain with future plans to accommodate other platforms such as Ethereum and Hyperledger. The use of Quorum blockchain presents challenges such as lack of transaction ordering of transactions and policy enforcement which limits it widespread use.

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

Figure 2 presents a high-level architecture for the proposed drug traceability system together with the stakeholder and their interactions with the smart contract. 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 :

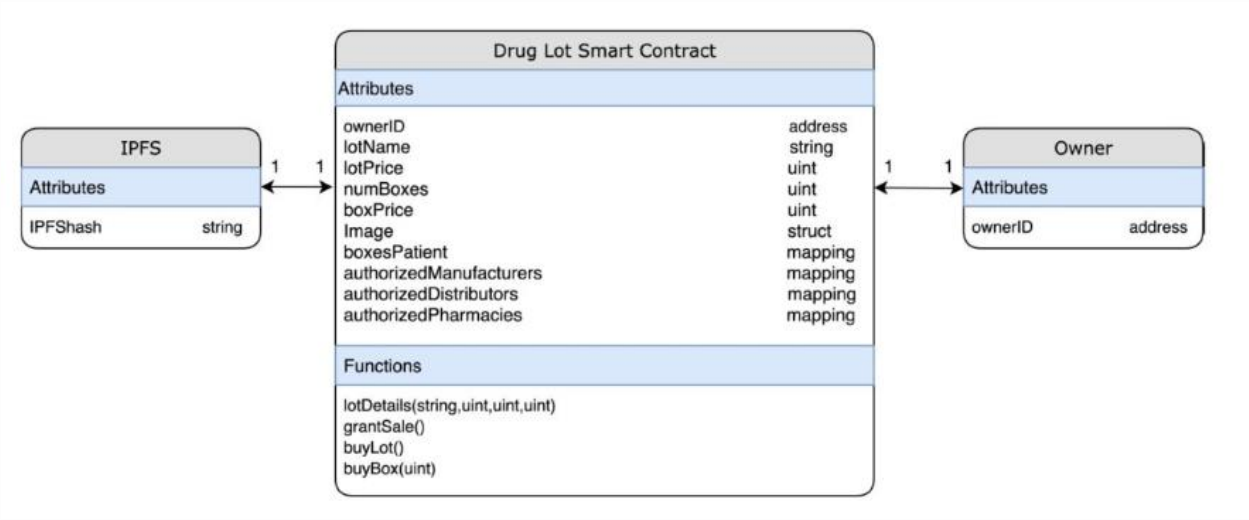
In this section, we present a comparative analysis of the proposed solution for traceable supply chain for pharmaceutical drugs with relevant existing solutions. A summary of this analysis is presented in Table 1.

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 solution

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



SECURITY ANALYSIS FOR THE BLOCKCHAIN-BASED HEALTHCARE SUPPLY CHAIN :

In this subsection, 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).

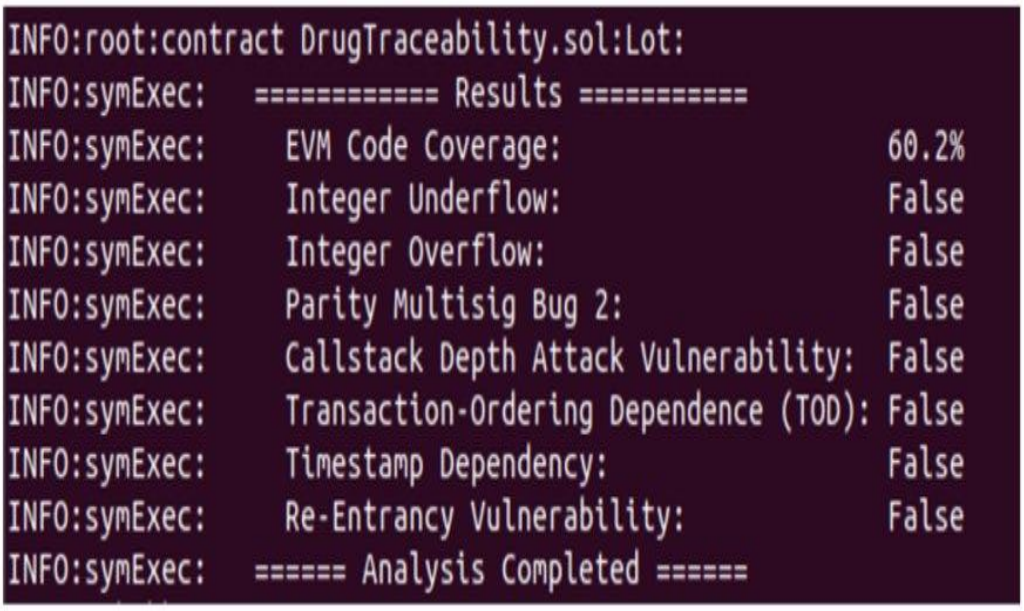
1. **Integrity:** The primary objective of the proposed blockchain solution is to keep track of all the transactions that occur within the healthcare supply chain ensuring traceability of the history of the Lots, ownership transfers and their corresponding boxes. This is ensured in the proposed solution 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.
2. **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 lotDetails function and pharmacies will be accountable for any prescription they give to a function because buyBox function will show where each patient is getting the drugs from
3. **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.
4. **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.
5. **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.

6. **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 that.

SMART CONTRACT SECURITY ANALYSIS

7. 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 such as the one shown in Figure 12. This figure shows the code coverage in addition to the availability of some crucial vulnerabilities that can be manipulated for malicious attacks.



8. FIG.

Smart contract vulnerability analysis