IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 10, 2020, accepted January 4, 2021, date of publication January 8, 2021, date of current version January 19, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3049920*

# A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain

**AHMAD MUSAMIH[1], KHALED SALAH[2], (Senior Member, IEEE), RAJA JAYARAMAN[1], JUNAID ARSHAD[3], MAZIN DEBE[2], YOUSOF AL-HAMMADI[2], AND SAMER ELLAHHAM[4]**

[1]Department of Industrial and Systems Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates
[2]Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, United Arab Emirates
[3]School of Computing and Digital Technology, Birmingham City University, Birmingham B5 5JU, U.K.
[4]Heart and Vascular Institute, Cleveland Clinic Abu Dhabi, Abu Dhabi, United Arab Emirates

Corresponding author: Raja Jayaraman (raja.jayaraman@ku.ac.ae)

This work was supported by the Khalifa University of Science and Technology under Award CIRA-2019-001.

**ABSTRACT** Healthcare supply chains are complex structures spanning across multiple organizational and geographical boundaries, providing critical backbone to services vital for everyday life. The inherent complexity of such systems can introduce impurities including inaccurate information, lack of transparency and limited data provenance. Counterfeit drugs is one consequence of such limitations within existing supply chains which not only has serious adverse impact on human health but also causes severe economic loss to the healthcare industry. Consequently, existing studies have emphasized the need for a robust, end-to-end track and trace system for pharmaceutical supply chains. Therein, an end-to-end product tracking system across the pharmaceutical supply chain is paramount to ensuring product safety and eliminating counterfeits. Most existing track and trace systems are centralized leading to data privacy, transparency and authenticity issues in healthcare supply chains. In this article, we present an Ethereum blockchain-based approach leveraging smart contracts and decentralized off-chain storage for efficient product traceability in the healthcare supply chain. The smart contract guarantees data provenance, eliminates the need for intermediaries and provides a secure, immutable history of transactions to all stakeholders. We present the system architecture and detailed algorithms that govern the working principles of our proposed solution. We perform testing and validation, and present cost and security analysis of the system to evaluate its effectiveness to enhance traceability within pharmaceutical supply chains.

**INDEX TERMS** Blockchain, drug counterfeiting, traceability, healthcare, supply chain, trust, security.

## I. INTRODUCTION

Healthcare supply chain is a complex network of several independent entities that include raw material suppliers, manufacturer, distributor, pharmacies, hospitals and patients. Tracking supplies through this network is non-trivial due to several factors including lack of information, centralized control and competing behaviour among stakeholders. Such complexity not only results in in-efficiencies such as those highlighted through COVID-19 pandemic [1] but can also aggravate the challenge of mitigating against counterfeit drugs as these can easily permeate the healthcare supply chain. Counterfeit drugs are products deliberately and fraudulently produced and/or mislabeled with respect to identity and/or source to make it appear to be a genuine product [2], [3]. Such drugs can include medications that contain no active pharmaceutical ingredient (API), an incorrect amount of API, an inferior-quality API, a wrong API, contaminants, or repackaged expired products. Some counterfeit medications may even be incorrectly formulated and produced in substandard conditions [4].

According to the Health Research Funding Organization, up to 30% of the drugs sold in developing countries are counterfeit. Further, a recent study by World Health Organization (WHO) indicated counterfeit drugs as one of the major causes of deaths in developing countries, and in most cases the victims are children [7], [8]. In addition to the adverse impact on human lives, counterfeit drugs also cause significant economic loss to the pharmaceutical industry. In this respect, the annual economic loss to the US pharmaceutical industry due to counterfeit medicine is estimated around $200 billion [9], [10].

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

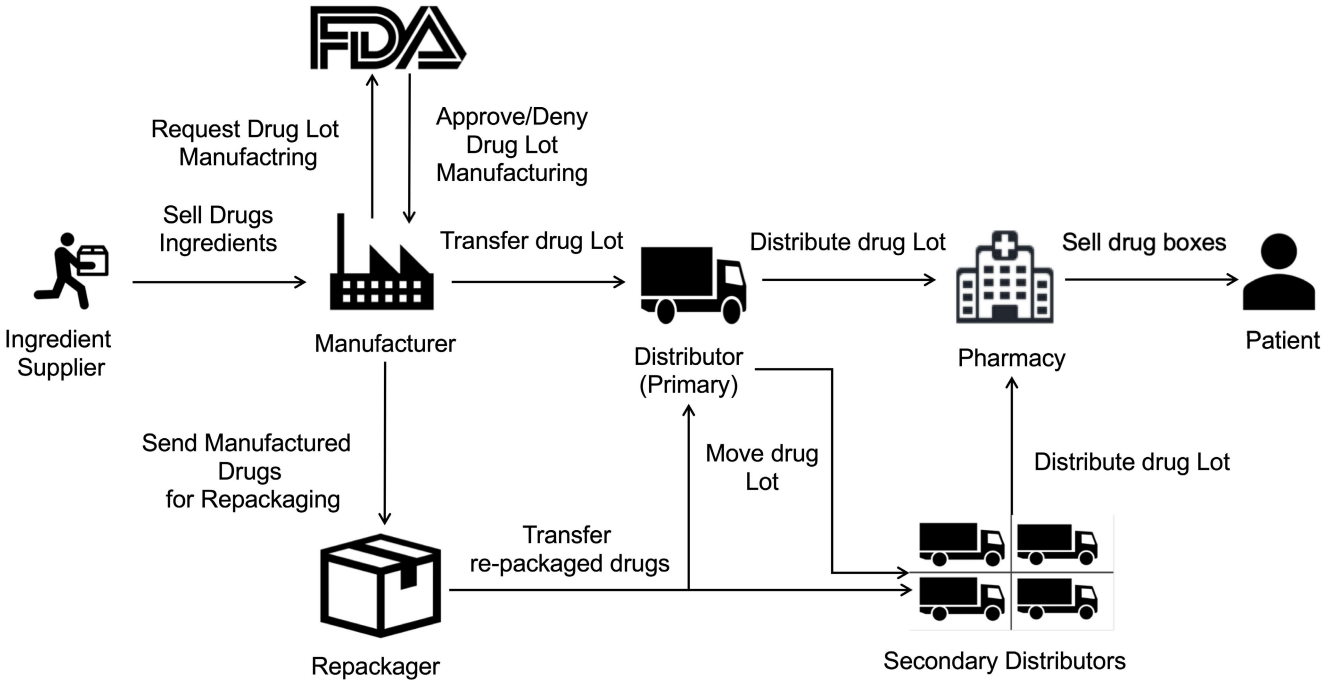


**FIGURE 1.** Drug supply chain stakeholders and their relationships.

A typical drug supply chain distribution process is illustrated in Figure 1. An API supplier is responsible for delivering the raw materials to manufacture drugs approved by a regulatory agency such as the US Food and Drug Administration (US FDA). The manufacturer packages the drugs into a *Lot* or sends it to a re-packager. The primary distributor receives several Lots of the product and is responsible for transferring them to pharmacies based on product demand or secondary distributors (in case the quantity of Lots is very large) who can transfer these Lots to the pharmacies. Finally, a pharmacy will dispense the drug to patients [11] typically based on a doctor's prescription. Throughout the supply chain, the transfer of drugs is usually facilitated by third party logistic service providers such as UPS or FedEx and in some cases the distributors operate their own fleet of vehicles to transport the products.

The primary reason for counterfeit drugs to reach end-user marketplace is due to the complex structure of a healthcare supply chain. Leveraging the complexity of this distribution process, medications can easily pass through with little or no trail of information and verifiable documentation [12]. Consequently, monitoring, effective control and tracking of products in healthcare supply chain is fundamental to combating counterfeits.

The importance of drug traceability (track and trace) is increasingly emphasized and mandated by several countries across the world. For example, the U.S. Drug Supply Chain Security Act (DSCSA) has made it mandatory for the pharmaceutical industry to develop an electronic and interoperable system that identifies and tracks prescription drugs as they are distributed across the United States [13]. Similarly, over the last 8 years, China required all the stakeholders involved in the drugs supply chain to record information of individual pharmaceutical products in a specialized IT system whenever drugs are sent to/from their warehouses [14]. Therefore, drug traceability has become an integral part of the pharmaceutical supply chain as it establishes authenticity, and aims to track and trace chain of custody of the product across drug supply chain.

Blockchain technology has introduced a new model of application development primarily based on the successful implementation of the data structure within the Bitcoin application. The fundamental concept of the blockchain data structure is similar to a linked list i.e. it is shared among all the nodes of the network where each node keeps its local copy of all the blocks (associated with the longest chain) starting from its genesis block [15]. Recently, many real-world applications have been developed in diverse domains, such as the Internet of Things [16], e-Government [17] and e-document management [18]. These applications leverage benefits of blockchain technology due to its self-cryptographic validation structure among transactions (through hashes), and public availability of distributed ledger of transaction-records in a peer-to-peer network. Creating a chain of blocks connected by cryptographic constructs (hashes) makes it very difficult to tamper the records, as it would cost the rework from the genesis to the latest transaction in blocks as illustrated by [19].

Within the context of blockchain-based traceability for pharmaceutical supply chain, [20] presents one of the initial efforts. Although our solution has similarities with this

effort due to the focus on pharmaceutical supply chain as well as the use of blockchains, we take a holistic view of the pharmaceutical supply chain, presenting an end-to-end solution for drug traceability whereas [20] only focused on a subset of these challenges. **Firstly**, our approach identifies and engages major stakeholders in the drug supply chain i.e. the FDA, supplier, manufacturer, distributor, pharmacy, and patient, whereas [20] is limited to the supplier, manufacturer, and wholesaler as the stakeholders. Consequently, the pharmacists are represented as an external entity which is not the case in a real drug supply chain. **Secondly**, we make explicit efforts to identify and define relationships among stakeholders, on-chain resources, smart contracts, and decentralized storage systems which is lacking in [20]. Furthermore, in view of the significance of interactions among stakeholders, we have included precise definitions to remove any ambiguity, whereas such interactions have not been defined as part of [20]. **Thirdly**, we use the smart contracts technology to achieve real-time, seamless traceability with push notifications so as to minimize human intervention and therefore undesired delays. Specifically, each drug Lot is assigned a unique smart contract that generates an event whenever a change in ownership occurs and a list of events is delivered to the DApp user. However, the smart contracts in [20] are programmed for specific roles such as supplier, manufacturer, and wholesaler which requires each participant to manually confirm which drugs are received. Such approach can introduce delays and inaccuracies in the immutable data stored on the ledger. **Finally**, we have conducted a cost and security analysis to evaluate the performance of the proposed solution including discussion on how the proposed solution can be generalized to other supply chains.

The challenge of achieving traceability to mitigate against counterfeit drugs is well-established and several efforts have been made to address this within pharmaceutical industry. However, a careful review of literature presents several gaps and opportunities for a comprehensive application of blockchain technology for drug traceability. In this context, the primary contributions of this article can be summarized as follows:

- We propose a blockchain-based solution for the pharmaceutical supply chain that provides security, traceability, immutability, and accessibility of data provenance for pharmaceutical drugs.
- We design a smart contract capable of handling various transactions among pharmaceutical supply chain stakeholders.
- We present, implement and test the smart contract that defines the working principles of our proposed solution.
- We conduct security and cost analysis to evaluate the performance of the proposed blockchain-based solution.

The reminder of this article is organized as follows. Section II presents a critical review of existing efforts with respect to traceability in the healthcare supply chain. This is followed by a description of the proposed blockchain-based track & trace system for phamaceutical products in section III. Section IV presents the implementation of the proposed system along with details of the testing and evaluation in section V. Section VI describes the efforts to evaluate the proposed system and analyzes the outcomes of evaluation. Section VII concludes this article summarizing contributions and highlighting avenues for further work.

## II. 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.

### A. 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].

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 [22]. In this context, Smart-Track [23] 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 [24] 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, [25] 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.

Corrado *et al.* [26], Supriya and Djearamane [27], and Jamal *et al.* [28] 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.

### B. 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.

Transparency and traceability are used interchangeably however, they represent very different concepts. Transparency is usually used when referring to high-level information of a supply chain. For example, product's components, facilities locations, names of suppliers, etc. with the objective to map the whole supply chain. However, traceability is related to granular information where it envisages choosing a specific component to trace, determines common standards to communicate with partners, implements methods to produce and gather accurate data, selects a platform to store traceability data, and determines how to share data on the platform. Although both terms represent different concepts, they rely on each other because accessing granular information requires full understanding of the supply chain.

In this respect, a number of existing approaches leverage cryptographic properties of blockchain to achieve a decentralized, verifiable track and trace system for pharmaceutical drugs. Mettler [32] have discussed the use of blockchain based approach for various issues in healthcare sector with no technical details or specific application. Kurki [33], presented the advantages of blockchain technology in pharmaceutical supply chain. However, similar to [32] only conceptual discussion was provided. Muniandy and Ong Tze Ern [20] proposed a traceability system using Ethereum for anti-counterfeiting. The proposed solution employs smart contract however it lacks implementation or evaluation which limits understanding the contribution.

Huang *et al.* [34] proposed a drug traceability system, *Drugledger*, which reflects the practical drug transaction logic in the supply chain, and generates both authenticity and privacy of stakeholders' traceability information without losing the resilience of the system. Drugledger completes its workflow based on the expanded UTXO data structure, especially that of package, repackage, and unpackage. However, recent studies such as [35] have highlighted concerns with the use of UTXO data structure with respect to its weakness in programmability, high storage cost, and low state space utilization.

Faisal *et al.* [36], proposed a Hyperledger-based solution for drug traceability in the pharmaceutical supply chain. Authors report increase in the performance in terms of throughput and minimizes latency of the proposed system with less utilization of resources, however their solution was not rigorously tested and was implemented in a small-sized network. This effort also highlighted the challenge of achieving scalable solutions with blockchain which has received significant attention in recent literature such as [22]. Similar concerns are valid for the approach adopted by Hulseapple [38] who developed a private blockchain concurrently with the Bitcoin, which is used as a ledger to hash certain data to secure the transactions in chain. Every product has its own permanent record on their blockchain, making it impossible to manipulate with the private keys. The system was designed to protect every stage of product transfer in the supply chain, creating a trustless system of transparency.

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.

## III. 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,

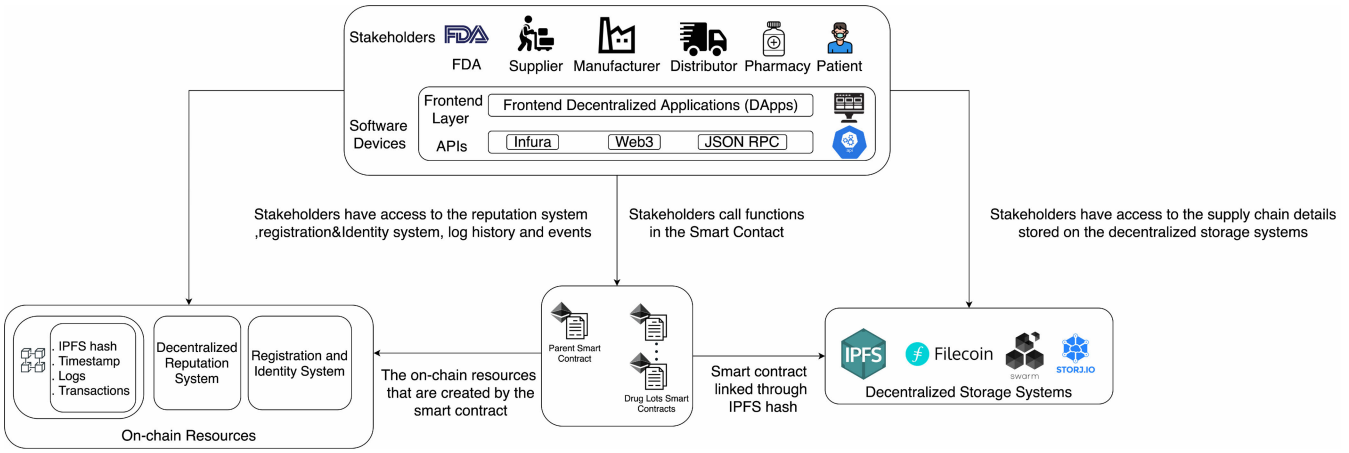


**FIGURE 2.** A high-level architecture for the proposed blockchain-based system for pharmaceutical supply chain.

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.

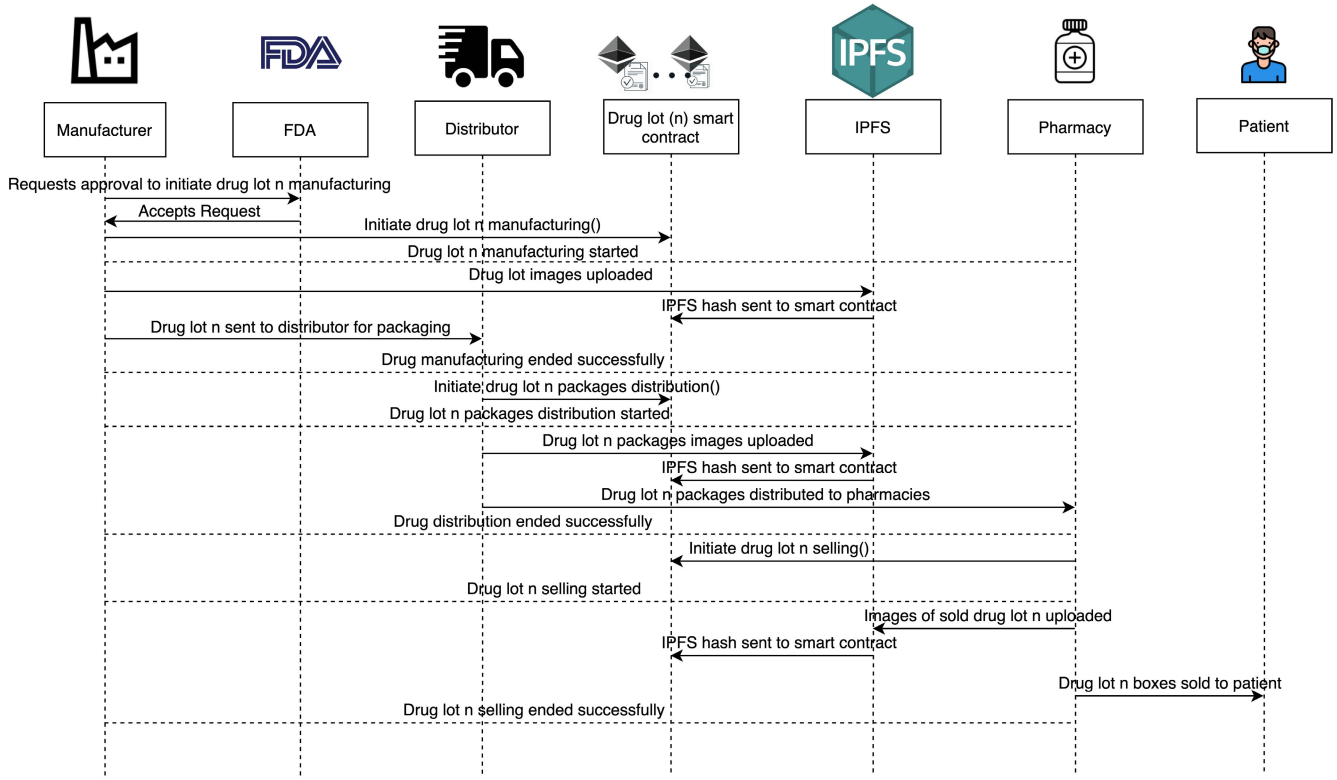


**FIGURE 3.** Sequence Diagram showing interactions among the participating entities of the smart contract.

**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.

### *A. 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 ledger 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

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

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

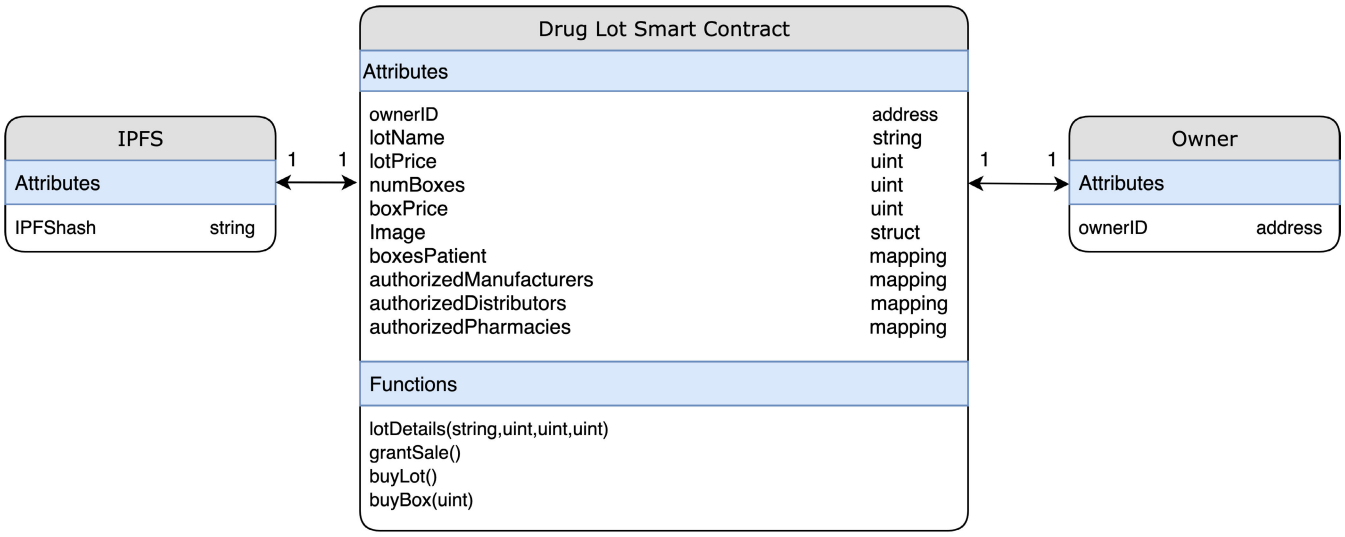


**FIGURE 4.** Entity Relationship Diagram.

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

| | Our Soluition | 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 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 Hyperledger-fabric. 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.

## IV. IMPLEMENTATION OF PROPOSED TRACEABILITY SYSTEM

The proposed solution is developed using the Ethereum blockchain platform. Ethereum is a permissionless public blockchain which means it can be accessed by anyone. The smart contract is written in Solidity language, and compiled and tested using Remix IDE. Remix is an online web-based development environment for writing and executing codes for smart contracts, and it also allows the user to debug and test the environment of the Solidity code. The full code[1] has been made publicly available.

[1]https://github.com/DrugTraceability/DrugTraceability/blob/master/Code

### A. IMPLEMENTATION DETAILS

The manufacturer will first deploy the smart contract in which details of the manufactured drug Lot will be defined, declared and an event will be triggered and announced to all participants in the supply chain. In case new participants are added to the network, they will have access to the events since they are permanently stored on the ledger and therefore they can track and trace the history of any manufactured drug Lot. The manufacturer also has the option of uploading an image of the Lot to the IPFS so that it can be accessed by participating entities to visually inspect the drug Lot. Prior to the sale of the newly manufactured Lot, it has to be packaged, the manufacturer will announce to other participants that the newly manufactured Lot is available for sale by sending an event. Participating entities interested in buying the newly manufactured Lot will have to access a function that is specialized in selling Lots, and once the transaction is finalized, an event will notify the participants declaring the new owner of the Lot. The manufacturer will not be eligible to deploy the smart contract for the drug Lot unless it is approved by the FDA but for the sake of simplicity, this approval is not implemented in the smart contract.

Figure 4 illustrates the relationship among the different entities with the smart contract. First, the smart contract will be deployed using the attributes shown in Figure 4 such as the *ownerID*, which has the Ethereum address of the current smart contract owner. One important thing to note here is that the owner ID is an address and not mapping because drug Lot smart contract can only have one owner ID and once the ownership changes an event will be emitted and stored on the blockchain, and these events will be used to trace the origin of the drug Lot. Because the smart contract represents a particular drug Lot, it has other attributes such as the *lotName, lotPrice, numBoxes,boxPrice, and Image*. Moreover, there are three mappings for the authorized entities that are

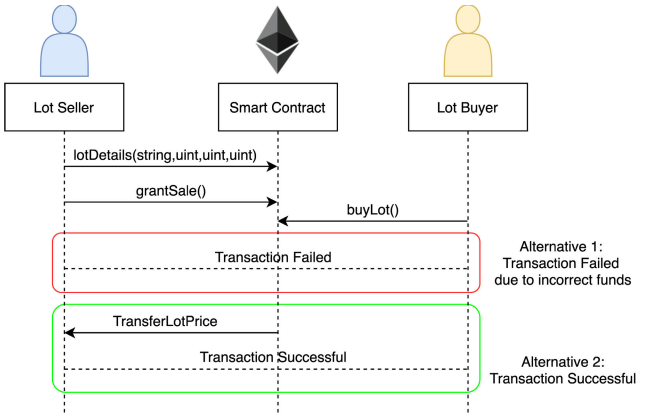


**FIGURE 5.** Function calls and events for two different scenarios for Lot sale.

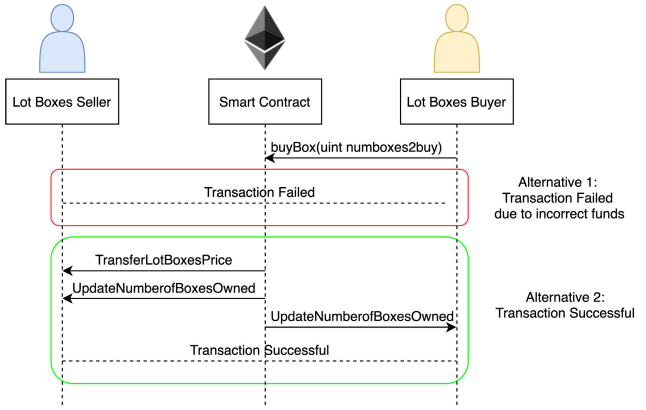


**FIGURE 6.** Function calls and events for two different scenarios for lot boxes sale.

allowed to access certain functions within the smart contract, namely, manufacturers, distributors, and pharmacies. The smart contract also has several functions needed to carry out the manufacturing process and sale process of the Lots. Adding the details of the manufactured Lot is accomplished by using function calls *lotDetails* that includes *lotName, lotPrice, numBoxes*, and *boxPrice* as an inputs. In addition, the manufacturer has the option of uploading images to the IPFS where the IPFS hash of the image is saved and accessed by other entities. The relationship between the smart contract and the IPFS is a 1:1 relationship because every Lot will have one image uploaded to the IPFS.

Figure 5 shows an illustrative scenario of a buyer attempting to buy the Lot from a seller. In a real-life supply chain, such a scenario will occur between the manufacturer and the distributor, or between the distributor and the pharmacy. The sequence diagram in Figure 5 can be generalized for both scenarios. Firstly, the Lot seller adds the Lot details by using the *lotDetails* function optionally uploading an image of that Lot to the IPFS as well as storing the hash along with other details of the Lot on chain. After that, the seller announces to all participants that the Lot is currently for sale via the *grantSale* function. An entity interested in buying the Lot executes the *buyLot* function which has two important requirements. Firstly, the executor of the function shouldn't have the same Ethereum address as the owner of the Lot, and secondly, the buyer should have sufficient funds to buy the Lot, thereby leading to two possible alternatives. Specifically, if the specified funds by the buyer do not match the price of the Lot, the transaction will fail. However, if the funds are equal to the price of the Lot then the transaction will be considered successful, and the funds will be transferred to the buyer.

Figure 6 shows a similar scenario to the one depicted in Figure 5 with subtle variations. In this case, the buyer will be specify a certain number of boxes from the Lot to be purchased. This scenario usually happens in a real pharmaceutical supply chain between the pharmacy and the patient. The buyer initiates the process by executing the *buyBox* function with the number of boxes needed and can result in two outcomes. If the transferred amount does not match the price of the boxes it will result in failure of the transaction. However, if the transferred amount is exactly equal to the price of the requested boxes, the price of the boxes will be transferred to the seller. Moreover, the number of boxes owned by the two entities will be updated according to the quantity purchased. Finally, the transaction will be finalized and declared successful to all participants.

To further clarify the various functions of the smart contract, we present various algorithms used in our proposed solution. It should be noted that when referring to a buyer or a seller it only includes the authorized entities who are given the permission to execute the functions The following are the main functions with their corresponding algorithms.

- **Creating a Lot**: Algorithm 1 explains the steps in creating a Lot. The inputs to the smart contract needed by the functions are shown with their descriptions. The function executes only if the address of the caller is the same as the address of the *ownerID*. If the caller is granted access, he/she will have the authority to update the fields in Algorithm 1. Once all fields have been updated the two events will update the status as shown in Algorithm 1.
- **Grant Lot Sale**: The algorithm 2 describes Granting Lot Sale of the drug. This algorithm is responsible for sending an event alerting all participants that the Lot is currently available for sale, and can only be triggered if the caller is the *ownerID* holder.
- **Buying Lot**: Algorithm 3 describes the transactions between the buyer and the seller of the drug Lot. It requires the caller of the function (buyer) to not have the same address as seller (to ensures Lot owner doesn't buy his own Lot) and requires the transferred amount to be exactly equal to the Lot price. Once both requirements are fulfilled, the sale amount will be transferred to the seller. Moreover, the *ownerID* will be updated. Finally, an event will be triggered to announce the sale of the Lot and update the new owner details. An important thing to note here is that only trusted entities are allowed to use

**Algorithm 1 Creating a Lot in Smart Contract**

**Input**: lotName, lotPrice, numBoxes, boxPrice, IPFShash, Caller, OwnerID
**Output**: An event declaring that the Lot has been manufactured
An event declaring that the image of the Lot has been uploaded
**Data**:
*lotName*: is the name of the Lot
*lotPrice*: is the specified price of the Lot
*numBoxes*: is the total number of boxes within a Lot
*boxPrice*: is the price of each box within a Lot
*IPFShash*: is the IPFS hash of the Lot image
*ownerID*: is the Ethereum address of the owner of the Lot
initialization;
**if** *Caller* == *ownerID* **then**
  Update *lotName*
  Update *lotPrice*
  Update *numBoxes*
  Update *boxPrice*
  Add *IPFShash*
  Emit an event declaring that the Lot has been manufactured
  Emit an event declaring that the Lot image has been uploaded to the IPFS server
**else**
  Revert contract state and show an error.

**Algorithm 2 Granting Lot Sale**

**Output**: An event declaring that the Lot is for sale
initialization;
**if** *Caller* == *ownerID* **then**
  Emit an event stating that the Lot is up for sale
**else**
  Revert contract state and show an error.

**Algorithm 3 Buying Lot**

**Input**: ownerID, Buyer, Seller, Transferred Amount, lotPrice
**Output**: An event declaring that the Lot has been sold
**Data**: *ownerID*: The Ethereum address of the current Lot owner
*Buyer*: The Ethereum Address of the buyer
*Seller*: The Ethereum Address of the Seller
*Transferred Amount*: The amount transferred to the function
*lotPrice*: The price of the Lot
initialization;
**if** $Buyer \neq Seller \wedge TransferredAmount = lotPrice$ **then**
  Transfer the price of the Lot to the seller
  Update ownerID by replacing the seller Ethereum address to the buyer Ethereum Address
  Emit an event declaring that the Lot has been sold
**else**
  Revert contract state and show an error.

the smart contract. Therefore, when a Lot is announced sold, the buyer can rest assure that the seller is trusted and the Lot will be delivered.

- **Buying Lot Boxes**: Algorithm 4 is similar to Algorithm 3, with subtle difference. The initiation of this algorithm is similar to Algorithm 3 but the buyer is required to specify the exact number of boxes within the Lot. The amount transferred by the buyer has to be exactly equal to the number of boxes the buyer wants to buy multiplied with the price of each box. The main difference here is that there is mapping for the addresses of the buyers with the number of boxes purchased, and the mapping gets updated every time this function gets executed successfully.

### B. 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.

Figure 7 illustrates 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 [45].

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 *lotSold* event to enter the pharmacy Ethereum

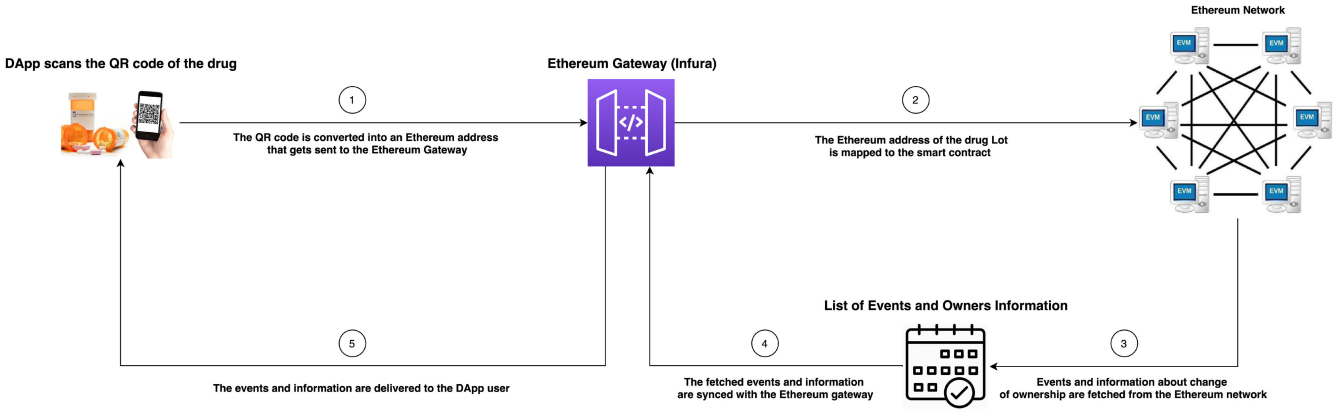


**FIGURE 7.** Application use case of the proposed blockchain-based solution.

**Algorithm 4 Buying Lot Boxes**

**Input**: ownerID, Buyer, Seller, Transferred Amount, boxPrice, numBoxes, numBoxesToBuy, Transferred Amount, boxesPatient
**Output**: An event declaring that the Lot boxes have been sold
**Data**: *ownerID*: The Ethereum address of the current Lot owner
*Buyer*: The Ethereum Address of the buyer
*Seller*: The Ethereum Address of the Seller
*Transferred Amount*: The amount transferred to the function
*boxPrice*: The price of the Lot box
*numBoxes*: The total number of boxes in the Lot
*numBoxesToBuy*: The number of boxes the buyer wants to buy
*boxesPatient*: Maps the number of boxes bought to the buyer address
initialization;
**if** $Buyer \neq Seller \wedge TransferredAmount = numBoxesToBuy * boxPrice$ **then**
  Transfer the price of the boxes to the seller
  Update ownerID by replacing the seller Ethereum address to the buyer Ethereum address
  Update numBoxes owned by the seller by decreasing the sold amount from it
  Update boxesPatient by assigning the purchased amount to the buyer address
**else**
  Revert contract state and show an error.

address to verify the drug Lot was sold to the pharmacy legally. After that, the *lotSale* 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 *imageuploaded* 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 *lotManufactured* event can be used to check if the Ethereum address of the manufacturer matches the original one. Finally, the *newOwner* event is used to view the Ethereum address of the original owner of the smart contract to confirm its authenticity.

**TABLE 3.** The Ethereum address of each participant in the testing scenario.

| | Ethereum Address |
|---|---|
| Participant1 | 0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c |
| Participant2 | 0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C |
| Participant3 | 0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB |

The Ethereum network presented in Figure 7 illustrates how 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 [46].

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.

## V. TESTING AND VALIDATION

In order to asses 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 in Table 3.

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

- **lotDetails**: 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

```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x44c99ce1ec0af6519400dc5641e20fd507c596f90096ffe116181619d7ab1a25",
"event": "lotManufactured",
"args": {
        "0": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
        "manufacturer": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
        "length": 1
```


**FIGURE 8.** Successful execution of lotDetails Function.


```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x15a51b79663b36aa87b7e256eddbad58070b43d374c4294e41b9e76ad43a4c04",
"event": "lotSale",
"args": {
        "0": "Aspirine",
        "1": "200",
        "2": "100000000000000000",
        "3": "100000000000000000",
        "_lotName": "Aspirine",
        "_numBoxes": "200",
        "_lotPrice": "1000000000000000000",
        "_boxPrice": "100000000000000000",
        "length": 4
```


**FIGURE 9.** Successful execution of grantSale Function.


```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0xeb373dc4c684e4ae6135618e7fc15d654b409d8071dc8126b4a5d18ac86590db",
"event": "lotSold",
"args": {
        "0": "0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C",
        "newownerID": "0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C",
        "length": 1
```


**FIGURE 10.** Successful execution of buyLot Function.


```
"from": "0x5e72914535f202659083db3a02c984188fa26e9f",
"topic": "0x82c28ddbad097bd1003a55cdb6788f38fbe3033fa91c813a8a00652716c0d45b",
"event": "boxesSold",
"args": {
        "0": "50",
        "1": "0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C",
        "_soldBoxes": "50",
        "newownerID": "0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C",
        "length": 2
```


**FIGURE 11.** Successful execution of buyBox Function.

each box. A successful execution of the function and its corresponding logs and events are displayed in Figure 8.

- **grantSale**: The grantSale 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 in Figure 9.
- **buyLot**: In this function, Participant2 (Table 3 shows the corresponding Ethereum address) is used to buy the Lot from Participant1. Participant1 has specified the correct amount of ether (which is 1Ether as shown in Figure 8) to transfer and the successful execution of the function is shown in Figure 10.
- **buyBox**: 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.

## VI. 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.

### A. 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 [47].

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.

Figure 2 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 [48]. This fact can be used to adjust the customize the algorithms used in this article to fit the needs of specific supply chain application.

### B. 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

**TABLE 4. Gas Costs of the Smart Contract Functions.**

| 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 |

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.

Table 4 shows 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 [49] 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 (Chainlink 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.

Table 3 presents that the cost in USD is very minimal for all four functions. The function that costs the most is the *lotDetails* 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, *grantSale* 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.

### C. 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).

- **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 *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
- **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

```
INFO:root:contract DrugTraceability.sol:Lot:
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                    60.2%
INFO:symExec:     Integer Underflow:                    False
INFO:symExec:     Integer Overflow:                     False
INFO:symExec:     Parity Multisig Bug 2:                False
INFO:symExec:     Callstack Depth Attack Vulnerability: False
INFO:symExec:     Transaction-Ordering Dependence (TOD): False
INFO:symExec:     Timestamp Dependency:                 False
INFO:symExec:     Re-Entrancy Vulnerability:            False
INFO:symExec:   ====== Analysis Completed ======
```

**FIGURE 12.** Smart contract vulnerability analysis.

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.

### D. 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 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.

### E. 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 blockchain-based 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.

## VII. CONCLUSION

In this article, 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 is 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.

## REFERENCES


[1] *Shortage of Personal Protective Equipment Endangering Health Workers Worldwide*. Accessed: Jun. 3, 2020. [Online]. Available: https://tinyurl.com/v5qauvp

[2] W. G. Chambliss, W. A. Carroll, D. Kennedy, D. Levine, M. A. Moné, L. D. Ried, M. Shepherd, and M. Yelvigi, "Role of the pharmacist in preventing distribution of counterfeit medications," *J. Amer. Pharmacists Assoc.*, vol. 52, no. 2, pp. 195–199, Mar. 2012.

[3] Z. RJ, "Roles for pharmacy in combating counterfeit drugs," *J. Amer. Pharmacists Assoc.*, vol. 48, pp. e71–e88, Jul. 2008.

[4] P. Toscan. *The Dangerous World of Counterfeit Prescription Drugs*. Accessed: Jun. 3, 2020. [Online]. Available: http://usatoday30.usatoday.com/money/industries/health/drugs/story/2011-10-09/cnbc-drugs/50690880/1

[5] T. Adhanom. (2017). *Health is a Fundamental Human Right*. Accessed: May 26, 2020. Available: https://www.who.int/mediacentre/news/statements/fundamental-human-right/en/

[6] *Growing Threat From Counterfeit Medicines*, World Health Organization, Geneva, Switzerland, 2010.

[7] D. Bagozzi. (2017). *1 in 10 Medical Products in Developing Countries Is Substandard or Falsified*. Accessed: Jun. 3, 2020. https://www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

[8] T. Guardian. (2017). *10% of Drugs in Poor Countries Are Fake, Says WHO*. Accessed: Jun. 3, 2020. [Online]. Available: https://www.theguardian.com/global-development/2017/nov/28/10-of-drugs-in-poor-countries-are-fake-says-who

[9] H. R. Funding. (2017). *20 Shocking Counterfeit Drugs Statistics*. Accessed: Jun. 3, 2020. [Online]. Available: https://healthresear.chfunding.org/20-shocking-counterfeit-drugs-statistics

[10] A. Seiter, "Health and economic consequences of counterfeit drugs," *Clin. Pharmacol. Therapeutics*, vol. 85, no. 6, pp. 576–578, Jun. 2009.

[11] U.S. Food and Drug Administration. *A Drug Supply Chain Example*. Accessed: Jun. 3, 2020. [Online]. Available: https://www.fda.gov/drugs/drug-shortages/graphic-drug-supply-chain-example

[12] A. Marucheck, N. Greis, C. Mena, and L. Cai, "Product safety and security in the global supply chain: Issues, challenges and research opportunities," *J. Oper. Manage.*, vol. 29, nos. 7–8, pp. 707–720, Nov. 2011.

[13] U.S. Food and Drug Administration. *Drug Supply Chain Security Act*. Accessed: Jun. 3, 2020. [Online]. Available: https://fda.gov

[14] State Food and Drug Administration of China. (Feb. 2016). *On suspension of drug electronic supervision system*. Accessed: Jun. 3, 2020. [Online]. Available: http://www.sda.gov.cn/WS01/CL0051/144782.html

[15] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "On the malleability of Bitcoin transactions," in *Proc. Financial Cryptography Data Secur.*, 2015, pp. 1–18.

[16] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of IoT data using smart contracts," *IET Netw.*, vol. 8, no. 1, pp. 32–37, Jan. 2019.

[17] K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain-based E-voting," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106583.

[18] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Comput. Electr. Eng.*, vol. 76, pp. 183–197, Jun. 2019.

[19] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://metzdowd.com

[20] M. Muniandy. O. Gabriel, and T. Ern, "Implementation of pharmaceutical drug traceability using blockchain technology," *Int. J.*, vol. 2019, p. 35, Jun. 2019.

[21] P. Olsen and M. Borit, "The components of a food traceability system," *Trends Food Sci. Technol.* vol. 77, pp. 143–149, Jul. 2018, doi: 10.1016/j.tifs.2018.05.004.

[22] A. Bougdira, A. Ahaitouf, and I. Akharraz, "Conceptual framework for general traceability solution: Description and bases," *J. Model. Manage.*, vol. 15, no. 2, pp. 509–530, Oct. 2019.

[23] K. Al Huraimel and R. Jenkins. (2020). *Smart Track*. Accessed: May 26, 2020. [Online]. Available: https://smarttrack.ae/

[24] *GS1 DataMatrix: A Tool to Improve Patient Safety Through Visibility in the Supply Chain*. Accessed: May 26, 2020. [Online]. Available: https://www.gs1.org/docs/healthcare/MC07_GS1_Datamatrix.pdf

[25] C. Faulkner. *What is NFC? Everything you Need to Know*. Accessed: Jun. 3, 2020. [Online]. Available: https://techradar.com

[26] C. Corrado, F. Antonucci, F. Pallottino, A. Jacopo, S. David, and M. Paolo, "A review on agri-food supply chain traceability by means of RFID technology," *Food Bioprocess Technol.*, vol. 6, no. 3, pp. 353–366, 2013.

[27] B. A. Supriya and I. Djearamane, "RFID based cloud supply chain management," *Int. J. Sci. Eng. Res.*, vol. 4, no. 5, pp. 2157–2159, 2013.

[28] S. M. K. Jamal, A. Omer, and A. A. Salam Qureshi, "Cloud computing solution and services for RFID based supply chain management," *Adv. Internet Things*, vol. 03, no. 04, pp. 79–85, 2013.

[29] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jun. 3, 2020. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[30] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[31] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 225. London, U.K.: Edward Elgar, 2016.

[32] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services*, Sep. 2016, pp. 1–3.

[33] J. Kurki, "Benefits and guidelines for utilizing blockchain technology in pharmaceutical supply chains: Case Bayer Pharmaceuticals," Bachelor thesis, Dept. Inf. Service Econ., Aalto Univ., Espoo, Finland, 2016.

[34] Y. Huang, J. Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in *Proc. IEEE Conf. Internet Things*, Jul./Aug. 2018, pp. 1137–1144.

[35] S. Delgado-Segura, C. Pérez-Solà, G. Navarro-Arribas, and J. HerreraJoancomartí, "Analysis of the bitcoin UTXO set," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), vol. 10958, A. Zohar, Ed. Berlin, Germany: Springer, 2019, pp. 78–91.

[36] F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics*, vol. 8, p. 505, Apr. 2019, doi: 10.3390/electronics8050505.

[37] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Gener. Comput. Syst.*, vol. 105, pp. 13–26, Apr. 2020.

[38] C. Hulseapple. (2015). *Block Verify Uses Blockchains to End Counterfeiting and Make World More Honest*. Accessed: Jun. 5, 2020. [Online]. Available: https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest

[39] C. Arsene. (2019). *Hyperledger Project Explores Fighting Counterfeit Drugs with Blockchain*. Accessed: Jul. 5, 2020. [Online]. Available: https://healthcareweekly.com/blockchain-in-healthcare-guide

[40] *The MediLedger Project*. Accessed: Jul. 5, 2020. [Online]. Available: https://www.mediledger.com/network

[41] *Farmatrust Technical Whitepaper (V3.0)*. Accessed: Jul. 3, 2020. [Online]. Available: https://www.farmatrust.com/

[42] *IPFS is the Distributed Web*. Accessed: Jun. 3, 2020. [Online]. Available: https://ipfs.io/.
[43] D. Ko, Y. Kwak, D. Choi, S. Song, Seokil, "Design of cold chain application framework (CCAF) based on IOT and cloud," in *Proc. 8th Int. Conf. U, e-Service, Sci. Technol.*, 2015, pp. 11–13.
[44] V. Buterin. (2013). *Ethereum Whitepaper*. Accessed: Jun. 5, 2020. [Online]. Available: https://ethereum.org/whitepaper/
[45] *Web3j Documentations*. Accessed: Jul. 17, 2020. [Online]. Available: https://docs.web3j.io/
[46] B. Badr, R. Horrocks, and X. Wu, *Blockchain by Example: A Developer's Guide to Creating Decentralized Applications Using Bitcoin, Ethereum, and Hyperledger*. London, U.K.: Packt, 2018.
[47] D. Blanchard, *Supply Chain Management Best Practices*, 2nd ed. Hoboken, NJ, USA: Wiley, 2019.
[48] *Supply Chain Optimization*, Exforsys, New York, NY, USA, Sep. 2007.
[49] *Eth Gas Station*. Accessed: Jun. 3, 2020. [Online]. Available: https://ethgasstation.info/
[50] *European Parliament and Council of European Union (2016) Regulation (EU)*. Accessed: Aug. 29. 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[51] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *Proc. 17th Int. Symp. Infoteh-Jahorina (INFOTEH)*, East Sarajevo, Srpska, Mar. 2018, pp. 1–6, doi: 10.1109/INFOTEH.2018.8345547.

**AHMAD MUSAMIH** received the B.S. degree in electrical engineering from United Arab Emirates University, United Arab Emirates, in 2015, and the M.S. degree in engineering systems and management from Khalifa University in 2018, where he is currently pursuing the Ph.D. degree in engineering systems and management. He is currently a Full Time Researcher and a Graduate Student with the Department Industrial Engineering, Khalifa University, where he is also a Research and a Teaching Assistant. His research interests include blockchain, healthcare, and supply chains.

**KHALED SALAH** (Senior Member, IEEE) received the B.S. degree in Computer Engineering with a minor in computer science from Iowa State University, USA, in 1990, and the M.S. degree in computer systems engineering and the Ph.D. degree in computer science from the Illinois Institute of Technology, USA, in 1994 and 2000, respectively. He was with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, for ten years. In 2010, he joined Khalifa University, where he is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. He is currently a Full Professor with the Department of Electrical and Computer Engineering, Khalifa University, United Arab Emirates. He has over 190 publications and three patents. He was also a recipient of the departmental awards for the Distinguished Research and Teaching in prior years. He is a member of the IEEE Blockchain Education Committee. He serves on the Editorial Board of many WOS-listed journals, including *IET Communications*, *IET Networks*, Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS, and AJSE. He was a recipient of the Khalifa University Outstanding Research Award 2014/2015, the KFUPM University Excellence in Research Award of 2008 and 2009, and the KFUPM Best Research Project Award of 2009 and 2010. He is the Track Chair of the IEEE Globecom 2018 on Cloud Computing. He is an Associate Editor of the IEEE Blockchain Newsletter. He has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of Blockchain, IoT, Fog and Cloud Computing, and Cybersecurity.

**RAJA JAYARAMAN** received the bachelor's and master's degrees in mathematics from India, the M.Sc. degree in industrial engineering from New Mexico State University, and the Ph.D. degree in industrial engineering from Texas Tech University. His Postdoctoral Research was on technology adoption and implementation of innovative practices in the healthcare supply chains and service delivery. He is currently an Associate Professor with the Department of Industrial and Systems Engineering, Khalifa University, Abu Dhabi, United Arab Emirates. He has led several successful research projects and pilot implementations of supply chain data standards in the U.S. healthcare system. His research interests include application of blockchain technology, systems engineering, and process optimization techniques to characterize, model, and analyze complex systems with applications to supply chains, maintenance planning, and healthcare delivery.

**JUNAID ARSHAD** received the Ph.D. degree in computer security from the University of Leeds, U.K., in 2011. He is currently an Associate Professor with the School of Computing and Digital Technology, Birmingham City University, U.K. He has been actively involved in publishing high-quality research within cybersecurity and has successfully published at high-quality venues, including journals, book chapters, conferences, and workshops. His research interests include investigating security challenges for diverse computing paradigms, such as distributed computing, cloud computing, the IoT, and distributed ledger technologies. He regularly serves on program and review committees of several journals and conferences. He is an Associate Editor of the *Cluster Computing* and IEEE Access journals.

**MAZIN DEBE** received the B.Sc. degree in computer engineering and the M.Sc. degree in electrical and computer engineering from Khalifa University, Abu Dhabi, United Arab Emirates. He is currently with the Center for Cyber-Physical Systems, Khalifa University, as a Research Associate. He has authored or coauthored four research articles in highly ranked IEEE conferences and journals. His research interests include blockchain technology, the Internet of Things, fog computing, and supply chain applications.

**YOUSOF AL-HAMMADI** received the bachelor's degree in computer engineering from Khalifa University (previously Etisalat College of Engineering), Abu Dhabi, United Arab Emirates, in 2000, the M.Sc. degree in telecommunications engineering from the University of Melbourne, Australia, in 2003, and the Ph.D. degree in computer science and information technology from the University of Nottingham, U.K., in 2009. He is currently an Acting Dean of graduate studies and an Assistant Professor with the Department of Electrical and Computer Engineering, Khalifa University. His main research interests include the area of information security, such as intrusion detection, botnet/bots detection, viruses/worms detection, machine learning and artificial intelligence, RFID security, and mobile security.

**SAMER ELLAHHAM** received the bachelor's degree in biology and the M.D. degree from The American University of Beirut, Beirut, Lebanon. He finished his internal medicine residency at the Georgetown University Hospital, Washington Hospital Center, Washington, DC, USA, and his fellowship in cardiology at the Virginia Commonwealth University Health System, USA. He was with the Georgetown University Hospital, Washington Hospital Center, and in several clinical and held leadership positions. He moved to United Arab Emirates in 2008. He is currently with Cleveland Clinic Caregiver, Cleveland, USA, as a Senior Cardiovascular Consultant and the Director of Accreditation with the Quality and Safety Institute, Cleveland Clinic Abu Dhabi. He is a member of MD, CPHQ, and EFQM, and a Fellow of ACMQ, ACP, ACC, AHA, and CCP. He is the Middle East Regional Chair, an ISQua Expert of the Patient Safety Movement Foundation, and a member of the AHA Hospital Accreditation Science Committee, the European Society of Cardiology Heart Failure Writing Group, the ex-Middle East Representative of the JCI Standards Subcommittee, and the American College of Cardiology Accreditation Foundation Board.

He is the Eminent Editor of the *Journal of Cardiology & Cardiovascular Therapy* and an Associate Editor of the *American Journal of Medical Quality*. He serves on the Editorial Board of the *Journal of Clinical Cardiology and Cardiovascular Research*, *Developments in Clinical & Medical Pathology*, the *Joint Commission Journal on Quality and Patient Safety*, *Telehealth and Medicine Today*, *Blockchain Journal*, *Medical Science*, the *Open Journal of Cardiatic Research*, the *UPI Journal of Pharmaceutical, Medical and Health Sciences*, *Open Access Research in Anatomy, Gerontology & Geriatrics studies* and the *Open Access Journal of Clinical Trials*, *Hypertension Today Journal* and *Focus on Hypertension Journal*, the *Journal of Heart Health, Cardiovascular Pharmacology, Scientific Research, and Community*, the *Journal of Surgery and Surgical Procedures*, *EC Cardiology*, the *Journal of Cardiovascular and Pulmonary Medicine*, the *Canadian Journal of Biomedical Research*, the *American Journal of Research in Medical Sciences*, and the *International Journal of Open Medicine and Surgery*.