IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 21, 2020, accepted November 8, 2020, date of publication November 11, 2020,
date of current version November 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3037363

Blockchain-Based Verifiable Tracking of Resellable Returned Drugs

MAZIN DEBE[1], KHALED SALAH[1], (Senior Member, IEEE), RAJA JAYARAMAN[2], AND JUNAID ARSHAD[3]

[1]Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates
[2]Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates
[3]School of Computing and Digital Technology, Birmingham City University, Birmingham B4 7XG, U.K.

Corresponding author: Mazin Debe (mazin.debe@ku.ac.ae)

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

ABSTRACT An enormous amount of drug supply is regularly wasted due to several reasons related to incorrect prescription, purchase of unnecessary quantities, drug intolerance, allergy, or interactions. On the other hand, these medicines may be needed by patients who cannot afford to purchase them. To address this challenge, we propose a fully decentralized solution that governs the return and redistribution of unused drugs that are fit for usage. Our approach exploits the decentralized blockchain technology, smart contracts, and decentralized storage systems such as the Interplanetary File Systems (IPFS). We develop a system that provides the ability for customers as well as pharmacies to return re-usable, resellable drugs for donation or resale at a lower price. The proposed scheme tracks the production of drugs from manufacturers to traders that subsequently sell them to customers. Unused drugs can be returned after approval by specialized entities and then redistributed. In particular, we present the decentralized system architecture and implement a prototype on a test Ethereum blockchain platform to present the suggested workflow. Further, we provide system evaluation focused on assessing system functionality, performance, execution cost, and security of smart contracts and their robustness. We have also made our smart contracts code publicly available on Github. [1].

INDEX TERMS Blockchain, ethereum, healthcare, returned drugs, trustworthy tracking.

I. INTRODUCTION

Tracking drugs is a vital feature to ensure the trusted and safe delivery of medicine in-line with acceptable conditions. The life cycle of a typical medicine starts with the manufacturers that produce lots or batches of drugs. These lots are then processed through multiple entities ending with traders that sell these drugs to customers. This supply chain undergoes several changes of ownership until drugs are sold to a customer, with the process being recorded to track the medicine from its origin until it has been sold. However, the prescribed drugs may not be consumed due to several reasons such as change of dosage advised by the doctor, change in the course of treatment, or allergic reactions, etc. leading to drugs that are no longer needed by the patient. Ideally, these drugs should be passed along to other patients that would benefit from them. However, this process is not easy to manage as these drugs need to be examined by appropriate authorities and proven to be fit for further use before being made available for redistribution. The redistribution of unused, safe medicine for a lower price or for free can save the lives of many patients who cannot afford medication, especially in countries where such drugs are expensive [1]. Moreover, this process can save millions of dollars annually in medicine that otherwise would have just gone to waste as well as a positive impact on the environment as most unused medicines are often disposed of in garbage cans or water bodies.

A system for tracking unused drugs and validating their condition typically requires a centralized server to trace each medicine as it is transferred between different stakeholders. These stakeholders include manufacturers, distributors (pharmacies and hospitals), and customers. Although this central authority tracks the medicine journey, it suffers from major drawbacks. For instance, there are security and privacy concerns regarding centralized systems as they are always susceptible to being attacked and compromised. A decentralized approach, such as using the blockchain technology,

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

[1]https://github.com/MazenDB/ReturnedDrugs

eliminates the dependency on a central server to track the delivery of medicine. A blockchain is a decentralized ledger that records transactions in a tamper-proof manner. Some blockchain networks employ a smart contract, which is a piece of code deployed on the blockchain used to implement arbitrary logic customized by the user. Smart contracts can be used to trace the drug from manufacturing to sale and to record the return of drug packages, approve and re-sell them to new customers.

A conventional drug supply chain can track medicines throughout its journey, i.e., from the manufacturer to the distributor and from the distributor to a pharmacy or a hospital/medical center. However, employing blockchain extends this functionality to expand the chain of custody to include the consumers of this medicine, where it can record the purchase of any medicine along with the customer and prescription details. By doing so, blockchain can also provide patients the ability to re-sell or donate unused medicine back to the distributor. This approach provides an immutable history for the medicine from dispatching the original lot by the manufacturer until a seller collects it. Furthermore, the blockchain ledger holds records that show when a drug package was returned, approved, and re-sold while ensuring that all returned packages are sealed, tamper-proof, and safe to use condition. The major contributions of this article are:

- We propose a decentralized system leveraging the blockchain technology to facilitate the safe and secure return and redistribution of unused drugs. The solution engages all relevant entities to ensure that the process of retaking, approving, and re-selling drugs is safe and certified by authorized members.
- Utilizing blockchain capabilities, we present an automated method to choose a reseller through an auctioning mechanism. In addition, we provide a way for patients to give feedback about the resellers based on their performance.
- We provide implementation details for the system functionality on the Ethereum blockchain. We present the sequence of interactions for purchasing, returning, and resale of the unused drugs as well as selecting and evaluating resellers. This implementation is achieved through a virtual blockchain platform using Remix IDE.
- We present detailed system evaluation focused on assessing system functionality, performance, execution cost, and security of smart contracts and their robustness. Different scenarios were investigated and presented to assess the feasibility of the solution. We also compare our approach to existing solutions and highlight challenges that remain for the effective adoption of the proposed solution in wider domains.

The remainder of the article is organized as follows: Section II explains the concept of blockchain and smart contracts. Section III presents a critical overview of the related work. Section IV presents the proposed approach for the returning and resale of unused drugs. Section V explains the implementation details followed by section VI which demonstrates the smart contract testing results. Section VII presents an analysis and evaluation of the proposed approach. Section VIII concludes the article.

II. BLOCKCHAIN BACKGROUND

Blockchain is a distributed ledger technology that gained popularity from one of the most common cryptocurrencies, the Bitcoin [2]. The blockchain can be viewed as a system of interconnected peers that share the same state machines. Members of the blockchain network transact information between each other, and these transactions are grouped together to form a structure called a block. Each block consists of numerous transactions that are assembled and appended to the existing list of blocks by blockchain miners. Blocks are mined and agreed upon among the blockchain network participants following a consensus protocol. A variety of consensus protocols have been proposed to determine the behavior of the blockchain network [3]. Various consensus protocols follow different approaches to reach an agreement on which miner validates and aggregates transactions into a block that is then acknowledged by other members of the network. This block is broadcasted to the entire peer-to-peer network and replicated at all nodes to store a common public state of the blockchain.

A blockchain can be public or private, depending upon the use-case involved. Both private and public blockchains have been gaining a lot of popularity due to their infinite applications. Extensive research has been conducted to study the application of blockchain in the fields of IoT, AI, Supply Chain, and Fog Computing, as it can be seen in these articles. [4]–[7]. The pharmaceutical supply chain, in specific, is one of the most suitable applications for blockchain. Introducing a distributed ledger to handle tracking drugs has several beneficial advantages [8]. By nature, blockchain is an immutable record of transactions, and hence, all interactions captured are permanent, persistent, and tamper-proof. Hence, the drug delivery process that utilizes the blockchain technology will be secure, and the quality of service provided to patients is required to meet a certain standard. Blockchain can restrict access of information to certain members of the network (through permissioned blockchain model), which ensures the integrity of data.

Some blockchain networks deploy smart contracts to implement customizable business logic. Smart contracts are passive elements used in blockchains such as Ethereum and Hyperledger to achieve numerous functionalities. For easier usage of the blockchain, smart contracts are often deployed as back-end systems that communicate with decentralized applications (DApps) at the front-end. DApps offer a usable interface for users to interact with the blockchain layer. In the case of the drug supply chain, DApps can be used to transfer data about drug lots between different entities, sell drugs to patients, and return unused drugs via a simple logical interface.

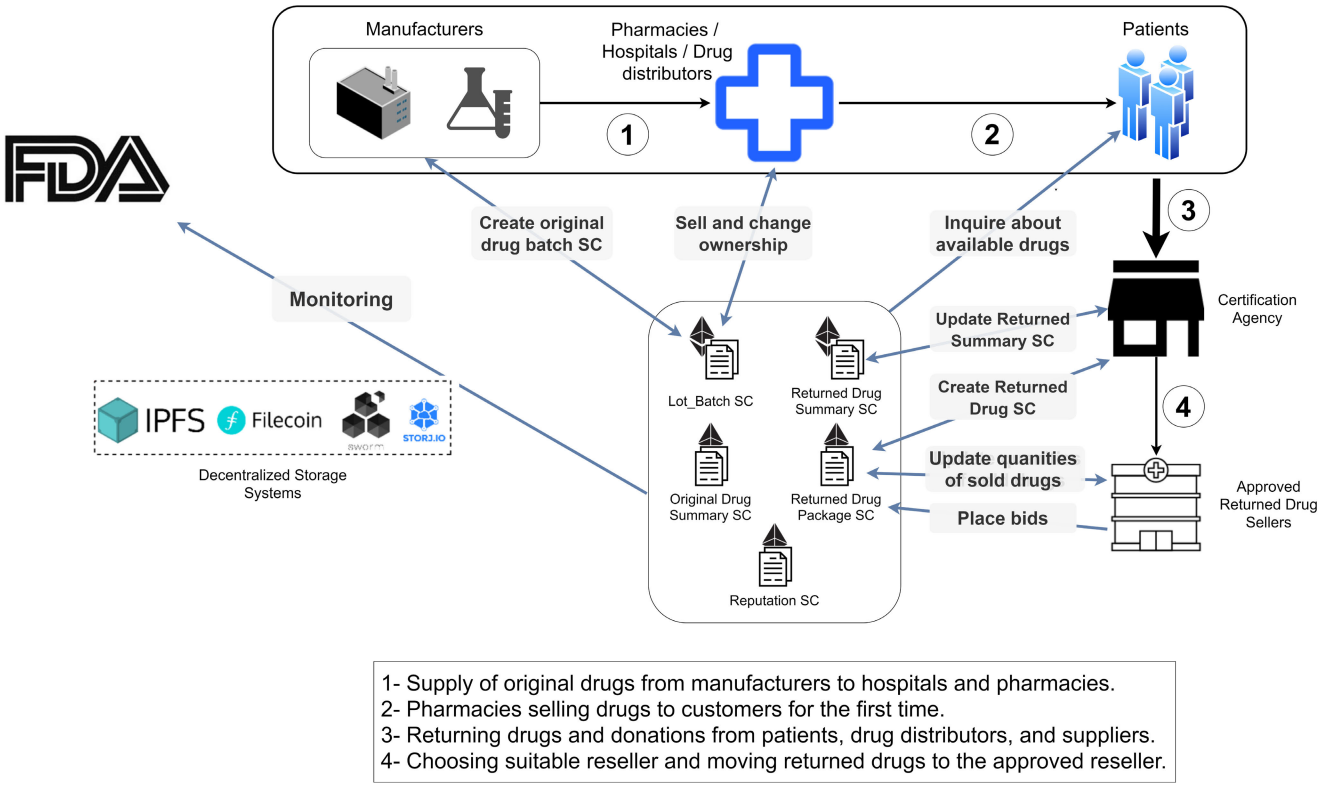

FIGURE 1. Proposed decentralized architecture for tracking returned drugs.

III. RELATED WORK

This section presents a critical overview of existing work done on drug delivery and tracking solutions. Most of these solutions utilize a central server to manage drug lots and re-usable packages. The blockchain technology is not used extensively in any of the mechanisms that enable patients to return unused drugs for redistribution.

The tracking of medicine from manufacturers to distributors is often achieved through well-established methods and tracking systems. Research in the food and drug supply chain industry has been an area of continuous development, as evident in some of the early research articles such as [9] that presented the traceability in the Agri-food Supply Chain and [10] that discussed how to streamline the supply chain in pharmaceutics. The latter presented clear shortcomings in the conventional decision-making process. These problems are consequences of a large number of stakeholders and the large inventory available and result in significantly inflating the process cycle time. Some solutions, such as introducing continuous processing, has been proposed to shorten this cycle time [11]. Nonetheless, the concept of centralization acts as a bottleneck in such a system.

Since the emergence of the blockchain technology, notable efforts have been made to exploit it to achieve drug tracking as an alternative to the current systems. The authors in [12] present a blockchain-based solution called Drugledger. Their model achieves the privacy and authenticity of data by breaking down the service providers into separate entities. Another solution presented a blockchain-based supply chain to establish trusted medical records for drugs and patients [13]. These records can be accessed for a limited time only. Trace and Track is another model developed to store records of medicine [14]. It combines an IoT framework with blockchain to introduce trust into a trust-less interaction between stakeholders and fight counterfeit drugs. Some real-life applications have also been developed to deploy the blockchain for pharma supply chain management. Good Shepherd pharmacy in the US and its sister company RemediChain developed a blockchain platform that manages the donation of unused drugs [15]. Another solution that utilizes blockchain for the medical supply chain is modum.io [16], which uses the blockchain along with IoT devices to store medicine records efficiently and securely.

The majority of the existing traditional solutions use a centralized server to manage the pharmaceutical supply chain. In contrast, we are proposing to use a decentralized approach to eliminate the need for a centralized entity, thereby maintaining data integrity, privacy, and security. Several other presented solutions utilize the blockchain technology but target different aspects of the medicine supply chain. These applications offer mechanisms for drug traceability, detecting counterfeit drugs, preventing fraud, and other applications. However, none of this work proposes a way to return unused drugs, validate them, and sell them to patients. On the other hand, one of the main contributions of our solution is suggesting a mechanism to accept returned drugs by certified agencies that offer them for resale. Undoubtedly, this is

implemented in a decentralized manner on the blockchain via Ethereum smart contracts.

IV. PROPOSED APPROACH

Fig. 1 presents a high-level architecture for our proposed system that tracks the journey of medication from its origin to the purchase by consumers. This supply chain has attracted attention from existing work; however, our proposed architecture connects all stakeholders via the blockchain network that cryptographically records all transactions. Several blockchain networks can be utilized for the use-case of this approach. These include the Ethereum network, both private and public, Hyperledger Fabric, and Multichain. While some parts of the supply chain can be implemented to be private, most of the smart contract data need to be available publicly. The blockchain network chosen in our solution is the public Ethereum blockchain. Ethereum is a public blockchain that supports smart contracts written in Solidity language. This network is suitable as the data should be publicly available for all members to check and verify. Nevertheless, each entity has specific privileges and is given the authority to a specified set of methods that it can invoke. For example, the Food and Drug Administration (FDA) is considered the highest level of authority and can access all information in the system. Each of these members is identified in the blockchain to other nodes by a 20-byte Ethereum Address that is linked to all of its relevant data.

The tracking of drugs begins when a manufacturer prepares drugs and medications according to orders received from hospitals, pharmacies, or any drug distributor. After manufacturing the drug lot or batch and performing testing on the generated drugs, the manufacturer updates a summary smart contract of the drug batch. This contract holds all the information about approved drugs, manufacturers, and sellers. The manufacturer also uploads an image of the lot to a decentralized storage system such as the InterPlanetary File System (IPFS). The drug is identified in the summary contract by a drug code. The lot is approved if the manufactured drug is registered and validated according to the summary contract.

After the drug lot has been approved, a new smart contract is created for that lot. The smart contract is identified by a unique address and contains information about the drug, including its name, date of expiration, price, and the number of boxes in the lot. The required quantity from the lot is shipped to the retailer and then sold to patients individually. Whenever a sale takes place, the seller updates the smart contract by providing the box number that was sold. This is done to help verify the source of the box if this box is returned. With the sale of a drug box, the blockchain no longer tracks the movement of the drug box.

If a customer wishes to return the medicine at a lower price or donate it, the customer returns the medicine to a certification agency that manages redistribution. In addition, both manufacturers and drug sellers can provide these drugs for resale. These agencies that receive returned or donated drugs are certified by the government to approve drugs eligible for resale. The certification agency verifies the suitability of the drugs for resale, which includes various assessments including confirmation of the shelf life of the medicine, verifying that the packaging is still sealed, and that it was stored in appropriate conditions including temperature, luminosity, and humidity etc. Satisfactory completion of these assessments means that the medicine is considered fit for usage. In addition to certifying drugs, the certification agency creates a new smart contract for the returned package containing relevant data referring to the origin of the drug as well as new data. Furthermore, the certification agency updates the returned drug summary smart contract with the new address of the returned package. The certification agency also uploads a new image of the repackaged drug to the decentralized storage system.

The selection of a drug reseller to receive the drug package is made through an auctioning mechanism. A reseller offers the returned drugs at a lower price or donates them depending on the previous owner's request. Patients can then review these drugs and can purchase them at lower prices or for free. The certification agency starts an auction with its preferred parameters, including the starting price and the closing time for the auction. Approved resellers can place bids in this auction to get the returned package. In order to distinguish good resellers, each one is given a reputation score. A certification agency can enforce a minimum reputation score for auctions to ensure the desired quality of service. After the transaction with the patient, the patient provides its feedback to the reputation smart contract, which updates the reputation score of the reseller.

As blockchain is an immutable ledger, certification agencies, as well as customers, can trace the history of each drug and the change of ownership throughout its life cycle. This can be achieved by exploring transactions and events to and from the smart contract, which are permanently stored on the blockchain. For instance, if at any point in the life cycle of the medicine, a medication is discovered to be spoiled or damaged, the last entity to approve the quality of the products is to be held responsible. Therefore, all members are forced to perform appropriate tests on the goods to avoid any repercussions, either financially or the credibility of the entity among the members of the network. Moreover, all certification agencies and drug resellers are envisaged to be certified to ensure trust in the process of returned drug validation.

The pharmaceutical supply chain consists of several stakeholders, where primary elements are elaborated below.

- **FDA:** To monitor drug suppliers, pharmacies and healthcare centers, and any entity involved in the process of producing and selling drugs, a central authority is essential. The FDA is a federal agency in the United States responsible for maintaining public health by monitoring and controlling the production of foods and pharmaceutical drugs. The FDA authorizes drug prices, sales, as well as certification agencies, and drug resellers. Furthermore, it has privileged access to all

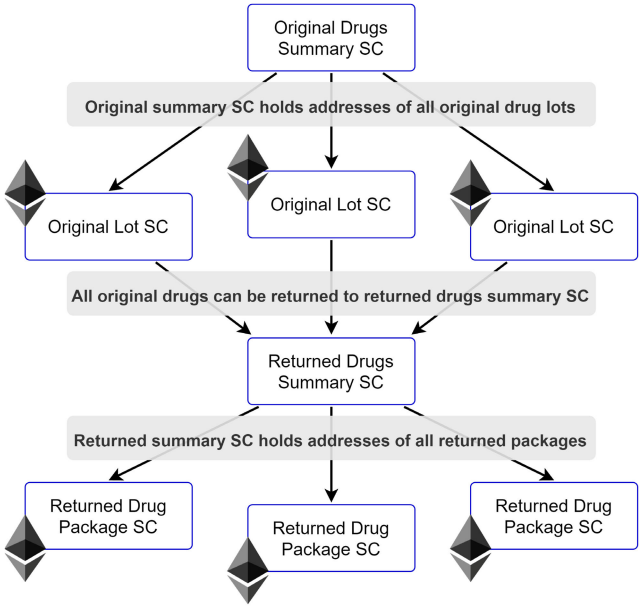

FIGURE 2. Smart contract structure design.

methods and data in the smart contract, which all other entities may not have.

- **Manufacturers:** Manufacturers initiate the supply chain and produce drugs in lots in order to ship them to retailers. Manufacturers create a smart contract for each new lot and provide the summary smart contract with the new lot address. This new smart contract is considered the original smart contract of a new drug and contains all the information about the lot. Manufacturers also upload images of the produced package to IPFS.
- **Drug Distributors:** These include pharmacies, hospitals, healthcare centers, and wholesalers that receive drugs and present them for sale. Drug Distributors are the original drug sellers before patients return it. They update the relevant lot smart contract when selling a drug package to a customer.
- **Patients/Customers:** The customers that approach the pharmacies and hospitals to purchase drugs are a key element in our system as they are the source of the unused medicine that is returned. These customers are recorded when purchasing medicine and also upon returning that medicine and are identified by a unique address. It is noteworthy that patients do not need to have an Ethereum Address as they are not Ethereum clients and do not interact with the smart contracts.
- **Certification Agencies:** These are government-entrusted entities assigned to validate and authorize the redistribution of resellable, returned drugs. To approve the resale of drugs, these agencies can check for broken seals, expiry dates, storage conditions, and perform the necessary tests to ensure the viability of the drugs for usage. Any medication that is suspected to be tampered with and/or unfit for usage is not approved.
- **Resellers:** They are members approved by the FDA to receive certified drugs for resale and redistribution. Resellers can sell these drugs at a much lower price or even donate them to specific entities as it sees fit. These entities can participate in auctions placed by certification agencies to acquire re-usable drug packages.
- **Smart Contracts:** The interaction between all those presented entities are governed by Ethereum smart contracts. Smart contracts are generated for each new lot of drugs being produced as well as for each returned drug package. In addition, a smart contract exists that holds a summary of all original drugs as well as one for returned drug packages. Only one of each drug summary smart contracts is deployed on the blockchain; however, original lot and returned package contracts are dynamically by manufacturers and certification agencies, respectively. The original summary contract verifies manufacturers, sellers, produced drugs, and original lot smart contract Ethereum addresses. The returned drug summary contract keeps track of approved certification agencies and resellers as well as Ethereum Addresses of returned packages. The original lot contract, on the other hand, only handles transactions related to that lot, and the same applies to the returned package smart contract. Moreover, the latter also governs the auction for selecting resellers. The last smart contract is the reputation contract that updates resellers' reputation scores according to their performance.
- **Decentralized Storage:** The images of original drug lots and returned drug packages have to be securely stored. A database system cannot be used in this system as it is inconsistent with the decentralization of the blockchain. This poses a vulnerability in the system that is overcome by decentralized storage. Solutions such as IPFS and Filecoin can be used to store these images and communicate with the blockchain in a decentralized manner.

V. IMPLEMENTATION OF BLOCKCHAIN-BASED SOLUTION

This section discusses the implementation details of the aforementioned approach in addition to the application use-case.

A. IMPLEMENTATION OF ALGORITHMS

We implement the system architecture presented in the previous section on a virtual Ethereum network for proof of concept. The deployment utilizes the online development environment, Remix IDE. Remix IDE supports solidity language for smart contract testing.

Fig. 2 reflects the design of the smart contract structure in our implementation. Smart contracts are divided into four types: Original summary smart contract, Lot smart contract, Returned drug summary smart contract, and returned package smart contract. Following is a brief explanation of each of these contracts.

1) **Original summary smart contract:** The rules and regulations of the pharmaceutical supply dictate the

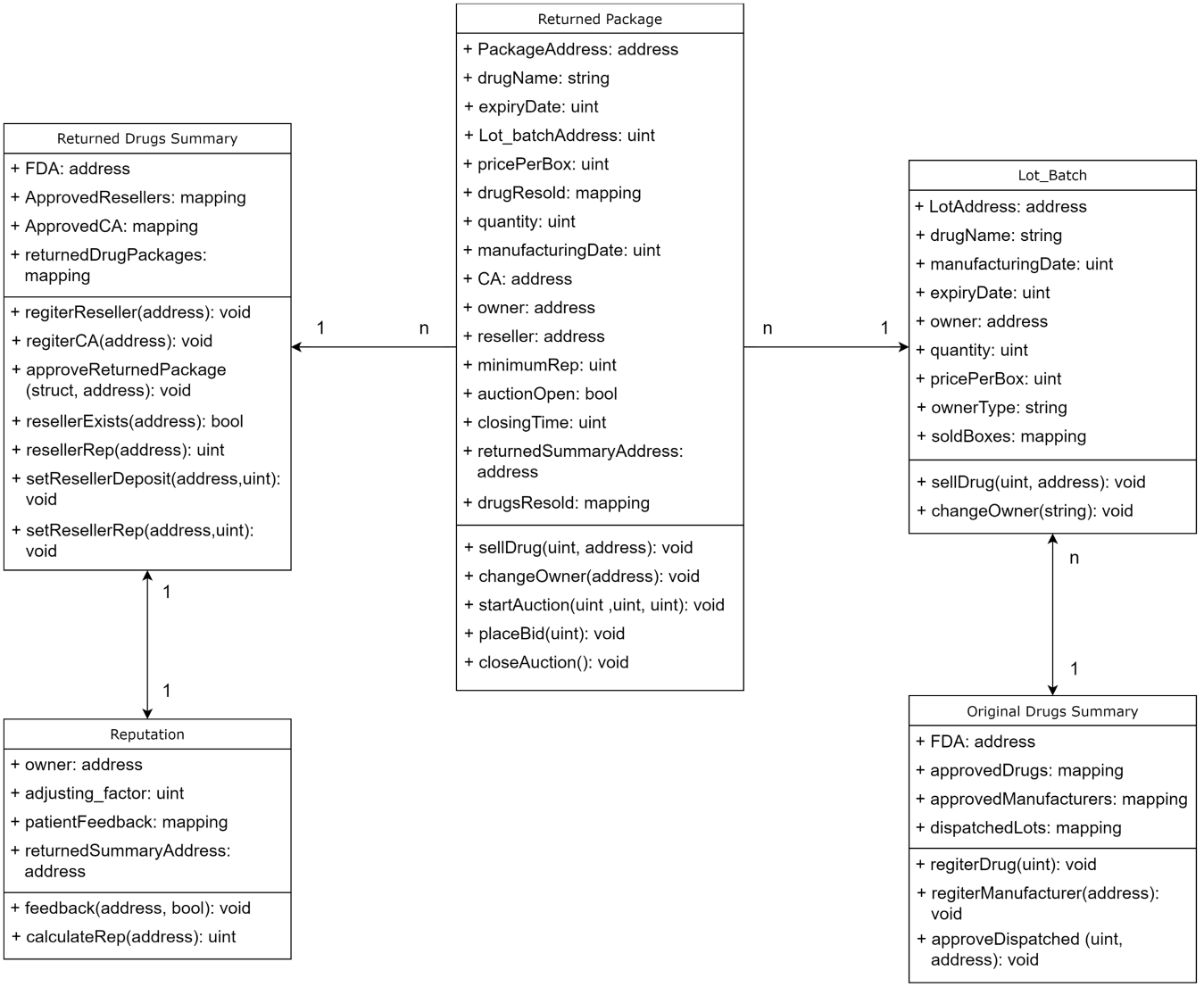

FIGURE 3. Relationship between different entities of the smart contract.

entity responsible for managing various stakeholders. Typically a governmental or federal agency, such as the FDA, creates one summary smart contract. This contract is accessed to register manufacturers and sellers of drug lots in the original supply chain. In addition, the drug manufactured should have been previously approved by the FDA for production and distribution. However, the summary contract does not hold details of each lot after being dispatched to avoid redundancy.

2) **Lot smart contract:** For each drug lot, a new smart contract is created by the manufacturer of the lot to track the boxes within it. This type of smart contracts represents the original drug contract before returning by patients. The lot contract tracks the drug lot as it moves from one owner to the next. When a drug package is sold, the seller sends a transaction to the corresponding lot contract to update its records.
3) **Returned drug summary smart contract:** When drug packages are returned, the returned drug summary smart contract is informed. This smart contract is deployed once to keep track of all certification agencies and approved drug resellers. It is deployed by the same authority that created the original summary smart contract. This smart contract can be considered the parent contract for all re-usable drugs. When a drug package is returned, the returned drug summary contract is consulted to validate the certification agency and the appointed reseller.
4) **Returned drug package smart contract:** For each drug package that a patient returns, a new smart contract is created to capture the details of the returned package. This smart contract is deployed by the certification agency that approved its redistribution. The smart contract is updated whenever the drugs from that packaged are re-sold. This smart contract also handles selecting returned drug resellers.
5) **Reputation smart contract:** This is a separate smart contract that manages the reputation score for approved

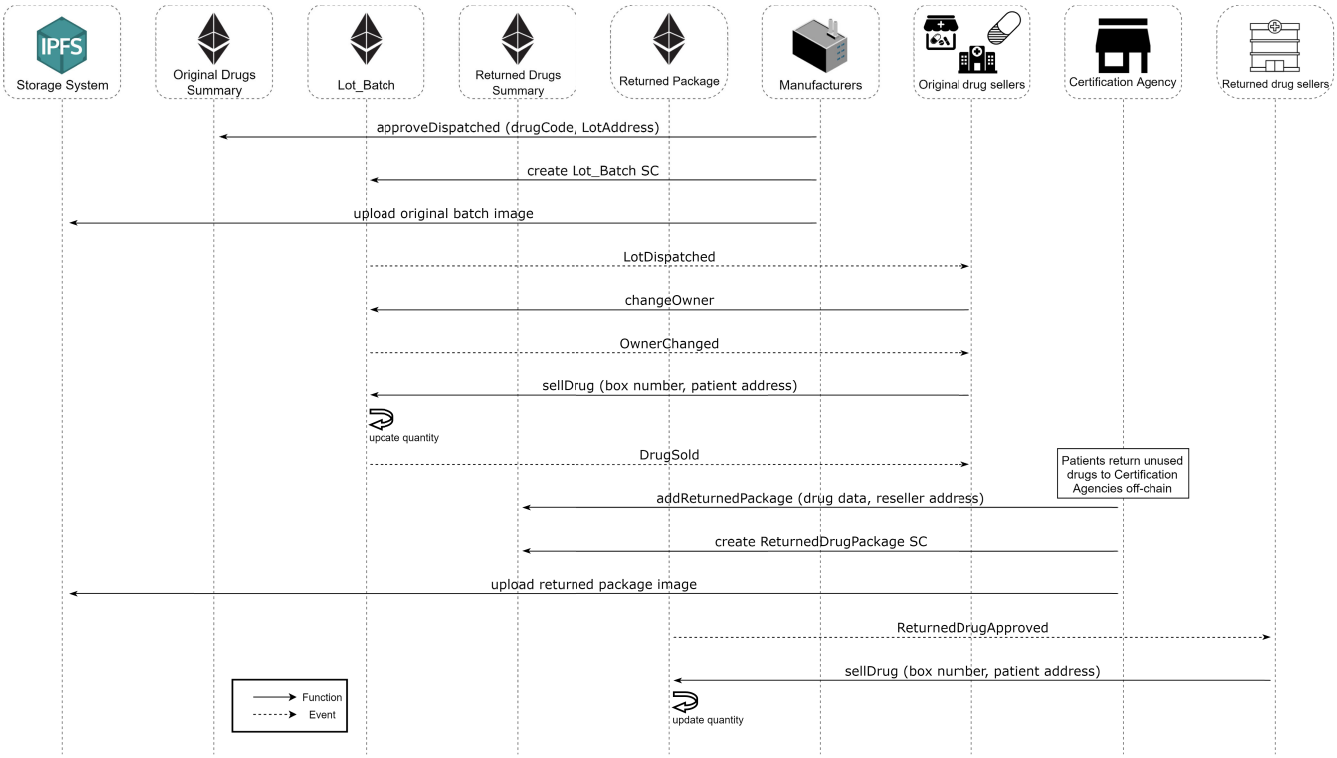

FIGURE 4. Interactions showing the function calls for purchase, returning and resale of drugs.

resellers to ensure honesty and quality of service. The reputation smart contract, like the summary contracts, is the responsibility of the agency that overlooks the supply chain.

Fig. 3 shows the various smart contracts that interact together and how they are related to each other. When a new lot of drugs is created by a manufacturer for the first time, it creates a new instance of the lot contract for it. All operations related to that batch of drugs go through the lot contract. This lot is identified by a unique Ethereum address given to the smart contract. This address is linked to data the drug name, its current owner, price of each box, the number of drug boxes it contains, manufacturing, and expiry date. In addition, this smart contract keeps track of all sold boxes. The addresses of all lot smart contracts are recorded in the original summary contract. Moreover, the returned package smart contract is created upon returning a drug from any lot. Multiple drugs can be re-sold from the same lot and given different Ethereum addresses. When the drugs are admitted for resale, it is given a new price and new seller based on an auction-based selection algorithm. This smart contract contains this information, as well as the address of the original lot and the address of the certification agency that approved it. Besides creating this contract, the returned drug summary contract is also updated. This summary smart contract keeps track of all approved certification agencies, resellers, and returned packages in one place. All returned packages need to be added to this summary contract. To establish trust in resellers, patients provide their feedback on the interaction with the reseller, both positive and negative. This directly affects a reputation score that is managed by the reputation smart contract. This contract modifies the reputation score of resellers according to their behavior.

Fig. 4 presents the interactions between smart contracts and different entities on the blockchain that lead to adding, selling, retaking, validating, and re-selling drugs. The manufacturer is the owner of the original lot contract, and it is responsible for creating a new instance for each new lot produced and requesting approval for dispatching the lot from the original summary smart contract. This summary contract validates the drug being produced and the manufacturer creating the lot smart contract. Manufacturers also add images of the original lot to the decentralized storage system. Once the lot has been dispatched, the ownership changes through the supply chain until it reaches the final drug sellers. When a pharmacy or a hospital sells a drug box to a patient, it updates the relevant lot smart contract. After the purchase, the patient can return the drug to a certification agency off-chain. Once an authorized agency approves the medicine, the drug is admitted, and the agency adds that drug package to the returned drug summary contract. This contract validates the agency, the reseller, and the package data. Then, a returned drug package contract is created, and an image of the returned package is uploaded to the storage system by the certified agency. The drug is then transferred to the approved reseller for redistribution. Whenever the reseller sells a drug box, it updates the drug package contract.

Fig. 5 presents the sequence of messages that lead to select an appropriate reseller and validate its integrity. It starts with the commencement of an auction by the certification agency.

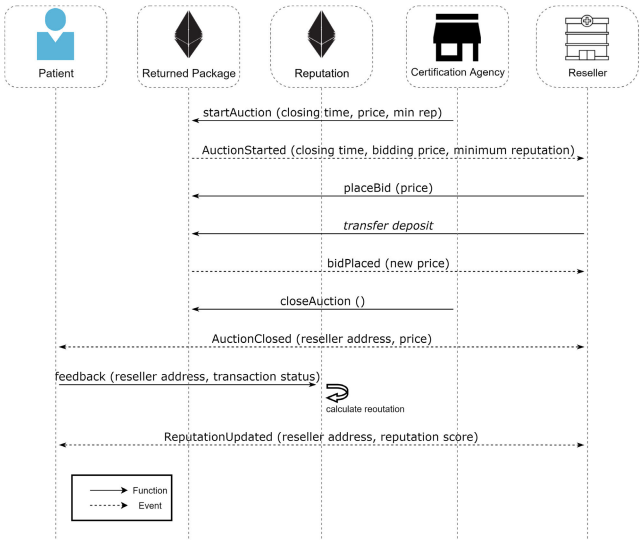

FIGURE 5. Interactions showing the process of choosing a reseller and updating reputation score.

The auction has specific parameters set, such as the price to start bidding at and the minimum required reputation for resellers to bid. The auction is announced via an event that is triggered by the returned package smart contract. Resellers that are interested in acquiring the drug place increasing bids and transfer deposits to ensure their commitment. The certification agency then closes the auction, and the last bidder gets the drug package. When the drug gets sold eventually, the patient can provide its feedback to a reputation smart contract. This contract records the feedback and computes the new reputation score internally, as explained earlier in the Implementation section. Then, the reputation score is updated and announced to all entities.

The tracking of drugs in our solution consists of two main parts: the original drug supply and the returned drug validation. The pseudocodes for these two processes are represented in algorithms 1 and 2, respectively. These algorithms provide a brief explanation of the smart contract code at a higher level as opposed to the aforementioned Solidity code. The first algorithm starts with the production of every drug lot. The manufacturer of this lot deploys an original lot contract, uploads the drug lot image to the decentralized storage system. The ownership of the drug lot then changes from the manufacturer to the next entity as the drug lot moves through the supply chain and is claimed by different members until it reaches a retailer. Hospitals and pharmacies that sell the drug boxes to end users update the relevant smart contract after each transaction.

Similarly, algorithm 2 represents the process of returning a drug package by a customer. The same logic applies when donating drugs by a customer, a retailer, or even a wholesale distributor. The drugs are supplied to a certification agency that informs the summary contract and creates a new returned package smart contract. This agency provides the package to a reseller that updates said smart contract whenever a customer purchases a returned drug.

Algorithm 1 Dispatching of Original Drug Lots

Input: drug data, drug code, lot address
Modifier: onlyManufacturer
Send drug data to the original drug summary contract.
if *drug code is valid* $\wedge$ *manufacturer is approved* **then**
    Authorize dispatching of Drug lot and commit to the original summary contract.
    Create the original drug lot contract on the blockchain.
    Manufacturer uploads the drug lot image to the decentralized storage system.
    Change ownership of lot until the acquisition by a seller via the lot smart contract.
    Sell Drugs to patients using the smart contract.
    Update the quantity in the smart contract.
else
    Revert.
end

Algorithm 2 Returning and Resale of Drug Package

Input: drug data, reseller address
Modifier: onlyCertificationAgency
if *drug is approved by CA* **then**
    Send drug data to the summary contract.
    if *CA address is verified* $\wedge$ *reseller address is verified* **then**
        Add Returned Drug Package to the summary contract.
        Create a returned package contract.
        Upload repackaged drug image to the decentralized storage system.
        Choose a reseller to receive the package
        Transfer re-usable package to the selected reseller.
        Selling Drugs.
        Updating quantity in returned drug package SC.
    else
        Revert.
    end
else
    Revert.
end

The process of choosing a reseller is done using an auction mechanism. The returned summary contract has a list of approved resellers that are allowed to sell re-consumable drugs. Once a drug is returned, and a certification agency approves it, it starts an auction that allows the resellers to possess this resellable package and sell it as shown in algorithm 3. It starts by opening the auction and announcing to all resellers that it is open for bidding. The resellers compete by offering an increasing price that they believe that they would still gain profit from selling. The certification agency could also put an upper price cap on the price for the interest of the

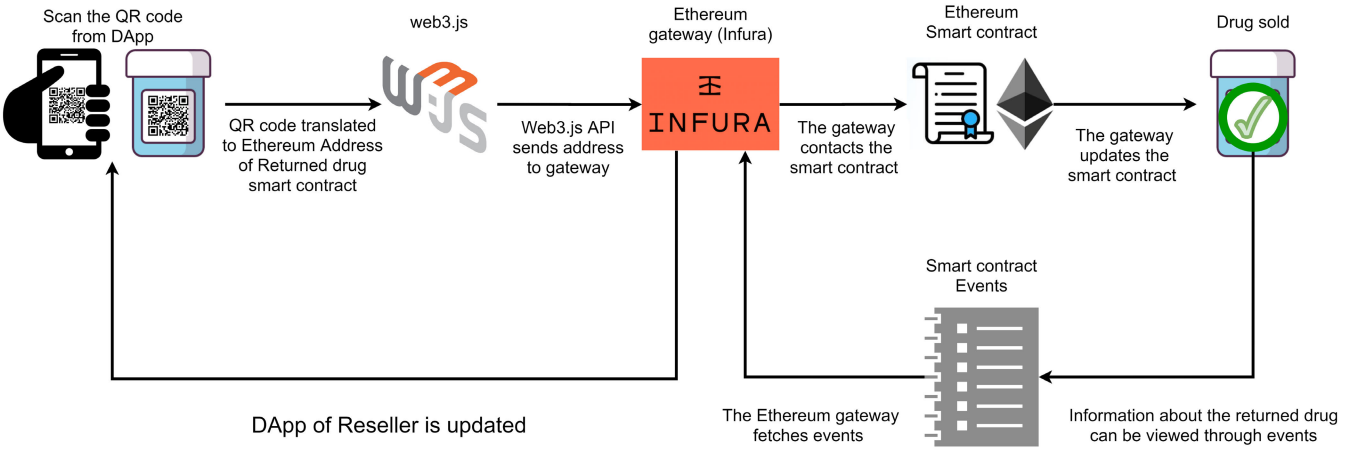

FIGURE 6. Utilizing the DApp of the blockchain-based solution to purchase reusable drugs.

customers. When a bidder offers a price, they transfer that amount to the returned package smart contract that is being auctioned as a deposit to ensure their commitment. After every new bid, the available deposit is returned to the previous bidder before accepting the new bid. The auction continues until the closing time. Upon auction closure, the winning bidder is announced, and the drug package is assigned to them. The available balance in the returned package smart contract belongs to the winning bidder. Therefore, that amount is transferred back to the corresponding reseller.

When certification agencies start an auction, they announce a starting price, a closing time, as well as a minimum reputation score, as shown in algorithm 4. Any reseller that wants to place a bid should satisfy the reputation requirements. After an interaction, a patient can inform the smart contract if a transaction was satisfactory or inadequate. Equations 1 and 2 below describe how the reputation score of a reseller, $Rep(t)$ is updated after good or bad feedback by a patient, respectively. The adjusting factor, AF, described, is an arbitrary measure of how forgiving the smart contract is. Changing this value results in causing the reward to become more generous or the punishment more severe. The constant values presented in addition to AF were designed to scale the reputation value up or down depending on the feedback. AF is recommended to be given a value of 2 or more. In our implementation, we give AF a value of 4, where we consider the raters to be trusted and would give an honest response. If the patients are considered to be not credible, this factor can be increased.

$$Rep = Rep + \frac{Rep * 0.95}{4 * AF} \tag{1}$$

$$Rep(t) = Rep(t-1) - \frac{Rep(t-1) * 0.95}{4 * (10 - AF)} \tag{2}$$

B. DECENTRALIZED APPLICATION

This section presents the process of utilizing the DApp by patients to purchase re-consumable drugs from approved resellers. The returned drug package is linked to a smart contract that contains all of its metadata, methods, and events. Any modification to the drug package is logged in this smart contract, which is identified by its unique Ethereum address. This address is translated to a QR code that is printed on the drug boxes for easier, more efficient transactions. Fig. 6 explains how to use DApps to sell drugs to patients. Initially, the QR code would be stamped on the drug box. Resellers scan them to get the Ethereum address of the relevant smart contract to contact in addition to the number of this box. The DApp uses the web3.js library to reach an Ethereum gateway such as Infura. This is an Ethereum client that communicates with the Ethereum blockchain on behalf of the user. Ethereum gateways such as Infura enable users to access the blockchain without being obliged to locally install full Ethereum nodes. Due to resource requirements of establishing a full Ethereum node, gateways such as Infura provide a light-weight solution for users to interact with the blockchain. Moreover, Infura supports libraries that are vital to communicate with Ethereum, such as the Web3.js API suite

Having the address of the smart contract, the gateway provides access to all of its methods and events. Therefore, the status of the smart contract can be modified, assuming it satisfies the access policy of the smart contract. In addition, the Ethereum gateway can access all the events emitted by the smart contract. The gateway then can update the user about any requested information. Accessing the information through an Ethereum client ensures the integrity of the data as it is stored in an immutable and permanent ledger. Moreover, the authenticity of the drug can be ensured by tracking the trail of events of ownership change from the Certification Agency. For even more verification, the original lot Ethereum address is included in the returned package smart contract. The history of the original ownership of the drug can be tracked using said address. This process is done without the interference of the user to automatically access smart contracts for sale and drug verification.

VI. TESTING AND VALIDATION

This section discusses the validation of the expected outcome for the implemented approach. The code for the solution

Algorithm 3 Selecting Reseller by Bidding

Input: closing time, start price, minimum reputation
Modifier: onlyReseller
if *Auction open already* **then**
    Set auction parameters.
    Set auction status as open.
    Announce the start of a new auction by triggering an event.
else
    Revert.
end
`/* Bidding starts by resellers. */`
if *The reseller is approved* $\wedge$ *reseller meets the minimum reputation requirements* $\wedge$ *auction is open* **then**
    Check the price offered by the reseller.
    if *price is higher than the previous bidder* $\wedge$ *the amount of ethers transferred is sufficient* **then**
        if *it is not the first bidder* **then**
            Transfer back deposit to the previous bidder.
            Change deposit of the previous bidder to zero.
        end
        Change the address of the highest bidder.
        Save deposit of new bidder.
    else
        Reject Bidder.
    end
else
    Reject Bid.
end
`/* Certification Agency requests auction closure */`
if *auction is open* $\wedge$ *closing time has passed* $\wedge$ *at least one bid has been placed* **then**
    Change the auction status to closed.
    Return deposit to the reseller.
    Announce the closing of the auction.
else
    Keep auction open.
end

was implemented, deployed, and tested on Ethereum using Remix IDE. Remix provides a test Ethereum network for deploying and testing smart contracts. Remix also has various plugins that support the debugging of the deployed code, performing unit testing, and conducting a sufficient performance analysis on the code. A log is generated and displayed for each transaction to simulate a real Ethereum network. These logs can be used to explore transactions as they include the inputs, outputs, events triggered, as well as the execution and transaction gas cost of the transaction. In addition, errors and exceptions are also displayed in these logs. Errors include exceeding the gas cost limit, run time errors, and restrictions enforced by the smart contract itself. Such constraints are required to maintain a level of privacy in the system. As such, some methods are restricted to only specific members.

Algorithm 4 Updating Reputation of Resellers

Input: reseller address, transaction status
Output: updated reputation score
if *reseller is approved* $\wedge$ *patient has not provided feedback about this reseller* **then**
    Record feedback. **if** *transaction was satisfactory* **then**
        Reseller is rewarded by increasing its reputation score, as shown in equation 1.
    else
        Reseller is punished by decreasing its reputation score, as shown in equation 2
    end
    .
else
    Reject feedback.
end


```
"event": "LotDispatched",
"args": {
        "0": "0xb783B6200Db90dC145A6dd1186FA5eA45B71E237",
        "1": "Drug XYZ 500mg tablets",
        "2": "2000",
        "3": "100",
        "4": "0x7bEEaf4441eA4a37946024dEB6ba14093351028A",
        "LotAddress": "0xb783B6200Db90dC145A6dd1186FA5eA45B71E237",
        "DrugName": "Drug XYZ 500mg tablets",
        "Quantity": "2000",
        "PricePerBox": "100",
        "Manufacturer": "0x7bEEaf4441eA4a37946024dEB6ba14093351028A",
        "length": 5
}
```


FIGURE 7. Event showing a new drug lot being dispatched.

To evaluate the functionality of our smart contracts, we deployed both the original drug supply summary smart contract at 0xc5a98F66719ee680272d8289B8CE227174E2CDDc and the returned drug summary smart contract at the address 0×48ebDb0D8107D12E58266EC9efdc82b047f59FFA. The addresses of both of these contracts are static and were embedded in all lot smart contracts and returned package smart contracts. In addition, we simulated a complete supply chain process by creating a couple of lot smart contracts with a certain quantity of approved drugs. These contracts are identified by an Ethereum address and include information about the drug lot. The drug lot was approved by the original drug summary contract to have a valid drug type and is produced by a legitimate manufacturer. The lot was dispatched, and it was claimed by different entities ending with a retailer. These changes were observed through the previously mentioned logs. Fig. 7 shows an event being triggered announcing a new drug lot is produced. It is worth noting that the address that triggered the event denoted in the first field of the event is the same as the first argument in the args array, lotAddress, which is the address of the smart contract itself.

After selling some drug boxes to consumers, a part of it was returned for re-selling. Fig. 8 shows all the data of the re-usable drug along with the address of the smart contract after it has been approved. It includes the drug name,

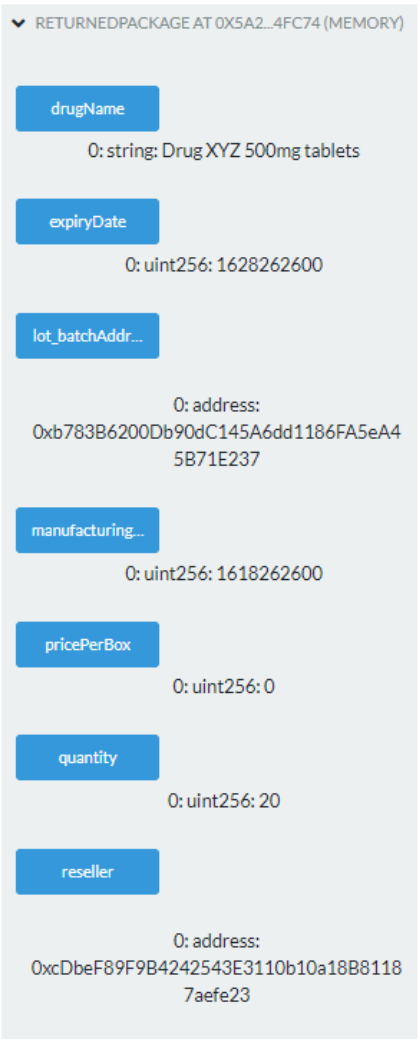

FIGURE 8. Information about the returned drug package with original lot address.

manufacturing, and expiry date, the address of the current owner of the drug, the price (donated for free in this case), the number of boxes that were returned, and the address of the reseller that was selected. Most importantly, this type of smart contract contains the address of the original lot that these packages belonged to. This is vital for checking the history of these specific boxes, including the manufacturer, retailer, the original price, and the entire chain of ownership. If the smart contract at that specific address does not exist, the return is rejected as it is considered inauthentic.

After the purchase was made, a customer can return that medicine if it has not been opened, used, and has been stored in appropriate conditions. The certification agency performs the appropriate testing off-chain to approve or reject the drug. Assuming the return price is significantly lower as per the guidelines of the officials, the customer can attempt to return that drug for other patients to benefit from. Once the certification agency has approved the drug and added it to the returned summary contract, it creates a new contract for the returned package and broadcast an event to announce the


```
"event": "ReturnedDrugApproved",
"args": {
        "0": "0x5A24Ca80e56d53605D5095028F68aCE7eEA4Fc74",
        "1": "Drug XYZ 500mg tablets",
        "2": "20",
        "3": "0",
        "4": "0x73e36E24929428677b365db693f447Ab33d22E80",
        "DrugPackageAddress": "0x5A24Ca80e56d53605D5095028F68aCE7eEA4Fc74",
        "DrugName": "Drug XYZ 500mg tablets",
        "Quantity": "20",
        "PricePerBox": "0",
        "CertificationAgency": "0x73e36E24929428677b365db693f447Ab33d22E80",
        "length": 5
}
```


FIGURE 9. Event showing availability of new resellable drug.


```
"from": "0x0d091d0a6effc6a6ab12122ad72aba02cc43dcf9",
"topic": "0xda9b3f90988de47f2eb5997479c050aa013bcae7c236940a8b6064c7de6c7481",
"event": "DrugResold",
"args": {
        "0": "0x0d091d0a6EFfc6a6Ab12122ad72aBA02Cc43DCf9",
        "1": "15",
        "DrugPackageAddress": "0x0d091d0a6EFfc6a6Ab12122ad72aBA02Cc43DCf9",
        "boxNumber": "15",
        "length": 2
}
```


FIGURE 10. Event showing the resale of a returned drug package.

availability of a new re-consumable drug and shown in fig. 9. The agency assigns a new seller for the drug, as seen in the event being broadcasted.

After the new returned drug package smart contract has been created, the reseller can now sell or donate the drug to other patients. Fig. 10 shows an event triggered when a patient purchases one of the drug boxes out of a resellable drug package from a drug reseller. The event states the box number as well as the drug package address that corresponds to the smart contract Ethereum address. Alternatively, the smart contract could reject the sale in case of any errors, such as the expiry of the returned drug, as shown in fig. 11.

VII. EVALUATION AND ANALYSIS

This section presents a cost analysis of the developed solution and discusses the security aspect of the system. In addition, the generalization of the system is discussed in addition to a comparative analysis with other solutions as well as the challenges faced by such an approach.

A. COST ANALYSIS

Each function call in the smart contract code requires some gas to execute. Gas is a standardized unit to measure the cost of computer operation execution of a transaction in an Ethereum smart contract. Each operation executed costs a specific amount of gas. The cost for all the operations in a function is referred to as the execution gas. The actual gas cost for the transaction, called the transaction gas, also includes the cost of sending the transaction to the blockchain. The methods in the smart contract are executed on a virtual Ethereum network on Remix IDE. This development environment offers an approximation of the cost incurred from each transaction. The cost depends on multiple factors, including the input parameters, code size, the complexity of the code, and the gas cost requested by the sender [17]. Table 1 shows all function calls in the smart contracts along with the execution cost in gas approximated by Remix. Also, the cost in

TABLE 1. Gas cost of Ethereum functions in USD.

Method name	Transaction gas cost	Execution gas cost	Slow execution (USD)	Avg. execution (USD)	Fast execution (USD)
Create lot SC	589052	375600	0.05510	0.06735	0.09796
Create returned SC	845654	593106	0.08701	0.10634	0.15468
registerDrug	44419	22955	0.00337	0.00412	0.00599
reregisterManufacturer	45687	23007	0.00338	0.00413	0.00601
approveDispatched	26787	3915	0.00057	0.00070	0.00102
changeOwner	34994	13146	0.00193	0.00236	0.00343
sellDrug	60291	38827	0.00569	0.00696	0.01012
registerReseller	45665	22985	0.00337	0.00412	0.00599
registerCA	45687	23007	0.00338	0.00413	0.00601
addReturnedPackage	45777	23097	0.00339	0.00414	0.00602
sellDrug (resale)	58122	36658	0.00538	0.00657	0.00956
startAuction	107421	85381	0.01253	0.01530	0.02227
placeBid	87270	65806	0.00966	0.01179	0.01716
closeAuction	32363	26091	0.00383	0.00468	0.00680
feedback	70022	47150	0.00692	0.00845	0.01230
calculateRep	74445	51765	0.00760	0.00928	0.01350

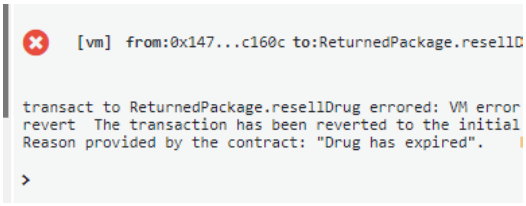

FIGURE 11. Error message showing that the drug cannot be re-sold as it has expired.

USD is presented for easier interpretation. While there is no standard conversion between gas and a fiat currency such as the US dollar, the transaction executor chooses the rate of conversion depending on his preference. Transactions on the Ethereum are executed by miners in the network. Miners validate the transactions and form them into blocks and append them to the blockchain, for which they are rewarded with two ethers. In addition, for each transaction, the sender adds a reward to incentivize the miners to pick their transaction from the transaction pool. This is denoted by the gas price set by the sender. Higher gas price results in a higher probability for the transaction to be mined and added to a block to be deployed on the blockchain. The cost analysis includes three rates of conversion corresponding to slow, average, and fast execution of the transaction, and we are going to use the average gas price suggested by ETH Gas Station as of April 12th, 2020 [18].The slow or cheap execution requires 0.9 Gwei per gas, while the average execution costs 1.1 Gwei per gas, and fast execution costs 1.6 Gwei per gas. The costs for creating the two smart contracts are the highest, as can be seen in the table. This is due to deploying and running the contracts on the Ethereum blockchain, in addition to calling the constructor. The full smart contract code is much bigger in volume than a typical function call, and so is the cost of its execution. Nevertheless, similar to normal method calls, the cost of deploying the smart contract is contingent on the size of the contract, the number of parameters passed to the constructor, the complexity of this constructor, along with an extra cost incurred for sending the smart contract to the blockchain. It is to be noted that at the time of writing this article, 1 Ether equals 163.67 USD. The cost of all methods is \$0.09 or lower for each method for slow execution, \$0.1 or lower for average execution, and \$0.15 or lower for fast execution. This proves the feasibility of utilizing smart contracts for tracking re-consumable drugs.

B. SECURITY ANALYSIS

In this subsection, an analysis of the system's security will be presented. Our proposed solution is built on the Ethereum blockchain. The blockchain technology offers invaluable security advantages and features for the system. Some significant security features related to our solution are discussed below:

- **Authorization and Accountability:** The pharmaceutical supply chain is complex with a large number of contributors, including suppliers, sellers, buyers, and many more. Losing track of the status of the medicine and miscalculation becomes highly possible, with a large number of drugs moved around. On the blockchain, all transactions are permanent and cannot be modified, which means that all activity is recorded, and each member is held accountable for their actions. In addition, we have implemented modifiers that allow certain authorized members to access specific methods. Each member is given limited capability based on its predefined role. For instance, only certification agencies are allowed to add returned drug packages to the returned drug summary smart contract.
- **Availability:** The stakeholders in the system or anyone that requires access to the smart contracts are always guaranteed that the smart contract will be responsive at all times. This assumption is valid due to the decentralized nature of the blockchain. The same smart contract is available on thousands of mining nodes at the same time. Therefore, if some of those nodes are unavailable for any reason or are overwhelmed with transactions, a number of others will be available for confirmation of any transaction within the 20 seconds block time of the Ethereum blockchain. This results in extremely slim chances of the data being compromised due to a DDoS attack against our system. All data is stored securely in an immutable tamper-proof decentralized ledger that eliminates the single point of failure.

- **Non-repudiation:** All transactions performed on the blockchain are secured by a digital signature from the message sender. Therefore, no member can deny buying, selling, approving, or disapproving drugs on the blockchain. All logs are maintained in the ledger and are permanent and protected from being tampered with. This maintains the accountability of each member for all of their actions. All activities are traceable back to its source, which is recorded in a permanent ledger. This forces entities to follow all the policies by updating the ledger, performing the appropriate testing on returned drugs, and ensuring the process is transparent and authentic.

In addition to these security features, there is a need to ensure that the proposed system is robust as it will be publicly available. Therefore, it could be a target for some attacks such as:

- **DDoS Attacks:** A Denial-of-Service (DoS) attack is a cyber-attack where an attacker attempts to force a system to be unavailable by intentionally overwhelming it with a large number of packets. A Distributed-Denial-of-Service (DDoS) attack is a special case of DoS where the incoming packets are from multiple sources. These devices may be colluding together or were compromised by the attacker. The blockchain technology is resilient to such attacks to a great extent. The decentralized nature of the blockchain enables it to run even if several nodes were compromised.
- **The Majority attack:** Miners join the Ethereum networks to mine blocks by grouping transactions, validating them, and forming blocks to append it to the global blockchain and update the world state. Due to the use of the Proof-of-Work (PoW) consensus protocol, a miner's chance of adding his block is associated with his hashing power. Therefore, a single miner or a small group of miners cannot gain control over the entire network [19], [20]. However, if a group of miners was able to control over half of the entire hash rate of the Ethereum network, they can control the network. This is known as the majority attack or the 51% attack [19]. Additionally, transaction malleability targets disrupting the state of a blockchain by introducing malicious transactions that are semantically similar to benign transactions [21].
- **The DAO attack:** This type of attack compromises a blockchain-specific vulnerability inspired by the attack on the DAO in 2016 [22]. This incident was caused as the blockchain was susceptible to *"call to unknown;;* and *"reentrancy"*; hence, this attack is also known as the reentrancy attack. This vulnerability was mitigated by a hard fork in the blockchain that fixed those bugs.

C. GENERALIZATION

Our proposed solution is designed to be generic enough for most supply chain applications. Nonetheless, the implementation that uses Ethereum blockchain smart contracts should be public as all members can view the smart contract as well as events broadcasted by the smart contract. Although some methods are only accessed by authorized members, the state of the smart contracts is publicly visible for all members of the Ethereum blockchain. Our solution supports applications that require the transfer of goods between entities with limited accessibility for each member. In addition, some approvals might need to be collected for certain operations. With minimal adjustments, the source code for the smart contracts described in this article, our solution can be implemented in numerous use cases similar to pharmaceutical supply chains.

TABLE 2. Comparison with state-of-the-art.

Features	Huang et al. [12]	Jamil et al. [13]	Alangot et al. [14]	Bocek et al. [16]	our work
Blockchain-based	✓	✓	✓	✓	✓
Smart Contract	✗	✓	✗	✓	✓
Publicly Available	✓	✗	✓	✓	✓
Tracking Drugs	✓	✓	✓	✓	✓
Returning Drugs	✗	✗	✗	✗	✓
Decentralized Storage	✗	✓	✗	✗	✓
DApps	✗	✓	✗	✓	✓

D. QUALITATIVE COMPARISON

The comparative analysis, in contrast with the latest solutions described in Table 2, shows that our proposed approach offers a solution to track and approve re-usable drugs as they are returned from original owners. Existing solutions suffer from drawbacks such as centralization [11], private implementations [13], or lack of smart contract support [12], [14]. On the other hand, our solution proposes a decentralized solution to track drugs from the original manufacturer as well as the return of unused drugs. This approach utilizes the Ethereum blockchain smart contracts to implement a publicly available system. However, the decentralized front-end application for users to utilize our solution requires some improvement. This is one of the future goals that we are looking to implement in future development.

E. CHALLENGES

Blockchain had a significant impact on the healthcare industry. It is showing incredible potential in applications such as the pharmaceutical supply chain. In this section, we present major challenges facing our blockchain-based approach.

- **Smart contracts:** Programming blockchain smart contracts introduce some constraints on the system as compared to classic centralized servers [23]. Smart contract developers face challenges such as the high standard for security by the blockchain, limited debugging, and Solidity restrictions. In addition, smart contract code needs to be highly efficient by storing only vital information and minimizing operations. The cost of execution of Ethereum functions depends mainly on the complexity

of the method. Therefore, optimizing algorithms is crucial to reduce gas consumption as much as possible.

- **Scalability:** There is a limit on the throughput of any system implemented using blockchain networks. For instance, Ethereum blockchain offers about 15 transactions per second [24], [25]. This poses a cap on the number of transactions in the proposed approach. As the input flow increases, it is not reflected in the output flow due to this limitation. A scalable service provider should be able to allocate more resources whenever need. However, this is not possible in such systems implemented on the blockchain.
- **Time delay:** Nodes in the blockchain consume a lot of time and power to group transactions, validate them, store them, form a block, and finally broadcast their results to other nodes [26]. This is done for each node until all miners on the network reach consensus and agree on a block to append. The Ethereum blockchain adjusts the difficulty for the consensus protocol to take about 20 seconds. This time period gives the nodes enough time for processing and communicating with other nodes. In addition to the time for block formation, some time is allocated for the block to be confirmed. The block is considered to be confirmed if it is followed by a specific number of blocks such that no other parallel side chains would overwrite the current chain of blocks. When a total of 10 blocks formed in front of some block, also called ten confirmations, that transactions in that block are considered to be irreversible and permanent. In Ethereum, this would take approximately 3 minutes per block. However, if multiple transactions from different sources in our system were included in the same block, they would be confirmed at the same time. In addition, low gas prices offered by users of the blockchain introduce additional delay, as it lowers the probability that miners would include their transaction in the upcoming block.
- **Privacy concerns:** The public availability of the source code introduces a privacy compromise, although blockchain still maintains the anonymity of all of its members. Most blockchain networks, including Ethereum, do not enforce policies to protect the data privacy [27]. All transactions are distributed across the entire network. Some measures were taken to ensure that only authorized entities can trigger certain methods in smart contracts. However, all information is still publicly available for anyone to view. Knowing such information is an invasion of privacy and can be exploited to harm the stakeholders involved.

VIII. CONCLUSION

In this article, we have presented a blockchain-based solution to track the origin of returned, reconsumable drugs from its manufacturing until they are re-sold to customers. This process involves interaction from many different members that are all governed by the smart contracts. The smart contract code deployed on Ethereum has been made available as a Github repository. We used Remix development environment to deploy our solution, test and validate its functionality and outcome, and perform important analyses. All functionalities of the smart contract are shown to produce the expected outcome as per the problem description. According to the cost analysis presented, the estimated execution gas for the methods involved was shown to be minimal. Given the mentioned Ether rate at the time of this writing, all methods require $0.1 or less to execute for an average gas price. This low cost proves the feasibility of deploying such a system to be used for drug tracking and resale. Moreover, our security analysis discussed the resilience of smart contract code against major security vulnerabilities and attacks. Our solution can also be altered to be applicable to other use cases, as described. Finally, we presented a qualitative comparison against some of the similar solutions in addition to the major challenges that face our blockchain-based approach. As future work, we are in the process of developing an end-to-end solution with back-end and front-end DApps to be implemented on the Ethereum mainnet. The mentioned smart contracts present the back-end of the system, while the front-end is similar to web applications, where it focuses on the user interface and the overall user experience.

REFERENCES

[1] *Silent Murder*. Accessed: Jul. 7, 2020. [Online]. Available: https://www.dandc.eu/en/article/medicines-are-too-expensive-poor-people-developing-countries-local-production-could-make

[2] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jul. 15, 2020. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.

[4] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "Monetization of services provided by public fog nodes using blockchain and smart contracts," *IEEE Access*, vol. 8, pp. 20118–20128, 2020.

[5] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[6] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for AI-powered network operations," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 1–8, Sep. 2018.

[7] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019.

[8] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, Jan. 2019.

[9] C. Costa, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti, "A review on agri-food supply chain traceability by means of RFID technology," *Food Bioprocess Technol.*, vol. 6, no. 2, pp. 353–366, Feb. 2013.

[10] N. Shah, "Pharmaceutical supply chains: Key issues and strategies for optimisation," *Comput. Chem. Eng.*, vol. 28, nos. 6–7, pp. 929–941, Jun. 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0098135403002333

[11] J. S. Srai, C. Badman, M. Krumme, M. Futran, and C. Johnston, "Future supply chains enabled by continuous processing—Opportunities and challenges. May 20–21, 2014 continuous manufacturing symposium," *J. Pharmaceutical Sci.*, vol. 104, no. 3, pp. 840–849, 2015.

[12] Y. Huang, J. Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1137–1144.
[13] 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, no. 5, p. 505, May 2019.
[14] B. Alangot and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," in *Proc. Int. Conf. Ubiquitous Commun. Netw. Comput.* Cham, Switzerland: Springer, 2017, pp. 189–195.
[15] K. Coleman and J. Coleman. (Sep. 2018). "Good Shepherd Pharmacy Uses New Technology to Facilitate Medication Sharing Across the U.S." High Ground. Accessed: Aug. 1, 2020. [Online]. Available: https://www.highgroundnews.com/features/GoodShepherdBlockchain.aspx
[16] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.
[17] A. Rosic. *What is Ethereum Gas?* Accessed: Apr. 12, 2020. [Online]. Available: https://blockgeeks.com/guides/ethereum-gas/
[18] *ETH Gas Station*. Accessed: Apr. 12, 2020. [Online]. Available: https://ethgasstation.info/
[19] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[20] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 436–454.
[21] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790619316180
[22] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. Int. Conf. Princ. Secur. Trust*. Berlin, Germany: Springer, 2017, pp. 164–186.
[23] W. Zou, D. Lo, P. S. Kochhar, X. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Trans. Softw. Eng.*, early access, Sep. 24, 2019, doi: 10.1109/TSE.2019.2942301.
[24] *Ethereum 101: How Will Ethereum Scale?—Coindesk*. Accessed: Aug. 1, 2020. [Online]. Available: https://www.coindesk.com/learn/ethereum-101/will-ethereum-scale
[25] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19310805
[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
[27] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

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

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 joined Khalifa University, United Arab Emirates, in August 2010, and 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. Prior to joining Khalifa University, he worked for ten years with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. He is currently a Full Professor with the Department of Electrical and Computer Engineering, Khalifa University. He has over 190 publications and three patents. 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. He was a recipient of the Khalifa University Outstanding Research Award 2014/2015, the KFUPM University Excellence in Research Award of 2008/09, and the KFUPM Best Research Project Award of 2009/10, and also a recipient of the departmental awards for the Distinguished Research and Teaching in prior years. He serves on the Editorial Boards of many WOS-listed journals, including *IET Communications*, *IET Networks*, *Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS,* and *AJSE*. He is the Track Chair of the IEEE GLOBECOM 2018 on Cloud Computing. He is also an Associate Editor of IEEE *Blockchain Newsletter* and a member of the IEEE Blockchain Education Committee.

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. He is currently an Associate Professor with the Department of Industrial and Systems Engineering, Khalifa University, Abu Dhabi, United Arab Emirates. His expertise is in multicriteria optimization techniques applied to supply chain and logistics, healthcare, energy, environment, and sustainability. His postdoctoral research was centered on technology adoption and the implementation of innovative practices in the healthcare supply chains and service delivery. He has led several successful research projects and pilot implementations in the area of supply chain data standards in the U.S. healthcare system. His primary research interests include applying technology, systems engineering, and process optimization techniques to analyze complex systems. His research has appeared in top-rated journals, including *Annals of Operations Research, IISE Transactions, Computers and Industrial Engineering, Energy Policy, Applied Energy, Knowledge Based Systems,* IEEE Access, *Journal of Theoretical Biology*, *Engineering Management Journal*, and others.

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. He 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 is an Associate Editor of the *Cluster Computing* and IEEE Access and regularly serves on program and review committees of several journals and conferences.