IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 15, 2020, accepted September 30, 2020, date of publication October 6, 2020, date of current version October 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3029196

A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability

PENG ZHU[1], (Member, IEEE), JIAN HU[1], YUE ZHANG[2], AND XIAOTONG LI[3]

[1]School of Economics and Management, Nanjing University of Science and Technology, Nanjing 210094, China
[2]California State University, Northridge, CA 91330-8372, USA
[3]College of Business, The University of Alabama, Huntsville, AL 35899, USA

Corresponding authors: Peng Zhu (pzhu@njust.edu.cn) and Xiaotong Li (lixi@uah.edu)

This work was supported in part by the National Natural Science Foundation of China under Grant 71874082 and Grant 71774084, in part by the Ministry of Education of China, Humanities and Social Sciences Project under Grant 18YJA870021, and in part by the Philosophy and Social Sciences Project of Colleges and Universities funded by Education Department of Jiangsu Province, China, under Grant 2016SJD870005.

ABSTRACT Medication quality and safety are crucial to the health of the public. Responding to the urgent need for medication information provenance and anti-counterfeiting, this study proposes a blockchain based method for medication information storage, inquiry, and anti-counterfeiting along a medication supply chain. Leveraging the features of decentralization, tamper-proof, traceability, and participative node maintenance of blockchain technology, the proposed method can assure the transparency and openness of medication supply chains. An access control policy model based on smart contract is designed to prevent medication information from being altered or disclosed at nodes of the blockchain. In addition, a point-accumulation upgrade/downgrade mechanism is introduced to improve the consensus mechanism. The proposed solution eliminates the needs for centralized institutions and third-party organizations, and provides a full record of the medication circulation process. Our simulation results show that efficiency and security are enhanced by the improved consensus algorithm and access control mechanism. As a result, our method can render high level of security and privacy protection that is critical to the integrity of a medication information management system.

INDEX TERMS Medication anti-counterfeiting, traceability, blockchain, PBFT consensus, supply chain.

I. INTRODUCTION

In recent years, the world has witnessed frequent public health incidents involving counterfeiting behavior by firms or individuals in the medication/medical supplies industry and the related supply chains. According to the estimate of the World Health Organization (WHO), 10% of medications sold worldwide are counterfeits, and the percentage is as high as 30% in some developing countries. In the wake of COVID-19 pandemic broken out in early 2020, counterfeit medicines and counterfeit vaccines are rampant, severely threatening the health of the people around the world. This situation calls for more effective medication quality and safety administration targeting medication counterfeiting.

The problems behind the incidents of medication quality and safety concentrate on the data record counterfeiting at various nodes on the medication supply chain. The lack of openness of the information along the supply chain often leads to the lack of data transparency and the difficulty in medication information provenance. These are major flaws in medical supply chain monitoring and administration, causing difficulty in establishing and maintaining accountability regarding medication quality and safety [1]. Therefore, the core functions of medication quality and safety administration include anti-counterfeiting of medication information and traceability maintenance along the medication supply chain. For the above needs, traditional medication administration institutions usually adopt a centralized model, requiring that all nodes along the supply chain upload medication information to a central repository which is maintained and managed by a curator (or a few curators). That kind of medication administration arrangement subjects the data to the risks of data alteration/modification and (undesirable) disclosure. In this sense, traditional medication administration institutions are clumsy and faulty facing today's medication safety needs [2]. A medication administration arrangement

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

that is more open, more transparent, and supporting better traceability is in demand, and will have the potential to greatly improve the current situation of medication safety.

Blockchain, an emerging technology after mobile computing, the Internet of Things (IoT), and artificial intelligence (AI), is by essence a ''database technology with modification-proof for historical records'' [3]. Blockchain provides new potentials for the anti-counterfeiting and traceability of medications. With the desirable characteristics of decentralization and modification-proofing, it doesn't rely on any third-party organization or third-party individual. The technology can record all the information of the medication along the supply chain from production to final sales by the sequence in time, and the information recorded in this manner cannot be altered. The monitoring/regulating institutions can also participate in the process of recording such information onto the blockchain [4]. The blockchain-based infrastructure can achieve information sharing, information tamper-proofing, and information traceability, thereby effectively improving the safety and traceability of the medication supply chain.

The main purpose of the current study is to expound how blockchain can be applied onto medication anti-counterfeiting and traceability. Leveraging blockchain's features of distributed node maintenance, hash taper-proofing and time stamp, we construct and implement a feasible anti-counterfeiting and traceability method for medications. We will articulate the procedure of such a method, including medication supply chain information collection and storage, and medication information traceability. We will use Python coding to construct a blockchain environment to conduct a virtual traceability simulation as an experiment to test our solution.

The main contributions of this study include:

- Identifying the flaws of current medication quality and safety administration system;
- The architectural design of the proposed application of blockchain technology to medication anti-counterfeiting and traceability system, with the articulation and demonstration of the process details; this is the key part of the study;
- Coding with Python, to simulate the process of medication information storage, modification, and provenance, with the result being presented with data visualization techniques;
- Simulation of the proposed method, and testing the method's feasibility; then assessing the proposed method's performance in security and its benefits over costs.

The article is organized as follows: Section 2 provides a literature review on medication anti-counterfeiting, and on the related applications of blockchain; Section 3 discusses a blockchain-based method for medication anti-counterfeiting and traceability; Section 4 provides the details of testing and experiments with a simulation; Section 5 assesses the performance of the proposed method, and analyzes the data output. The article ends with a conclusion section.

II. RELATED WORK

In this section, we will review the recent progresses in blockchain technology, and to identify other related research works on the application of blockchain to traceability.

In recent years, traceability has become a popular concept in the field of supply chain management; this phenomenon has propagated to supply chains involving very different means of production and very different product types [5].

Traceability techniques provide the source of relevant raw data, the procedure of the processing of such data/information, and the new information generated by the activities related to a product that travels along the supply chain. Traceability also plays the role of the tool for tracing and for communicating among participating entities, to assure the accessibility of the information throughout the whole supply chain [6]. Olsen and Borit, in a paper discussing food safety [7], provided the general definition of traceability; they hold that ''traceability is the ability to access any or all information relating to that which is under consideration, throughout its entire lifecycle, using recorded identifications.'' The main purpose of tracing/traceability is to look for the historical records of a specific product(s), with the purpose of addressing the issues of food safety and food preservation [8]. In this regard, tracing and traceability aim at monitoring and tracking an item moving through all steps in a food supply chain from food production, processing, distribution, to final sales, so as to assure that the originating point of a food quality problem can be identify quickly, and accountable parties be held for the problem [9]. In today's society, we have witnessed frequent incidents of medication counterfeiting and quality problems, which is very troublesome to the public. In this context, tracing and traceability of medications is critically important to the public, to the operation of the pharmaceutical manufacturing and distribution industries, and to the governments. If there can be a reliable tracing and traceability system, patients, regulators, and stakeholders in medication manufacturing and distribution (pharmaceutical companies, retailors, medicine stores, and clinics) can then quickly follow a medication from the source through to the destination. That capability will be an important assuring mechanism for maintaining and improving public health.

More and more scholars worldwide have started to research how to construct a practical method for medication traceability (to trace the distribution and flows of medications, and to identify any possible counterfeits and their point of happening). The mainstream solutions are mostly IoT (Internet of Things) technology employing RFID (Radio Frequency ID), that is based on a centralized client-server architecture, to register and trace the information flow along the supply chain [10]–[12]. This kind of centralized methods have several problems: First, an entity (person or organization) can easily access and modify the medication information uploaded onto the server, which could infringe into the privacy of related parties, and affect the authenticity of the related medication information. Second, the architecture of tracing with centralized server is not efficient, and the related

nodes (clients in client-server architecture) on the supply chain may suffer isolation, or lack information transparency. The above problems could be effectively solved with the two essential features of blockchain: non-modifiability, and distributedness.

The blockchain technology originated from an article by Satoshi Nakamoto entitled ''Bitcoin: A peer-to-peer electronic cash system'' [13]. In this article, Nakamoto described a brand new Bitcoin digital currency system that is decentralized and that does not need to rely on any trusted authority. The blockchain is the core technology underlying such a system. Literally, the data container in blockchain is a Block; newly added data is packaged into a block in a batch manner at set time intervals. Every piece of data and every block must be agreed upon and a consensus must be reached by participants who are eligible to perform data recording operations in the blockchain [14]. In a blockchain, each block includes the cryptographic hash of the prior block (the block generated in the previous time interval) in the blockchain, linking the two blocks that are generated in the two consecutive time intervals [15]. When all blocks generated in the above manner are all chained together following the hash algorithm, a chain is eventually formed, thus ''blockchain.'' Li *et al.* [16] hold that blockchain is like a decentralized, distributed database; it can assure that, by using cryptographic algorithms, the data on the chain cannot be modified or forged. The time stamps for blocks on a blockchain allow the blockchain to record, in time sequence, the delivery and confirmation history of each transaction, and other related information and data in the transaction, thus realizing the chain-wise arrangement of data [17].

The application of blockchain in traceability begins with the traceability of supply chain products (see, for example, [18]–[20]). These studies have effectively verified that blockchain technology can address the main shortcomings of traditional traceability architecture and solutions. More and more scholars are beginning to pay attention to the application of blockchain in anti-counterfeiting and the traceability of medicines.

Bocek *et al.* [21] use blockchain technology to maintain the immutability of data in the medicine supply chain and the accessibility of temperature records to the public, while reducing the operating costs of the medicine supply chain. There are many complex and strict environmental control processes in the medical industry. Through blockchain technology, all environmental control data is transmitted to the chain, where smart contracts are used to fully evaluate the properties of medicines, and each package can be monitored during the transportation of medications (Kumar and Tripathi [22]). The most important part of medicine product safety management is to trace how counterfeit medicines were originally manufactured in the supply chain. The functions of the blockchain can make medication information fully traceable from the manufacturer to the final consumer, thereby achieving the objective of identifying counterfeit medicines. Kumar and Tripathi's study used blockchain and encrypted QR security codes to address the problem of medicine safety. Every medicine had a unique QR code generated at the time of production, which represents the identity of the medicine and can circulate along the entire supply chain. Only the authorized links on the supply chain could view, verify and sign the security code. Saxena *et al.* [23] analyzed the impact of counterfeit medicines on the healthcare supply chain and evaluated the current solutions to reduce the number of counterfeit products entering the market. They established PharmaCrypt (a new blockchain-driven tool) through feedback received from industry experts to reduce the possibility of counterfeit medicines entering supply chain. Botcha *et al.* [24] proposed a method to enhance the traceability of the medicine supply chain using IoT devices and blockchain. They demonstrated that blockchain technology can ensure traceability from the source to the consumer, thereby building trust and improving service quality of the pharmaceutical industry.

Recently, a large number of studies have been conducted on the transparency, immutability and security of blockchain technology for the medicine supply chain. However, most of the blockchain-based medicine information management recommendations lack practicality. Pham *et al.* [25] proposed a new product ownership management method based on blockchain, which is used in a system to resist counterfeiting of medicines and improve the practicability of medicine management. The implementation of small-scale experiments showed that the system proposed in the article can work normally in the actual environment. This research provides a technical research foundation for the medicine traceability blockchain.

In summary, blockchain, as an emerging technology, draws broad attentions in its possible applications in traceability. Due to its technical characteristics such as decentralization, data uniqueness, unforgeability of transaction records, etc., blockchain can achieve reliable and transparent tracing of data stored on the chain, and can effectively assure the accuracy and consistency of data stored in every participating nodes on the supply chain [26]. Therefore, it is reliable to apply this technology to the anti-counterfeiting and traceability of medicine information, to realize the transparency of medicine information, and to assure accountability and information integrity throughout the supply chain circulation process.

III. PROPOSED BLOCKCHAIN-BASED SOLUTION

In this section, we will describe the solution employing blockchain technology in medication anti-counterfeiting and tracing. Through the construction of our method, we will describe in details the tracing and traceability throughout the medication supply chain. We will also design the access privilege assignment and consensus mechanism for the participating entities in the blockchain-based medication anti-counterfeiting and traceability system.

A. GENERAL MODEL

GS1 (Global traceability standard 1) [27], established by the Unified Code Committee of the United States, is a global standard for cross industry product, transportation unit, asset, location, service identification and information exchange. GS1 points out that traceability system is driven by traceability data, and traceability data is generated by executing various business processes from input to final output [28]. GS1 requires all traceability objects to have a unique identification, which should represent only the product of interest. The unique identifier will flow through the whole process. Therefore, after a blockchain is applied to medication tracing and anti-counterfeiting, each medication is assigned a unique medication ID. The medicine ID is the unique identifier of the medication in traceability system. A medication, after passing the quality inspection in the manufacturing stage, has its information recorded onto the blockchain by the manufacturer; this information would then flow with the medication toward the final consumer. In the flow of the medication and its information toward the final consumer, the intermediary nodes such as wholesalers and retailers (pharmacies or clinics/hospitals) can all update the medication's current status through the peer-to-peer (P2P) network of the blockchain. In this process, every record of transaction or transition (changing hands from one node to another) would be recorded into the data layer of the blockchain, in the time sequence of the events. Finally, the whole process of medicine circulation can be inversely queried using the medicine ID (unique identifier for traceability). The details of the proposed blockchain-based method to medicine traceability and anti-counterfeiting are provided as follows:

- **Participating Entities:** The model of the blockchain-based medicine anti-counterfeiting and traceability system considers the following entities on the supply chain as the participating nodes: medicine manufacturers, medication distributors and sellers (such as clinics/hospitals, pharmacies, etc.), and regulators. Regulators join as the main node to monitor and verify all relevant mechanisms on the blockchain; medicine manufacturers, distributors and sellers act as intermediate nodes to upload and update medicine information; each participating entity can query and provide feedback about the data stored on the blockchain. Each entity has a blockchain address and interacts with one another through the blockchain network. The operation permission of accessing the data on the blockchain is determined by the role and function of the participating node specified by the chain administrator.
- **Objective:** In the process of the movement of medications along the supply chain, the downstream nodes, through tracing the historical data, can also form a monitoring mechanism: if the medication had some problems at the end stage, from the flow records (registries) on the blockchain, one can quickly trace to the node where the problem may have emerged. If the medication was involved in counterfeiting (was a product of counterfeiting), the non-modifiability of blockchain would allow concerned parties to conduct tracing and demand accountability.
- **System workflow:** As shown in Figure 1 above, in the proposed model, when a batch of medications have passed the inspection in the manufacturer's plant, the manufacturing-related information for this stage (including medication ID, manufacturer information, medication name, product batch number, production date, and expiration date) would be recorded and stored onto the blockchain. When the medication in concern flows down the supply chain to the distributor, the distributor can check and verify the medication information stored on the blockchain; after the medication passes the verification, the current entity possessing the medication would then update the medication information for the current stage, including the information of the delivery entity (the distributor), information of the deliver-to entity (recipient), the delivery time and receiving time. When the medication flows to the seller, the seller would update the current medication information and the final destination of the medication flow. In the above process, the regulators can be government institutions or pharmaceutical industry associations. The regulators do not participate in the update of medication information; they are only in charge of the monitoring and the maintenance of the chain of flow (the supply chain). The manufacturer can trace its own medication products' direction of flow and status in circulation, based on data on the blockchain; the distributors can verify the medications purchased based on data on the blockchain, to prevent from and protect against possible counterfeiting by the manufacturers; the consumers and the regulators can perform specific inquiries based on data on the application layer of the blockchain, to inquire about the recorded information of any one node, including the information about the very source node.
- **System architecture:** The system architecture includes three parts: blockchain network environment, a smart contract, and a web client, as shown in Figure 2. Blockchain network environment includes a data layer and a network layer. The data layer is the core layer, which can store the collected medicine data; the network layer is the basis of information transmission, including consensus mechanism, P2P network, and data verification mechanism in the network. The smart contract is contained in the contract layer, which is the core of the whole system method and encapsulates the code that delivers the system's functions [29], including the code delivery and deployment for medicine information traceability and anti-counterfeiting, access control/privilege assignment, etc. Web client is the general name for application layer and user layer, which enables consumers and all participants in medicine circulation process to interact with the blockchain, providing an indirect interface for user queries.

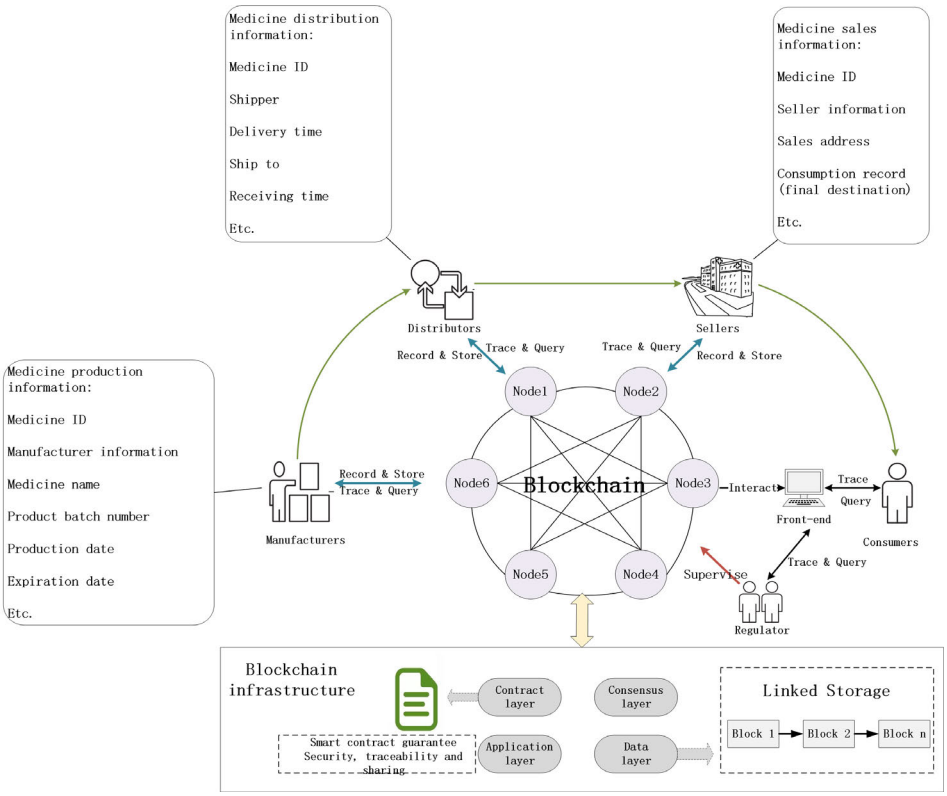


FIGURE 1. Blockchain-based medication anti-counterfeiting and traceability model.

B. ANTI-COUNTERFEITING AND TRACEABILITY

Blockchain-based medication anti-counterfeiting is to apply the blockchain technology to the medication supply chain, from manufacturer to the end consumer, to conduct data recording/registering and storage, through the autonomous uploading by each and every node on the supply chain, as shown in Figure 3.

The anti-counterfeiting of medication relies on the features of blockchain including non-modifiability, consensus mechanism, and traceability. Non-modifiability on a blockchain starts with storing a fixed-length hash value of the uploaded medication information, with a time stamp. A hash function is a type of function that can map information of any length to a fixed-length value. When medication information is uploaded, the whole information can be hashed to a fixed-length hash value [30]. The hash value for each piece of information is unique and cannot be reversely computed, that is, given a hash value resulted from a piece of information, it is impossible to obtain the original information though computation. When the input data has any tiny bit of change, the resulted hash value will change significantly. Therefore, in order to verify if the medication information on the blockchain is intact, it only involves a simple hash operation followed by comparing the computed hash value to the hash value stored on the blockchain. If the two values are identical, then the medication information is not modified or forged; otherwise the information would have been modified. The non-modifiability of blockchain can effectively prevent possible modification or forging at any node on the medication supply chain, thus ensuring the integrity, authenticity, and uniqueness of data on the blockchain.

The consensus mechanism enables multi-party participation by the nodes on the network of blockchain, allowing them to jointly maintain the same medication's information set. The more parties participating in the medication flow in the supply chain, the larger the data size jointly maintained, thus the more trustworthiness could be brought to the consumers [31]. The blockchain-based endorsement can become the effective trustworthiness mechanism, reducing the likelihood of a counterfeit. We will explain this mechanism in more details in the next section.

Medication traceability is the core component of medication anti-counterfeiting. From the moment the pharmaceutical company possesses a medication ID that is recorded and uploaded on the blockchain, till the medication eventually arrives at the hands of the final consumer. Through this whole process, each time information flows from one entity to another, there is a transfer of information (a transaction on the blockchain). Each blockchain transaction would generate a new block to record the transaction, including the transaction addresses of the output party and the input party, the transaction time, and the added contents of the transaction. These pieces of information are non-modifiable. Each participating entity must register a blockchain node, and obtain a unique address-identification token. Such a token consists of the public key and private key in asymmetric cryptography.

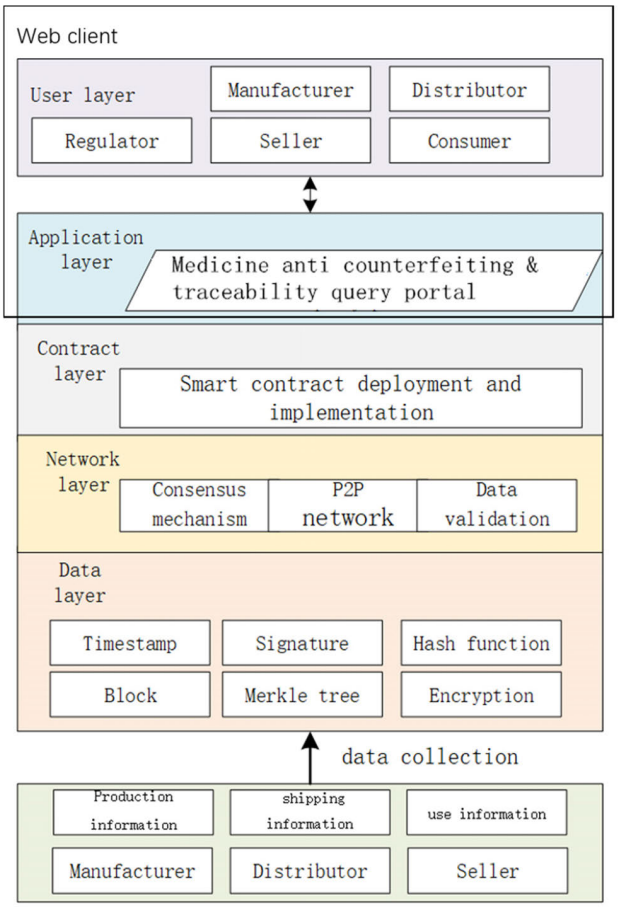


FIGURE 2. System architecture.

Each time there is a storage or transfer operation of medication information, the account(s) of related node(s) on the chain would be reconciled. Since the blockchain uses the hash function to join the current block with its immediate previous block to form a sequential chain of past transactions, from any node one can trace back to the immediate previous block based on its address.

Figure 3 demonstrates the complete process of a transfer of medication information, in which an information update and transfer happened at a node would be stored on the blockchain and would form a transaction database; each transaction would correspond to a block, and each block is distinguished by its own hash value. Inside the block there are the information contents of ''From'' output party, ''To'' input party, time stamp ''Time'', and transaction message ''Message''. The To-party in the previous block is the From-party of the next block, thereby connecting the two blocks.

With this design, the consumers and regulators can trace back with the medication ID, to query the medication's flow through the whole process of the supply chain, reaching as far back as the original manufacturer. At any node people can designate the address of a specific node on the supply chain and query and trace the transfer status of the medication before and after that node with the provided address, which can assure accountability along the supply chain.

Blockchain offers the features of non-modifiability, data integrity traceability, and consensus endorsement mechanism; these can effectively address the issues of medication traceability and anti-counterfeiting. If a medication production or distribution company attempts to evade its accountability regarding counterfeiting, it can only delete the counterfeit medicine under its name, but the other participating entities' data on the blockchain cannot be deleted. Because the piece of deleted information at one node already contributed to the generation of the hash value of the node itself and the hash value of the next node, the deletion of a portion of the information from an earlier node would cause conflicts of hash values of that node and all the nodes that follow. At the same time, all members on the blockchain can query a specific medication in question, obtaining its status data throughout the whole supply chain. By re-examining the quality data associated with the nodes on the chain, it would be easy to determine whether the problem of the medication was originated in the production process or in the logistical process.

C. CONSENSUS MECHANISM

In the decentralized chain for anti-counterfeiting and traceability, how to achieve consensus among all participating nodes to endorse the authenticity of medication information is the key step in the solution for anti-counterfeiting. To address this concern, practical Byzantine fault tolerance (PBFT), blockchain's consensus algorithm, is a mechanism applicable to a traceability chain participated by various types of nodes. The original design purpose of PBFT was to solve the Byzantine generals problem, in which there are nodes that are loyal (or non-faulty) and there are nodes that are dishonest (or faulty). When there are f number of Byzantine nodes (dishonest nodes), with PBFT, if the total number of nodes $N > 3f$, the distributed system can reach consensus. In blockchain network, f Byzantine nodes are allowed if $f < (N-1)/3$ [32].

However, when employing PBFT for consensus operation, there are large number of communications among nodes; as the number of nods increases, so will the number of dishonest nodes, causing the amount of network traffic generated by nodes in the consensus process to increase quickly, affecting the efficiency of consensus and block generation. Our study, based on the application scenario of medicine blockchain, improves PBFT by introducing score-keeping and up/down-grading mechanism, so as to allow the consensus algorithm to quickly converge to the optimal status when facing dishonest nodes, resulting in increased block efficiency and security.

The improved consensus mechanism categorizes nodes on the blockchain network into two types, based on the cumulative scores: one type is consensus nodes, *N-f* nodes, which will participate in consensus process; another type is candidate nodes, f nodes, which will not participate in consensus process, but would receive the reward/penalty points as the result of the consensus process. When there are dishonest

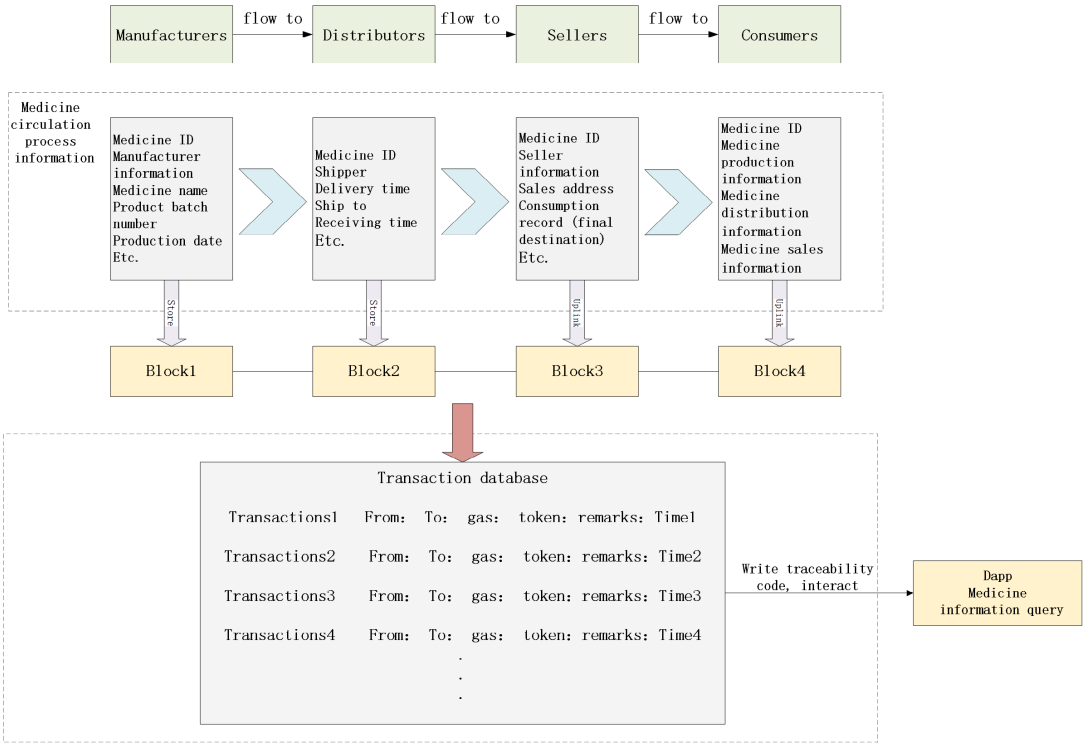


FIGURE 3. Medication information storage and traceability.

nodes among consensus nodes, after one round of consensus operation, the dishonest node would be dropped from the set of consensus nodes; and from the set of candidate nodes one with the highest score (cumulative points) would be selected to join the set of consensus nodes. This operation would ensure that the nodes in the consensus nodes type are honest nodes with high probability of consensus success. The detailed improvement ideas is shown in Figure 4.

Step 1: Number all the nodes participating in the medication traceability blockchain network, and set the initial points at 100. Define the consensus nodes set CS and candidate nodes set DS, $CS = \{0, 1, 2, \cdots, (N-f-1)\}$, $DS = \{(N-f), \cdots, (N-1)\}$, where consensus nodes in the number $N-f$, and candidate nodes in the number of f.

Step 2: Accept each node's request for medication information uploading to the medication block chain. The main node conducts the numbering of all nodes after receiving the requests. The role of the main node is assumed by the regulator.

Step 3: The consensus nodes perform the consensus operation; through pre-prepare, feedback, and commit steps, compare and verify the consistency of feedback message; Different comparison results would lead to different operations in the next step.

Step 4: If the feedback message is consistent with the locally stored message by the main node, then the message content is intact; the consensus nodes complete this round of consensus.

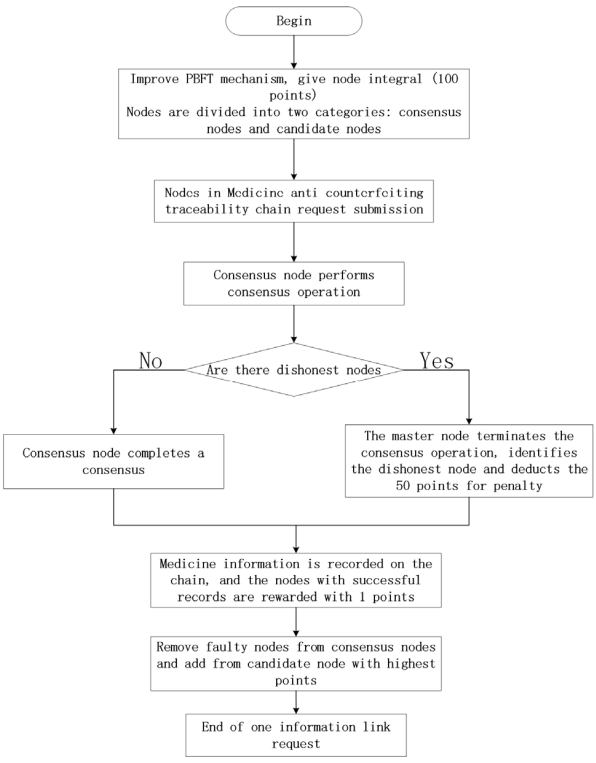


FIGURE 4. The improved PBFT consensus mechanism flowchart.

Step 5: If the feedback message is inconsistent, then the message content was judged to be modified; it can then be decided that the node sending this feedback message is a

dishonest node (that modified the content of the message). In this case, the main node would terminate this consensus operation, and launch PBFT algorithm involving all nodes on the blockchain network, to ensure that the number of dishonest nodes is within the required limit. Consensus has been reached.

Step 6: Lastly, the main node conducts rewarding or penalizing to honest and dishonest nodes, respectively, with the reward of 1 point or a penalty of 50 points. Next, perform upgrading/downgrading of nodes according to their scores, and drop the dishonest nodes to assure that the consensus nodes set contains honest nodes with higher probabilities of consensus success. The algorithm loops back to a new round of PBFT algorithm.

D. ACCESS PRIVILEGE AND MEMBER ADMINISTRATION

The blockchain medication anti-counterfeiting and traceability method designed in this study performs access privilege control and administration to implement customized access control policy. This control and administration can effectively solve the problem of privacy infringement to the medication information. We adopt role-based access control (RBAC) model to perform role categorization and to authorize corresponding operations. RBAC can map users to roles and, through definition of different roles as well as the relationship among roles, implement corresponding restrictions to assure data security [33].

Corresponding to different roles on the traceability chain, we set four different authorized privileges: the first group are regulators, who are government agencies or pharmaceutical industry self-regulating bodies that perform blockchain node maintenance and block verification for the main block, as well as medication information flow tracing and accountability enforcing. These roles do not include the update and maintenance of medication information, which are the charges of the intermediary nodes below. The second group are manufacturers, who are responsible for recording and uploading of information of shipped medication. When the medicine flows from the manufacturer to the downstream dealer, the initialization status of the medicine is updated by manufacturer. The third group are the intermediaries, including distributors and sellers (clinics/hospitals, pharmacies, etc.), who are the intermediary nodes for the movement and distribution of medications. When a medication is in the movement from one of the intermediaries toward the final consumer, it is the charge of an intermediary who currently holds the medication to update the medication status information. Finally, the fourth group, the consumers: they are the end user of the medication. With the access right to query, this final group can re-track the whole history of the transfer of the medication along the supply chain. The second group (manufacturer) and the third group (intermediaries) also have this privilege to query and trace back.

The implementation of access control is mainly based on the combination of blockchain-based smart contract functions and the RBAC model. The framework includes users, role sets, permission sets, policy management, smart contracts, and resources (such as medicine information, sales information, etc.). Smart contract is a protocol that allows trusted transactions without a third party. It can realize the automatic setting and invoke access rights. The workflow can be divided into preparation phase and execution phase. The preparation phase mainly manages users, roles, and access control policies, including adding, updating and deleting users, roles, and authorization policies, and responding to the results of roles and policy queries. The access request is judged and executed in the execution phase. This process is shown in Figure 5.

Preparation phase: 1) The user applies for registration and obtains the identity address on the blockchain. After registering in the blockchain, the user can only access/operate the data or access/operate the data through authorized agents; 2) The user sends a request to access/operate the target resource (such as medicine information, sales information, etc.), and the smart contract receives the user's request through the API and makes a response; 3) The smart contract queries the corresponding user-role information through the processEvent( ) function call. Once the query is completed, return the role information that the user has to the smart contract; 4) The smart contract queries the authority level of the role information according to the returned role information; 5) According to the corresponding role-permission, system makes a response and return to the smart contract.

Execution phase: 6) The smart contract returns the permissions and secret keys to the user through the processEvent( ) method to authorize the user; 7) After the user gets the corresponding permissions granted by the smart contract, it immediately sends an access/operation request to the target resource (such as medicine information, sales information, etc.), and user's identity is verified by the secret key to complete the access and operation; 8) relevant settings according to changes in policy management, including adding and deleting users, roles, and permission information.

The introduction of the RBAC access control mechanism in the medicine traceability blockchain, combined with the decentralized and automated authority operation of smart contracts in the blockchain, realize the entire management of medicine data information and its release, update, and cancellation. Through the smart contract based on the RBAC model, the access control strategy process is more flexible and the result is more credible, which effectively improves the security of medicine circulation and the mutual trust between nodes.

IV. THE ALGORITHM OF THE PROPOSED METHOD

In this section, we test the blockchain-based medication anti-counterfeiting and traceability method. We used Python 3.7 in the Anaconda Spyder environment to code the algorithm to simulate the medication information storage and traceability process along the medication supply chain. We discuss the complete implementation details and the algorithms below.

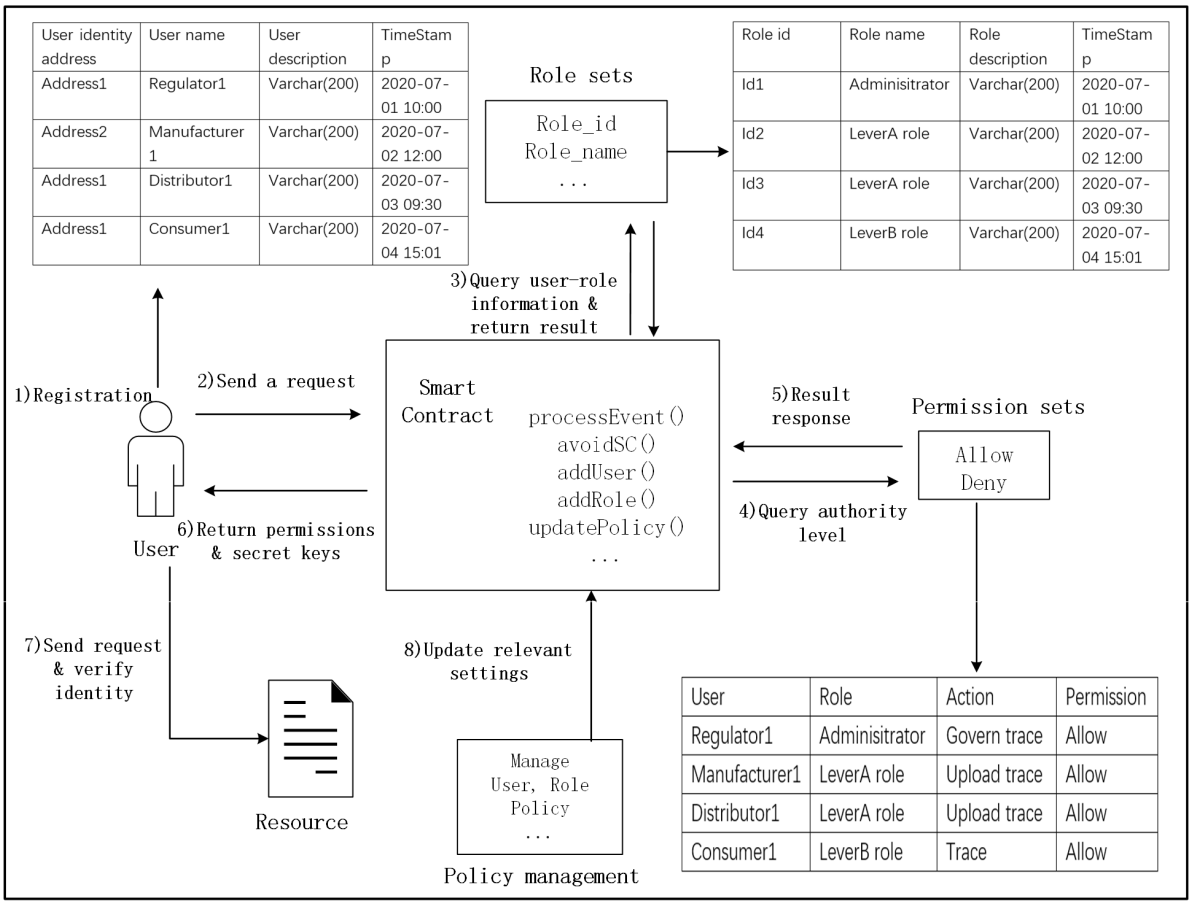


FIGURE 5. The improved PBFT consensus mechanism flowchart.

Algorithm 1 Record or Update Initial Medicine Information

Input: Address, SP state, MedicineID

1 *Address* is the identity mark of the node in medicine circulation; it is unique.
2 **if** *Address* == Manufacturer **then**
3 **if** *SP state* == Not Available information **then**
4 Emit an event to notify every node that an initial medicine information upload with *MedicineID* is submitted.
Generate first block.
SP state = information submitted.
5 **end**
6 **else**
7 Preview an error after returning the contract to its previous state.
8 **end**
9 **end**
10 **else**
11 Preview an error after returning the contract to its previous state.
12 **end**

Our proposed blockchain approach for traceability and medicine anti-counterfeiting is universal. Thus, it can be implemented on public or private blockchain infrastructure. Most of the functions are implemented by using the smart contract. Figure 6 shows the function call and detailed process between the smart contract and the participating entities during the process of medicine distribution/circulation.

The manufacturer initiates the request of medicine information storage on the chain through a blockchain broadcast, and other entities participating in medicine circulation reach a consensus to ensure the request is passed. Then, downstream entities use this request to add information and complete the consensus. In the final stage, all entities can initiate traceability request and obtain approval, and the smart contract sends data to the target entity. More details of the algorithm can be found in the next section.

A. INITIAL MEDICATION INFORMATION UPDATE

The manufacturer is the first link on the medication supply chain. When the medication is shipped, the initial information is updated. The updated information is recorded as the first block onto the blockchain.

B. CONSENSUS OPERATION

Given the information of the shipped medication, go on the chain to request node consensus and verification; only after

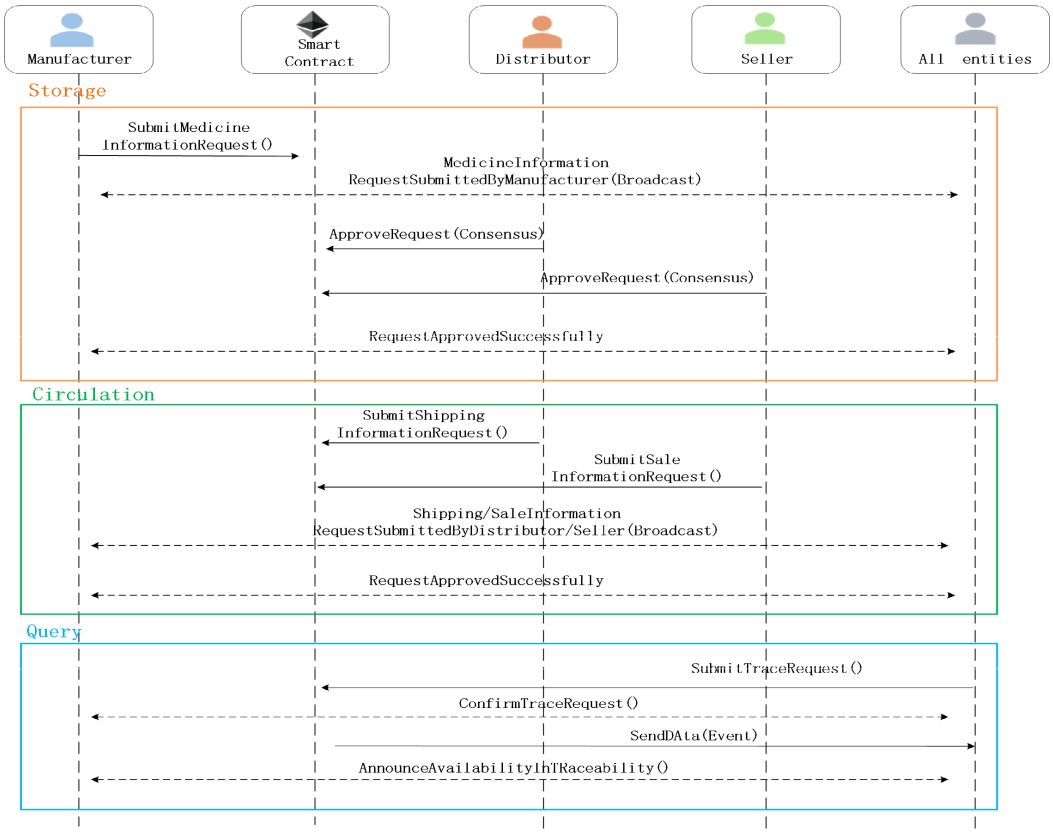


FIGURE 6. Sequence diagram of participating entities interacting with smart contract.

the above step can the medication information be stored onto the blockchain. The client end sends the request to be on the chain, the nodes on the server end go through three steps for consensus (pre-prepare, prepare, and commit) and reach the result (consensus achieved or not). When using the improved PBFT consensus mechanism, there also needs to be reward points or penalty points based on the consensus outcome.

C. MEDICATION FLOW PROCESS

Similar to the medication information recording by the manufacturers, the other nodes on the chain would conduct update and uploading of medication information, eventually forming the blockchain.

D. MEDICATION INFORMATION MODIFICATION

A manufacturer might attempt to modify medication information that is already recorded on the blockchain. The algorithm next compares the current block with its successive block and judge whether the current block is modified; the outcome is demonstrated through data visualization.

E. MEDICATION INFORMATION TRACEABILITY

A node takes the medication ID and the given address to conduct tracing and traceability on the medication information recorded on the blockchain.

V. TESTING AND VERIFICATION

In this section, we will test the proposed method and demonstrate the output with visualization, following the algorithms provided in last section. We will also explain the output of the visualization.

A. MEDICATION INFORMATION STORAGE AND MODIFICATION

Explanation about addresses: the nodes participating in the medication information recording, uploading, and transfer are a manufacturer, a distributor, two sellers, and a consumer. Each node has a unique blockchain address. The simulation involves the following node addresses:

- Manufacturer: 68be0ac013a54d2621cd05b1fef23f3ea35f5c3124ca839cbf6b85c4ee06c8a6
- Distributor: ce5bd83fb6794a4aec4074dd676de84fe7e9614159db325ff02f474f55d06842
- Seller1: c9a00c4809defac64084dea4b620e3cfd7ca0271bf5ba6c6e235ef8e724564ed
- Seller2: 83747c5730268562541975200305125 0d73ebcbec6ec8b8e5842af1fdff4cdf3

Algorithm 2 Consensus Operation

Input: Manufacturer, Master node, Consensus node, Candidate node, Information signature

Manufacturer is responsible for sending information uplink request.
Master node is responsible for the preliminary review of messages, by the supervisor.
Consensus nodes participate in the round of consensus operation.
Candidate nodes are candidate sets of consensus nodes.
Manufacturer sends medicine information uplink request to the *Master node*, and the *Master node* verifies.
if *Information signature*==ture **then**
broadcast a pre-prepare message containing information to *Consensus nodes.*
the *Consensus nodes* validate the pre-prepare message
if Verification passed **then**
broadcast prepare message
if *Consensus nodes* received more than 2f +1 prepare messages **then**
broadcast commit
if *Consensus nodes* received more than 2f+1 commit **then**
reach a consensus and return the result to the *Manufacturer*
end
else illegal request discard
end
end
else illegal request discard
end
end
end
else illegal request discard
end
if round of consensus was successfully completed **then**
add 1 point to each consensus node
end
else
find out dishonest node; deduct from these nodes 50 points; use whole network node to consensus and select the substitute with highest point to enter the consensus node in the *candidate nodes*
end

- Consumer1: cd04f05174f2641f054bc4a7cabc510ac46c065f50a3e39abdcf9268c84fe0e9

The manufacturer, distributor, and sellers would update their own corresponding medication information.

The data elements provided by the manufacturer are: MedicationID, manufacturer information, medicine name, product batch, production date, and expiration date;

Algorithm 3 Construction of Blockchain From Information of Medication Circulation Stages

Input: Address, SP state, MedicineID

Address is the identity mark of the node in medicine circulation; it is unique.
if *Address* == Distributor **then**
if *SP state* == No shipping information **then**
Record shipping information (shipper, delivery time, etc.)
Generate new block with medicine information updated by Distributor.
SP state = information submitted.
end
else
Revert contract state and show an error.
end
end
else
Revert contract state and show an error.
end
if *address* == Sell **then**
if *SP state* == No sale information **then**
Record sale information (sale address, etc.)
Generate new block with medicine information updated by Seller.
SP state = information submitted.
end
else
Revert contract state and show an error.
end
end
else
Revert contract state and show an error.
end
Blockchain is linked according to the block order.
end

Algorithm 4 Tampering With Medication Information

Input: fake medication ID, b, b1

fake medication ID is the medication ID to be modified / forged.
b represents the block already stored on the blockchain.
b1 indicates the next block.
Manufacturer tries to modify medication ID value with *fake medication ID* in block *b.*
if *b1*.previous_hash != *b*.hash **then**
print("invalid block").
end
else
print("valid block").
end

The data elements provided by the distributor are: MedicationID, distributor, receiving party, delivery time;

Algorithm 5 Tracing the medication information

Input: Medication ID, Address

Medication ID is the unique identification code of the medicine, which can accurately identify the medicine information and authenticity.

Address is the identity mark of the node in medicine circulation, and has uniqueness.

if *medication ID* == true and *address* == Manufacturer address **then**

  Create a'query success'notification message.

  Output medicine information updated by Manufacturer (batch number etc.).

end

else

  Notify with a'query failure'message.

end

if *medication ID* == true and *address* == Distributor address **then**

  Create a'query success'notification message.

  Output medicine information updated by Distributor (Delivery information etc.).

end

else

  Notify with a'query failure'message.

end

if *medication ID* == true and *address* == Seller address **then**

  Create a'query success'notification message.

  Output medicine information updated by Seller (Sales location, etc.).

end

else

  Notify with a'query failure'message,

end

if *medication ID* == true and *address* == Consumer address **then**

  Starting from last block to first block.

  Output the current block address.

end

The data elements provided by the sellers are: MedicationID, pharmacy name and address.

The above information is stored on the block chain, with time stamps embedded; a hash value of each block is generated from the provided medication information, and then the new block is connected with the initial block, forming the blockchain, as shown in Figure 7.

At any node, if the node attempts to modify the medication information or to fake a medication, say to change the medication ID from H19990361to H20010413, the outcome would be as the one shown in Figure 8:

Through the comparison of the hash value of the current block with the previous block's hash value, we can tell the invalid block from the valid block – the valid block has a prev-hash value being the same as the hash value of the previous block, which tells that the previous block did not experience a modification; in other words the previous block is authentic and valid. If the previous block were modified, its hash value would have been changed, thus the next block's prev-hash value would not match the hash value of the previous block, so the previous block would be displayed as an invalid block.

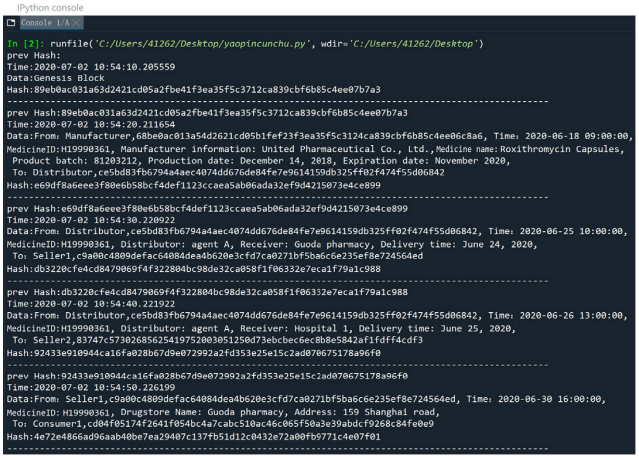


FIGURE 7. Medication information storage and uploading outcome.

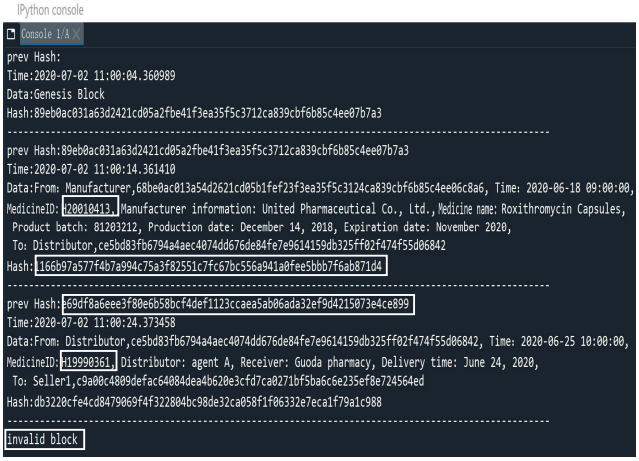


FIGURE 8. The outcome of medication information modification.

From the result we can see that when the ID of a medication on blockchain was modified, the hash value of the original block changed; then the successive block's prev- hash value did not match the hash of the previous block, thus causing the successive blocks becoming invalid.

B. MEDICATION INFORMATION TRACEABILITY

When a consumer acquires a medication, s/he can trace to any node or any given address to obtain the medication information, given the medicationID.

The consumer can input the medicationID and the designated manufacturer's address, s/he can trace the medication back to when it was shipped out; based on this information it can be found out whether or not the medication was swapped

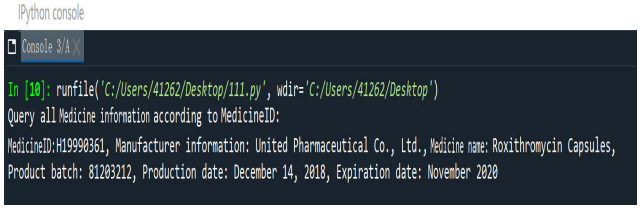


FIGURE 9. Given medicationID, trace the medication information at shipment.

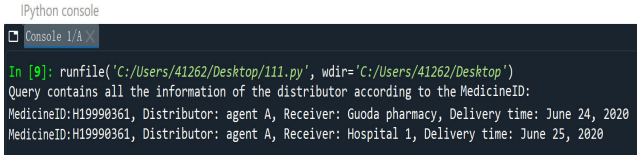


FIGURE 10. Using medicationID to trace a distributor's shipment information

with a counterfeit, or whether or not the medication information was faked.

By entering the medicationID and the designated seller address, one can query all information about the shipments by a seller; this information should demonstrate the whole process for the medication to arrive at the final retail store; thus the consumer can seek accountability regarding whether there were flaws related to that distributor or seller.

FIGURE 11. Given medicationID to trace back to the point of purchase.

Entering the medicationID and a designated seller address, the seller can be queried, achieving precision in locating the purchase place.

At the same time, using the last To-address as the query point, the backward tracing of all outputting entities can be realized, from the ultimate recipient address to the initial input address. This enables the backward tracing of related nodes through the whole blockchain, as shown in Figure 12.

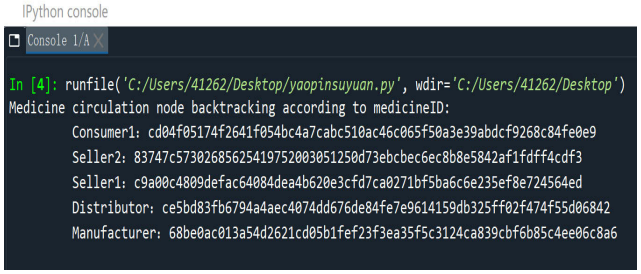


FIGURE 12. Backward tracing of the medication movement along supply chain.

In the step of the testing of medication information storage and modification, each block has a unique identification value; no node can modify the data that has been stored, which warrants that all information is authentic. This effectively lowers the possibility of the medication information being tampered or forged during its transfer. In addition, for the traceability of medication information, the blockchain can, based on a designated hashed transaction address, trace all medication information or transfer process associated with this address. This constitutes the cyclic management of medication in their movement along the supply chain. We now have the desirable "traceability of the source, trackability of the flow, inquire-ability of the information, and accountability of the responsible parties." This desirable state provides complete data and information for the consumers and regulators, which allows themselves to be conveniently updated with the state of anti-counterfeiting task, resulting in improved accountability regarding the related entities.

VI. DISCUSSIONS

In this section, we will evaluate and discuss the proposed anti-counterfeiting and traceability method based on blockchain, from the aspects of security analysis and performance analysis. Performance analysis includes transaction delay comparison, throughput comparison, operational efficiency verification, storage space occupancy, and energy cost evaluation. With comparative analysis, we will verify the reliability and feasibility of the proposed method. We will also discuss the challenges to and future directions for the proposed approach.

A. SECURITY ANALYSIS

We adopt the mathematical model in [34] to analyze the potential risk of the anti-counterfeiting blockchain being attacked. Assuming that the probability of an honest node being generated in a blockchain network is r, and the dishonest node or the attacker faking a block has the probability w; then the attacker nodes would control n nodes in the whole blockchain network with the probability:

$$w_n = \begin{cases} 1, & r \leq w \\ \left(\frac{2}{r}\right)^2, & r > w \end{cases} \tag{1}$$

From the quantitative law regarding the ratio of attacker nodes and legitimate nodes, this ratio satisfies Poisson distribution:

$$\lambda = n\frac{w}{r} \tag{2}$$

Therefore, the attacker would succeed with a probability:

$$p = \lim_{\lambda \to \infty} \sum \alpha < \kappa < \beta \frac{\lambda^{\kappa} e^{-\lambda}}{\kappa^{!}} \left(\frac{r}{w}\right)^2, \quad \kappa = 0, 1, 2, \ldots \tag{3}$$

As the number of both honest and dishonest nodes increases, the probability of a successful attack p would decrease gradually. In a real-world medication information

blockchain network, the improved PBFT algorithm would gradually increase the number of honest nodes; the ratio of dishonest nodes to honest nodes would be substantially lower than the benchmark of a successful attack, hence the proposed method is guaranteed to be extremely difficult to be attacked. Therefore, medication information can be stored and uploaded onto the blockchain in a very secure manner.

From another perspective, the proposed method adopts P2P distributed architecture, which helps to avoid a single-point attack. Meanwhile, the method grants role-based access privileges with great granularity based on the identity of users, ensuring that different stakeholders on the provenance chain have different roles. As a result, our method can ensure the privacy of data uploaded to the blockchain.

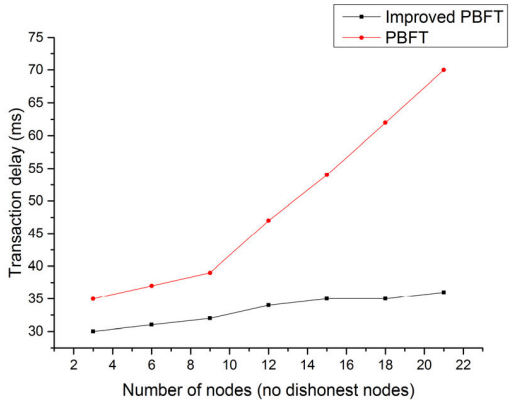
In addition, the storage and traceability of medicine information, as well as the authorization of user rights are mostly realized by writing smart contract code. However, there are some security vulnerabilities in a smart contract, such as external call error, malicious database, timestamp dependence, etc [18]. These unknown vulnerabilities will let hackers attack and compromise transactions. So, we choose two kinds of smart contract vulnerability security checking tools - ''SmartCheck'' and ''Oyente'' - to scan the possible vulnerabilities and errors in the contract code, consequently eliminating the weaknesses in the code. We then adjust the smart contract code according to the results to make it more complete.

B. PERFORMANCE ANALYSIS

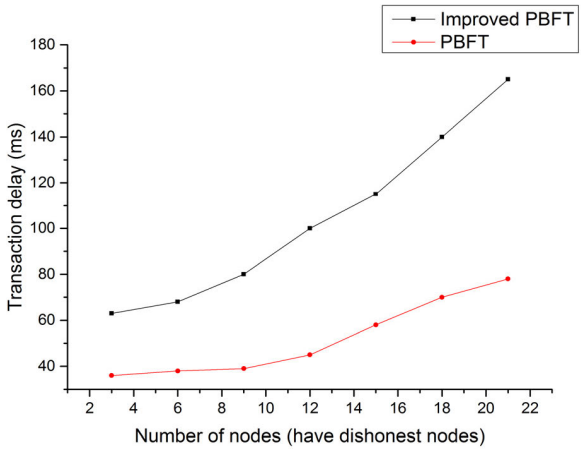
Addressing the issue of consensus mechanism and the generation of the blocks, the current study introduces point-accumulation to the PBFT consensus mechanism, which further improves the mechanism. In the two situations where there exist dishonest nodes and where no dishonest node exists, we make the following comparison of the two mechanisms (with and without point accumulation) on the criteria of transaction time delay and throughput.

Transaction delay is the time interval between the last request for uploading onto the blockchain and the time the consensus feedback is completed. We took 300 transactions with different number of nodes and calculated their transaction time delay. Figure 13 shows the average transaction delay of the two consensus mechanism average, with different number of nodes.

Figure 13(a) shows that, when there is no dishonest node, the improved PBFT has a transaction delay substantially lower than that of PBFT, and that as the number of nodes increases, the improved PBFT has a (significantly lower) transaction delay that increases much more slowly than that of PBFT, forming an almost flat curve. When there exist dishonest nodes, as shown in Figure 13(b), the improved PBFT algorithm would place the priority on switching consensus operation; it (the improved PBFT) will have a higher transaction delay, and that delay is seen to increase at a faster rate.



(a)



(b)

FIGURE 13. (a) Transaction delay between two consensus mechanisms, no dishonest nodes (b) Transaction delay between two consensus mechanisms, with dishonest nodes.

In Figure 14, the throughput is defined as the number of transactions transferred per second (TPS). In this paper, it refers to the number of blocks generated in a given time interval. We took 500 block generation requests with different number of nodes and recorded the number of consensus completed each second. Figure 14 shows the comparison of the two consensus mechanisms, with different number of nodes.

In both Figure 14 (a) and Figure 14 (b), no matter whether there exist dishonest nodes, as the number of nodes on the blockchain increases, the throughput of both mechanisms decreases; but in all cases the throughput of the improved PBFT is significantly higher than that of PBFT (nearly doubled).

For operational efficiency verification, we conducted 300 tracing operations of medication information. The run time and data inquiry efficiency results are shown in Figure 15. From the figure, we can see that the efficiency of using blockchain to track medication information on the blockchain is satisfactory, and the average time for each data inquiry is less than one second.

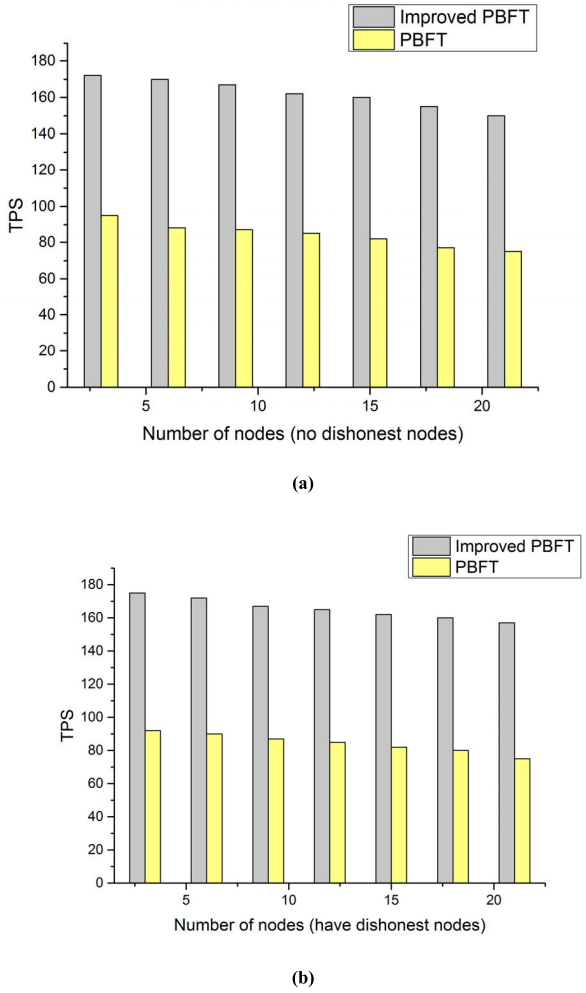


FIGURE 14. (a) Throughput of two consensus mechanisms, with no dishonest nodes. (b) Throughput of two consensus mechanisms, with dishonest nodes.

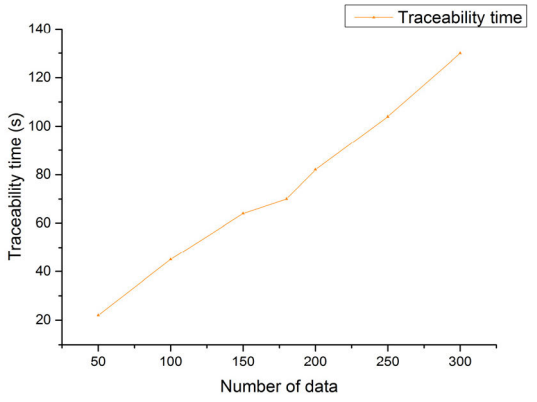


FIGURE 15. Medication information tracing efficiency.

In the existing medication blockchain systems, the consensus mechanisms of PoX series (PoW, PoS, etc.) are mostly used. When the system is started, a large number of medical institutions need to participate in the maintenance of the blockchain at the same time, often consuming significant energy. As a consequence, the energy cost is relatively high and the demand for or the burden on computing power is serious.

The improved PBFT mechanism used in our study only needs more than four nodes to start the system. Compared with the blockchain system based on PoX series, the medication blockchain system method designed in this paper has low energy consumption cost and does not need a lot of computing power to maintain. Therefore, it is more suitable for practical use under many real world scenarios. In addition, in terms of storage space occupation, the CPU utilization rate based on the improved PBFT consensus mechanism is only about 16%, which solves the problem of significant energy costs caused by excessive computing power consumption.

C. COMPARISON ANALYSIS

We compared the blockchain-based medication anti-counterfeiting and traceability method proposed in this study with those in three other articles. The results are listed in Table 1.

TABLE 1. Comparative Analysis.

Performance	This paper	Literature [11]	Literature [12]	Literature [35]
Information traceability	✓	✓	✓	✓
Medicine information integrity	✓	×	×	✓
Information privacy protection	✓	✓	✓	✓
Degree of decentralized storage	high	low	low	high
Efficiency	high	lower	lower	low

From Table 1, the anti-counterfeiting and traceability methods proposed in all four studies (our study and three others) can satisfy the basic requirements, that is, they all can trace the information, and they all take into consideration of preventing privacy infringements in the movement of medications. The method proposed in this study and that in research [35] are both based on blockchain technology; once the information is uploaded to the chain it is not modifiable. Methods with this feature have better information integrity than the other two tracing methods based on IoT. By the same token, the decentralized storage adopted in our method allows all participating medications have an independent and integrated medication flow information, resulting in higher degree of distributedness for the storage. However, how to further increase the degree of distributedness is a challenge that will be discussed in the next section. In terms of efficiency, our method improves the consensus process when the information is uploaded onto the blockchain, and traceability can reach a speed at millisecond magnitude.

D. FUTURE CHALLENGES

The blockchain-based medication anti-counterfeiting and traceability method proposed in this study can effectively address the frequent incidents of medicine counterfeiting, the inaccessibility and isolation of medication information, the difficulty in traceability, and the difficulty in pursuing accountability. As our study demonstrates, the blockchain technology helps to address the above issues, playing a critical role in the proposed method.

However, as an emerging technology, blockchain still faces many challenges in its applications. Firstly, while it is highly desirable that medication information stored on blockchain will be reliable and non-modifiable, the trustworthiness of medication information before uploading on blockchain fully depends on the trustworthiness of each node in the supply chain; the authenticity of such information still needs verification. Secondly, all information is stored on blockchain as proposed, which will demand and consume large amount of storage resources (memory utilization). Future design should address this issue, introduce such architecture as InterPlanetary File System (IPFS) distributed database [36], or to adopt double blockchain architecture [37]. By dividing the medication information into digest and record that are stored separately, these changes can make the proposed method more effective.

In addition, this study employs Python coding to simulate the blockchain operation and the testing of the method; the operation and testing were done only on a single PC rather than a clustering deployment. Whether there can be a better way to construct the blockchain environment in a clustering deployment to increase the effectiveness of the testing should also be studied in future research.

VII. CONCLUSION

The emergence of blockchain technology provides a good beginning point for medication anti-counterfeiting and provenance. Blockchain not only makes the flow of medications along the supply chain more transparent, but it also makes it more effective to conduct anti-counterfeiting and traceability of the medication information. In the pharmaceutical industry, openness and transparency can provide better tracing of the flow of medications, promote mutual trust, and prevent counterfeiting. Consequently, provenance can better hold pharmaceutical companies accountable. Targeting the core needs of the medication supply chain, we analyze the advantages of the blockchain platform, and perfect the anti-counterfeiting and traceability institutions by leveraging blockchain-based data management. At the same time, we improve the conventional PBFT consensus mechanism in the blockchain to enhance system operation efficiency in the process of medicine traceability. Our approach reduces the energy consumption, thereby making the blockchain technology more suitable for medicine traceability and anti-counterfeiting.

While blockchain has been believed to be the technology behind cryptocurrency, it is more important is to apply this emerging technology to various arenas to tap into its unique strengths. For future research, we will further explore blockchain's applications in medication anti-counterfeiting and traceability. The goal is to conduct deeper and more systematic analyses that achieve more beneficial and practical outcomes.

REFERENCES

[1] J. Fei and R. Liu, "Drug-laden 3D biodegradable label using QR code for anti-counterfeiting of drugs," *Mater. Sci. Eng., C*, vol. 63, pp. 657–662, Jun. 2016, doi: 10.1016/j.msec.2016.03.004.

[2] C. M. White, "Counterfeit drugs: A major issue for vulnerable citizens throughout the world and in the United States," *J. Amer. Pharmacists Assoc.*, early access, pp. 1–6, May 26, 2020, doi: 10.1016/j.japh.2020.04.020.

[3] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[4] J. Ma, S.-Y. Lin, X. Chen, H.-M. Sun, Y.-C. Chen, and H. Wang, "A blockchain-based application system for product anti-counterfeiting," *IEEE Access*, vol. 8, pp. 77642–77652, 2020, doi: 10.1109/ACCESS.2020.2972026.

[5] A. Genovese, A. A. Acquaye, A. Figueroa, and S. C. L. Koh, "Sustainable supply chain management and the transition towards a circular economy: Evidence and some applications," *Omega*, vol. 66, pp. 344–357, Jan. 2017, doi: 10.1016/j.omega.2015.05.015.

[6] M. H. Jansen-Vullers, C. A. Van Dorp, and A. J. M. Beulens, "Managing traceability information in manufacture," *Int. J. Inf. Manage.*, vol. 23, no. 5, pp. 395–413, Oct. 2003, doi: 10.1016/S0268-4012(03)00066-5.

[7] P. Olsen and M. Borit, "How to define traceability," *Trends Food Sci. Technol.*, vol. 29, no. 2, pp. 142–150, Feb. 2013, doi: 10.1016/j.tifs.2012.10.003.

[8] M. P. M. Meuwissen, A. G. J. Velthuis, H. Hogeveen, and R. B. M. Huirne, "Traceability and certification in meat supply chains," *J. Agribus.*, vol. 21, no. 2, pp. 167–181, 2003. [Online]. Available: https://research.wur.nl/en/publications/traceability-and-certification-in-meat-supply-chains

[9] T. Bosona and G. Gebresenbet, "Food traceability as an integral part of logistics management in food and agricultural supply chain," *Food Control*, vol. 33, no. 1, pp. 32–48, Sep. 2013, doi: 10.1016/j.foodcont.2013.02.004.

[10] T. Inaba, "Inference of product quality by using RFID-enabled traceability information a study on the US pharmaceutical supply chain," in *Proc. IEEE Int. Conf. RFID*, Apr. 2009, pp. 298–305, doi: 10.1109/RFID.2009.4911170.

[11] B. A. Alzahrani, K. Mahmood, and S. Kumari, "Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure," *IEEE Access*, vol. 8, pp. 76357–76367, 2020, doi: 10.1109/ACCESS.2020.2989305.

[12] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1634–1646, Oct. 2017, doi: 10.1109/JIOT.2017.2706752.

[13] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jun. 27, 2020. [Online]. Available: https://www.bitcoin.org

[14] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]," *IEEE Technol. Soc. Mag.*, vol. 34, no. 4, pp. 41–52, Dec. 2015, doi: 10.1109/MTS.2015.2494358.

[15] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Trans. Eng. Manag.*, early access, Sep. 2, 2019, doi: 10.1109/tem.2019.2928280.

[16] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020, doi: 10.1109/ACCESS.2020.2987831.

[17] Y. Xu and Y. Huang, "Segment blockchain: A size reduced storage mechanism for blockchain," *IEEE Access*, vol. 8, pp. 17434–17441, 2020, doi: 10.1109/ACCESS.2020.2966464.

[18] H. R. Hasan, K. Salah, R. Jayaraman, R. W. Ahmad, I. Yaqoob, and M. Omar, "Blockchain-based solution for the traceability of spare parts in manufacturing," *IEEE Access*, vol. 8, pp. 100308–100322, 2020, doi: 10.1109/ACCESS.2020.2998159.

[19] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019, doi: 10.1109/ACCESS.2019.2897792.

[20] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[21] 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, doi: 10.23919/INM.2017.7987376.

[22] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 568–570, doi: 10.1109/COMSNETS.2019.8711418.

[23] N. Saxena, I. Thomas, P. Gope, P. Burnap, and N. Kumar, "PharmaCrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs," *Computer*, vol. 53, no. 7, pp. 29–44, Jul. 2020, doi: 10.1109/mc.2020.2989238.

[24] K. M. Botcha, V. V. Chakravarthy, and A. Anurag, "Enhancing traceability in pharmaceutical supply chain using Internet of Things (IoT) and blockchain," in *Proc. IEEE Int. Conf. Intell. Syst. Green Technol. (ICISGT)*, Jun. 2019, pp. 45–48, doi: 10.1109/ICISGT44072.2019.00025.

[25] H. L. Pham, T. H. Tran, and Y. Nakashima, "Practical anti-counterfeit medicine management system based on blockchain technology," in *Proc. 4th Technol. Innov. Manage. Eng. Sci. Int. Conf.(TIMES-iCON)*, Dec. 2019, pp. 1–5, doi: 10.1109/TIMES-iCON47539.2019.9024674.

[26] *Blockchain for Supply Chain—IBM Blockchain | IBM*. Accessed: Jul. 12, 2020. [Online]. Available: https://www.ibm.com/blockchain/industries/supply-chain?p1=Search&p4=43700050370610644&p5=e&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-blockchainsupplychain_e&cm_mmca7=71700000060890069&cm_mmca8=kwd-338826950041&cm_mmca9=EAIaIQobChMIx_GJ-pfG6gIVmZOzCh1vqQkgEAAYASAAEgLi8_D_BwE&cm_mmca10=406205979572&cm_mmca11=e&gclid=EAIaIQobChMIx_GJ-pfG6gIVmZOzCh1vqQkgEAAYASAAEgLi8_D_BwE&gclsrc=aw.ds

[27] B. Sohn, K. Kwon, and D. Kim, "GS1 video: Open service system for video using MPEG 7 and GS1 standard," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jun. 2017, pp. 174–181, doi: 10.1109/IEEE.EDGE.2017.31.

[28] L. Duan, Z. Wang, Y. Duan, and Q. Du, "Research on object information retrieval and recommendation based on GS1 standard," in *Proc. IEEE 9th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Nov. 2018, pp. 1–4, doi: 10.1109/ICSESS.2018.8663943.

[29] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2886932.

[30] A. Hafid, A. S. Hafid, and M. Samih, "New mathematical model to analyze security of sharding-based blockchain protocols," *IEEE Access*, vol. 7, pp. 185447–185457, 2019, doi: 10.1109/ACCESS.2019.2961065.

[31] Q. Ding, S. Gao, J. Zhu, and C. Yuan, "Permissioned blockchain-based double-layer framework for product traceability system," *IEEE Access*, vol. 8, pp. 6209–6225, 2020, doi: 10.1109/ACCESS.2019.2962274.

[32] Y. Wang, S. Cai, C. Lin, Z. Chen, T. Wang, Z. Gao, and C. Zhou, "Study of blockchains's consensus mechanism based on credit," *IEEE Access*, vol. 7, pp. 10224–10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[33] E. Coyne and T. R. Weil. (2013). *ABAC and RBAC: Scalable, Flexible, and Auditable Access Management*. Accessed: Jul. 12, 2020. [Online]. Available: https://www.techstreet

[34] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, Jun. 2017, doi: 10.1109/ACCESS.2017.2720760.

[35] 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, doi: 10.1109/Cybermatics_2018.2018.00206.

[36] R. Kumar and R. Tripathi, "Implementation of distributed file storage and access framework using IPFS and blockchain," in *Proc. 5th Int. Conf. Image Inf. Process. (ICIIP)*, Nov. 2019, pp. 246–251, doi: 10.1109/ICIIP47207.2019.8985677.

[37] S. Peng, X. Hu, J. Zhang, X. Xie, C. Long, Z. Tian, and H. Jiang, "An efficient double-layer blockchain method for vaccine production supervision," *IEEE Trans. Nanobiosci.*, vol. 19, no. 3, pp. 579–587, Jul. 2020, doi: 10.1109/TNB.2020.2999637.

PENG ZHU (Member, IEEE) is currently an Associate Professor with the Nanjing University of Science and Technology, China. His main research interests include user behavior, human–computer interaction, blockchain technology, and data traceability. His articles were published on IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, *Electronic Commerce Research and Applications*, among others.

JIAN HU is currently pursuing the master's degree with the Department of Information Management, Nanjing University of Science and Technology. His research interests include blockchain technology and data traceability.

YUE ZHANG (JEFF) is currently a Professor of information systems with California State University, Northridge, USA. His research interests include IT's impact on society, electronic commerce, electronic government, social media applications, and IS/IT governance. His articles were published on *Communications of the ACM*, the *Journal of Electronic Commerce Research, Sustainability*, the *Journal of Internet Commerce*, among others.

XIAOTONG LI is currently a Professor of information systems with The University of Alabama, Huntsville. His research has appeared in many major journals including the *Journal of Management Information Systems, Marketing Science*, and others. He won the best paper of the year award, in 2006, for an article in the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT from the IEEE Engineering Management Society. He has served on the editorial board of *Marketing Science* [INFORMS] and is an Associate Editor of *Electronic Commerce Research and Applications* (Elsevier).