Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5163003, 14 pages
https://doi.org/10.1155/2022/5163003

Research Article

MB-BC: Drug Traceability System Based on Multibranched Blockchain Structure

Xudong Tan,[1] Zerui Kang,[1,2] Fan Wei,[1,2] Chenhao Gao,[1,2] Zhaoying Wei,[3] and Haiping Huang[1,2]

[1]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, 210023 Jiangsu, China*
[2]*Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing, 210023 Jiangsu, China*
[3]*College of Science, Xi'an Shiyou University, Xi'an, 710065 Shanxi, China*

Correspondence should be addressed to Haiping Huang; hhp@njupt.edu.cn

Received 17 May 2022; Accepted 11 July 2022; Published 25 July 2022

Academic Editor: Lei Liu

The establishment of a complete drug traceability system is essentially important for public drug security and the business of pharmaceutical companies which is aimed at tracking where the drug has gone along the drug supply chain. Traditional centralized server-client technical solutions have been far from satisfaction for their bad performances in data authenticity, privacy, system resilience, and flexibility. In this paper, we propose a drug traceability scheme called MB-BC, which realizes the security and traceability of drug data through a novel multibranched blockchain scheme. Different from the characteristics of transparency of traditional blockchains, MB-BC realizes fine-grained access control of data between all levels in the system, which improves the security and privacy of data. MB-BC has further improved the existing consensus mechanism, strengthened the supervision of pharmaceutical companies, and further improved the safety and robustness of the system. Furthermore, the system combines data access strategies with smart contracts; each branch chain can also issue its smart contract to provide personalized services. Finally, security and performance evaluations show that the solution is advantageous in terms of data security, system robustness, supervisibility, and traceability, as well as efficient in terms of blockchain throughput, data query time, and blockchain consensus consumptions, compared with other typical approaches.

1. Introduction

The fact that a large number of people involving children die from counterfeit medicines every year is gradually affecting the credibility of the government and medical institutions due to the improvement of counterfeit technology [1, 2]. How to achieve effective drug supervision still remains challenging for the government.

Drug supervision contains a series of supervisory processes that regulate the development, production, transportation, and purchase of drugs [3]. In 2013, the United States signed the Drug Supply Chain Security Act of the United States (DSCSA) [4] requiring the establishment of an operational electronic information system to identify and trace prescription drugs distributed in the United States. Using technologies such as big data and the Internet of Things (IoT), China has achieved rapid development in drug traceability systems. Pharmaceutical companies usually establish their traceability systems or use third-party traceability systems such as “Ali Health” to identify, read, record, and upload drug data to their respective center databases through technical means such as barcodes and RFID [5]. By scanning the traceable source code on the drug packaging, consumers can quickly identify the authenticity of the drug. The gradual improvement of the traceability system has made a great contribution to the safety of drug supervision.

However, there are still a series of problems hindering the development of a drug traceability system [6]. First of all, the most important thing as a traceability system is the authenticity of the drug data in the system. The centralized data storage will still have the problem of artificial data tampering [7, 8]. There may be a series of illegal operations such as modifying the expiration date, production date, and other key information of the drug to conceal the truth of the fake drug. In addition, the privacy protection of pharmaceutical companies on third-party platforms is also a major problem in the development of drug traceability systems [9]. Generally speaking, the data of each pharmaceutical company should be kept confidential.

The emergence of blockchain provides us with a good solution to the above problems. Blockchain technique combines modern cryptography, point to point communication, and distributed consensus protocol [10, 11]; these techniques will eventually form a blockchain framework. In recent years, many scholars have been absorbed in the drug traceability and supervision system based on blockchain architecture [12, 13]. However, most of the current blockchains are achieved based on Ethereum [14] or Fabric platforms [15], and they usually have been limited to the common block structure, for example, the single-chain structure, which may frequently lead to a series of problems such as fork and system failure [16]. In addition, the low efficiency of the current consensus mechanism is another important reason why the traditional blockchain system is difficult to be widely used [17, 18].

In this paper, an improved blockchain structure-based drug traceability system called MB-BC will be proposed, to achieve the safe traceability of drug data and improve the supervision efficiency of pharmaceutical enterprises. MB-BC inherits the advantages of a traditional blockchain traceability system and overcomes the defects mentioned above. Specifically, the contributions of this paper are summarized as follows:

(i) Based on the characteristics of the drug supply chain and the actual scenario, a drug traceability system model MB-BC is designed, which adopts a new hybrid blockchain structure of main chain and branch chain to realize the supervision of multiple drug enterprise nodes and improve the traceability efficiency of the system

(ii) Our proposal combines ciphertext policy attribute-based encryption (CP-ABE) technology with smart contracts to achieve fine-grained access for users at all levels and ensure data privacy security

(iii) In MB-BC, each branch chain can publish its own smart contract, which can effectively prevent attacks caused by smart contract vulnerabilities. In addition, an improved DPoS consensus mechanism in our proposal can also effectively prevent the concentration of power to a certain person through the review mechanism

The rest of this paper is organized as follows. In Section 2, we present related works. The preliminaries are introduced in Section 3. In Section 4, the system model and security model are presented. In Section 5, we propose a multibranch blockchain system model and introduce the on-chain operation of this model. The access control model based on CP-ABE and smart contract is given in Section 6. In Section 7, we analyze the security of the proposed scheme and evaluate its performance. Finally, we conclude this paper in Section 8.

2. Related Work

In the intelligent medicine scenarios of IoT, how to ensure the security of supply chain data and realize the tracking and monitoring of the medical data is a hot topic of research [19–22]. In 2008, Bitcoin was born, the concept of blockchain was derived from it, and its decentralization, data traceability, and nontampering characteristics [23, 24] provide feasible solutions for a series of security problems in the supply chain. For example, Tian [25] established an agricultural product supply chain traceability system based on radio frequency identification technology and blockchain technology. The system covers the entire process of data collection and information management in each link of the agricultural product supply chain and realizes the quality and safety monitoring and traceability management of agricultural products “from farm to fork.” Even if the relevant technology could also be extended to the drug supply chain, the drug manufacturing supply chain is different from the general production supply chain [26] because of higher requirements for traceability, securit,y and privacy.

In terms of traceability and supervision of the drug supply chain, according to DSCSA, Sinclair et al. [27] focused on the development of blockchain prototype solutions, from the perspective of the drug supply chain security law, explored and used Hyperledger Composer to build a simple drug traceability platform. Jamil et al. [28] also proposed a blockchain-based supply chain to establish trusted medical records for drugs and patients. This solution not only showed the feasibility of building traceability of blockchain platforms but also introduced a smart contract on this basis, which allows patients to check drug information within a limited time. Similarly, B. Alangot and Achuthan [29] also put forward a model for storing drug records called “trace and track.” It combines the framework of the Internet of Things with the blockchain, introduces trust into trustless interactions between stakeholders, and combats counterfeit drugs. Mettler [30] discussed Hyperledger, a research network across industries involving Cisco, Accenture, Intel, IBM, Block Stream, and Bloomberg, and recently launched the Counterfeit Medicines Project where the timestamp in the blockchain is used to attach to the produced medicines to verify the production date of the drug. During the quality monitoring of the above scenario, using blockchain technology, it is possible to detect the source of the product and the transfer between entities, and everyone can join and use it.

In terms of data security and privacy protection, Alzahrani and Bulusu [31] proposed a new supply chain structure called “block-supply” using blockchain and NFC technology, and aiming at medical application, it introduced a corresponding consistency protocol to improve the security of the system model. However, it does not consider the case that the validation leader is malicious and will cooperate with other malicious nodes in this scheme. Huang et al. [32] proposed a blockchain-based solution called "Drugledger." The privacy and security of drug data are ensured by decomposing the service provider into separate entities. To prevent the occurrence of counterfeit drugs, fraudulent customers, and other behaviors, Bocek et al. [33] introduced another blockchain-based medical supply chain, which uses IoT devices and blockchain to monitor drug temperature and data security while reducing the operating costs of the drug supply chain.

To sum up, the drug traceability literature based on blockchain now realizes the traceability and nontampering of drug data. However, it cannot be ignored that most of the literature has not explored the structure of the blockchain itself to adapt to the drug supply chain. The conventional single-chain structure is the root cause of the low efficiency of the blockchain, especially in the drug traceability system. A large number of pharmaceutical companies continue to upload drug production data, which is a huge challenge to the efficiency and scalability of the blockchain system. In addition, for a large number of different entities in the system, how to achieve fine-grained access control, provide personalized services, and ensure data security and privacy within the blockchain is also one of the important reasons that hinder the development of the blockchain drug traceability system. The above challenging issues will become the concerns of this paper.

3. Preliminaries

In this section, we provide some background knowledge needed in this paper, including bilinear pairing, blockchain technology, ciphertext policy attribute-based encryption (CP-ABE) [34], and Delegated Proof of Stake (DPoS) [35] consensus mechanism.

3.1. Bilinear Pairing. An important application of bilinear pairing in cryptography is the construction of short signatures. In the so-called bilinear pair, letG_1,G_2, andG_T be three-cycle groups with the same order$n$and G_1, G_2, and G_T be multiplicative groups. A bilinear map $G \times G \longrightarrow G_T$ has the following properties:

(1) Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for $g_1 \in G_1$, $g_2 \in G_2$, and $a, b \in Z_q$

(2) Nondegeneracy: for each $g_1 \in G_1/\{1\}$, there exists $g_2 \in G_2$and$e(g_1, g_2) \neq 1$

(3) Computability: there exists an efficiently computable algorithm for computing

3.2. Blockchain Technology. Blockchain technology, which originated from the famous Bitcoin virtual currency, has now been separated from Bitcoin as a separate technology. In essence, it is a distributed ledger database maintained by multiple participants, which combines technical features such as cryptography, consensus mechanism, and smart contracts [36], and has decentralized credibility, immutability, transparent data traceability, etc. features. Blockchain consists of three basic concepts:

(1) Transaction: refers to an operation on the ledger in the blockchain network, and the state of the ledger changes once

(2) Block: it is about packaging all transaction data within a period and generating a new block by the consensus mechanism. Each block is divided into a block header and a block body. The block header contains the hash value of the previous block, which is used to connect to the previous block, and also includes the timestamp and the hash value of the block body. The block body mainly contains transaction data organized in the form of a Merkle tree

(3) Chain: a data chain consisting of a series of blocks containing a large number of transactions

3.3. Ciphertext Policy Attribute-Based Encryption (CP-ABE). In 2006, a new cryptographic primitive CP-ABE was proposed, which provides attribute-based access control. By using CP-ABE, users can specify access policies for data encryption based on logical expressions of user attributes before uploading to a third-party database. The key agency will assign corresponding user attributes as the user's identity according to the different users. CP-ABE guarantees that only users whose attributes satisfy logical expressions can decrypt data and achieve fine-grained access control. The general CP-ABE algorithm consists of four basic steps:

(1) Setup. Generate master key MK and public parameter PK

(2) $\mathrm{CT} = \mathrm{Encrypt}(\mathrm{PK}, M, T)$. Use PK, access structure T, and encrypted data plaintext M to generate encrypted ciphertext CT

(3) $\mathrm{SK} = \mathrm{KeyGen}(\mathrm{MK}, A)$. Use MK and the user attribute set A to generate the user's private key SK

(4) $M = \mathrm{Decrypt}(\mathrm{CT}, \mathrm{SK})$. Use the private key SK to decrypt the ciphertext CT to obtain the plaintext M

3.4. Delegated Proof of Stake (DPoS). DPoS is designed to solve the performance problems of the PoW [37] algorithm and the risk problems caused by a small number of nodes holding a large number of shares that may appear in the later stage of the PoS [38] algorithm. In the DPoS algorithm, the PoS share mechanism is retained, and a method similar to the voting mechanism of the board of directors in modern enterprises is adopted [39]. Nodes use the shares they hold to vote for a small number of nodes called witnesses, and these witness nodes will act for the rest of the nodes to complete block generation and verification. By reducing the requirements for the number of confirmations, the DPoS algorithm greatly improves the speed of transactions and the blocks produced by the witnesses will be verified by subsequent witnesses. The advantage of this is that other ordinary equity nodes do not need to spend additional

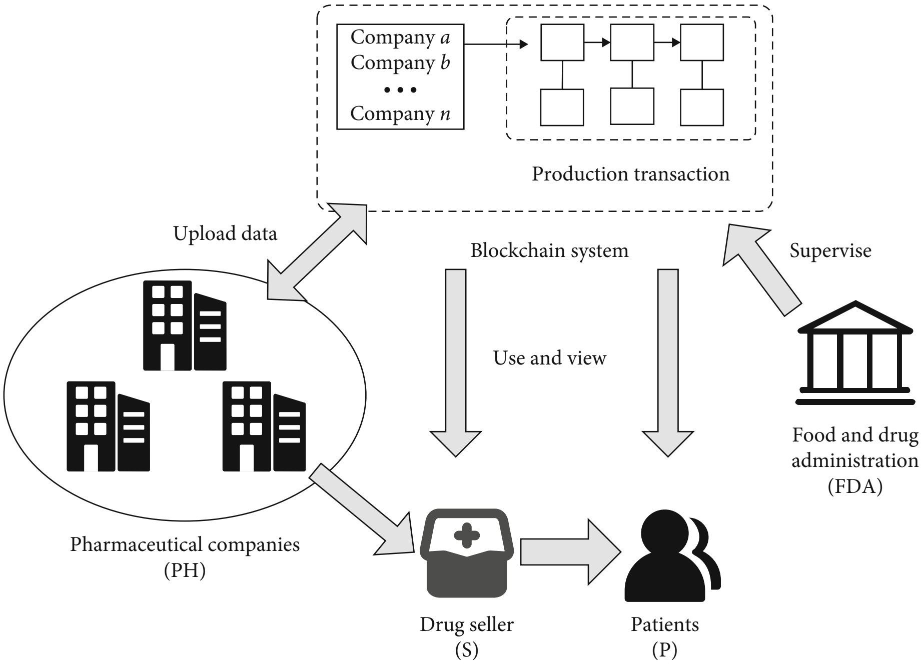


Figure 1: System model.

resources to verify each transaction. Stakeholders can vote for nodes they trust. After the system selects the witness node; if any node has doubts about the witness node, they can choose to exit.

4. Problem Statement and Model

4.1. System Model. As can be seen in Figure 1, the drug traceability system involves four entities: Food and Drug Administration (DA), pharmaceutical companies (PH), drug sellers (S), and the patients (P).

DA: the Food and Drug Administration is a trusted third-party organization managed by the government. As a government agency, DA is the generator of the main chain block and responsible for the supervision and management of system nodes. Also, it is responsible for system initialization and assistance department node registration work.

PH: pharmaceutical company, uniquely identified by PH, is the main data generator of the traceability system, and all drug data of PH will be packaged and added to the corresponding branch chain. According to the different functions, each company is classified into general department node or leader department node and only one leader department node exists in the branch chain.

S: drug seller, uniquely identified by S. The main drug sellers here include hospitals and pharmacies. They both buy medicines from PH and sell medicines to patients. So, they can flexibly join the corresponding branch chain.

P: patients, uniquely identified by P, can purchase medicines from a licensed drug seller S and trace the authenticity of the drugs through the drug code on the package.

At a higher level, the operation process of the drug traceability system based on MB-BC is as follows. First, PH presents the relevant legal operation certificate to DA and reports the relevant information of the company, and DA grants the authority and generates a block on the system main chain for the company. And then, the various departments under it will also register as general nodes in the system, generate drug production data, and upload it to the blockchain system after a consensus mechanism. Under this system model, the operations between companies are independent, and personalized smart contracts can be issued on their respective branch chains without interfering with each other. The data on the chain can be traced and cannot be tampered with. At the same time, CP-ABE and smart contracts are used to ensure data privacy and security and avoid unfair competition among pharmaceutical companies.

4.2. Security Model. In the MB-BC system model, DA is completely trustworthy. As a government agency, it is responsible for maintaining the stability of the drug market and supervising drug data. The pharmaceutical companies and drug sellers are semitrusted. Drug production data is the core secret of PH. In the face of all kinds of interest temptations, some pharmaceutical companies may perform a series of illegal operations, such as stealing production data from other pharmaceutical companies and colluding attacks. In a worse situation, some pharmaceutical company nodes may damage the system, such as block generation errors and issuing smart contracts with vulnerabilities.

5. Multibranch Blockchain (MB-BC) System and Solution

In this section, we propose the MB-BC structure and introduce the characteristics of the MB-BC, including main chain generation, data upload, smart contract, and consensus mechanisms.

5.1. System Setup. DA selects the group G_1 and G_2, where the order of G_1 is q and g is the generator of G_1. Then, DA defines a bilinear mapping: $G_1 \times G_1 \longrightarrow G_2$ and select two hashes: $H_1 : \{0, 1\}^* \longrightarrow G_1^*$ and $H_2 : \{0, 1\}^{256}$. DA randomly select $\alpha, \beta, r \in Z_p^*$, where $Z_p^* \in (1, 2 \cdots p - 1)$ and generates the system public key $\mathrm{MPK} = \{h = g^{\beta}, f = g^{1/\beta}, e(g, g)^{\alpha}\}$, and the system master secret key is $\mathrm{MSK} = \{r, \beta, g^{\alpha,}\}$. DA will broadcast MPK to the entire blockchain network. To simplify the description, the meaning of some special characters is shown as Table 1.

5.2. Main Chain Generation. Suppose that a pharmaceutical company PH_A wants to join the traceability system; first, the leader department D_m of PH_A needs to register through the platform, that is, fill in various registration information in the system and record it as $(m_{m1}, m_{m2} \cdots m_{mn})$; among them, $(m_{m1}, m_{m2} \cdots m_{mn})$ are the plaintext of registration information. After the review of DA is passed, the company's registration information is packaged into several transactions $M_{\mathrm{trans}D_m} = (\mathrm{Trans}_{m1}, \mathrm{Trans}_{m2} \cdots \mathrm{Trans}_{mn})$, where $\mathrm{Trans}_{mn} = (m_{mk}, m_{m(k+1)} \cdots m_{mn})$, then put $M_{\mathrm{trans}D_m}$ into the transaction buffer to wait for upload to the blockchain.

DA generates a unique number $\mathrm{ID}_d \in \{0, 1\}^*$ for PH_A and a key pair for the identity authentication of the leadership department and calculates $S_{\mathrm{ID}_d} = H_1(\mathrm{ID}_d) \in G_1^*$, the private key $\mathrm{sk}_m = r * S_{\mathrm{ID}_d}$, and the public key $\mathrm{pk}_m = g^{\mathrm{sk}_m}$. The public key pk_m is broadcast to the entire network by DA, and the private key is kept by D_m.

After completing the above steps, a new main chain block is generated for PH_A. As shown in Figure 2, the block includes a block header and a block body. The block header contains 4 bytes of the version number, 4-byte timestamp, 32-byte previous block hash, 4-byte organization number ID_d, 32-byte Merkle root, and 4 bytes of branched-chain distinction. The block body is the Merkle tree composed of PH's registration information $M_{\mathrm{trans}D_m}$. After the generation is completed, DA will broadcast the updated main chain to the entire network, and the rest of the nodes will update the blockchain after verification. In addition, similar to the general blockchain system, we will initially allocate 10 virtual currencies for PH_A, which is called PHgas in this scheme. Through PHgas, functions such as executing smart contracts can be completed.

In addition to the only leader department D_m, the rest such as production workshops and research and development departments are collectively referred to as general departments, denoted as $\{D_{s1}, D_{s2}, \cdots, D_{sn}\}$. After the registration is completed by D_m, general node D_{sn} will package the registration information $M_{\mathrm{trans}D_s} = (\mathrm{Trans}_{s1}, \mathrm{Trans}_{s2}, \cdots, \mathrm{Trans}_{sn})$, the number of the company ID_d, and the signature of the leader department which is defined as $\mathrm{Sign}_m = H_1(M_{\mathrm{trans}D_s})^{\mathrm{sk}_m}$ sends them to DA. DA verifies the authenticity of the signature by calculating $e(\mathrm{Sign}_m, g) = e(H_1(M_{\mathrm{trans}D_s}), \mathrm{pk}_m)$. If the equation holds, the verification is successful, and the node obtains the attributes $\mathrm{ID}_{sn} \in \{0, 1\}^*$ and associates ID_{sn} with ID_d, which means that the node is a subordinate department of PH_A. Finally, DA generates the identity authentication key pair $\{\mathrm{sk}_{sn}, \mathrm{pk}_{sn}\}$ for D_{sn}; among them, the private key is $\mathrm{sk}_{sn} = r * H_1(\mathrm{ID}_{sn})$ and the public key is $\mathrm{pk}_{sn} = g^{\mathrm{sk}n}$

Table 1: Common notation description.

Notations	Descriptions
q	Order of the group G_1
g	Generator of the group G_1
α, β, r, r_j, s	Secret value randomly generated by DA
$M_x \in \{i, \mathrm{trans}D_m, \mathrm{trans}D_s\}$	Plaintext data of drug data or registration information
Trans	Transaction packaged by data
$\mathrm{sk}_x, x \in \{m, s\}$	The private key of the nodes in the blockchain system
$\mathrm{pk}_x, x \in \{m, s\}$	The public key of the nodes in the blockchain system
ID_x, x ∈ {d, s}	Unique ID of the nodes in the blockchain system
PT	Access policy tree of CP-ABE
N	Nodes in the access policy tree
A	Attributes of the access policy tree
x	The number of child nodes of N in the access policy tree
K_N	The threshold value of each node N
y	The number of nodes in the access policy tree
$\tilde{C}, C, C_i$	Encrypted ciphertext set of CP-ABE
D, D_j, D_j^*	Decryption key set of CP-ABE

5.3. Data Upload. After the registration is completed, D_{sn} becomes a general node in the blockchain system and can upload "transactions" (i.e., drug production data) to the blockchain. Every time a piece of production data is generated, the data is packaged into a "transaction," which is recorded as $\mathrm{Trans} = \{\mathrm{CT}, \mathrm{Token}_{\mathrm{drug}}, \mathrm{ID}_d, \sigma_e\}$. The structure of the "transaction" is shown in Figure 3. Each piece of "transaction" contains the following content: CT is encrypted production data, which can be used for drug identification and retrospective use. $\mathrm{Token}_{\mathrm{drug}}$ is a specific type of drug, to distinguish subsequent lookups. ID_d is the number of the PH to which it belongs for witness classification. $\sigma_e = H_2(\mathrm{CT}, \mathrm{Token}_{\mathrm{drug}}, \mathrm{ID}_d)$ is the hash fingerprint of the first three to ensure that the transaction is not tampered with during transmission.

The general node sends the Trans and the signature $\mathrm{Sign}_s = H_1(\mathrm{Trans})^{\mathrm{sk}_{sn}}$to the network together. After the consensus witness node receives this message, it verifies the Sign_s and judges whether $e(\mathrm{Sign}_s, g) = e(H_1(\mathrm{Trans}), \mathrm{pk}_{sn})$ is established. If the equation holds, the verification is successful.

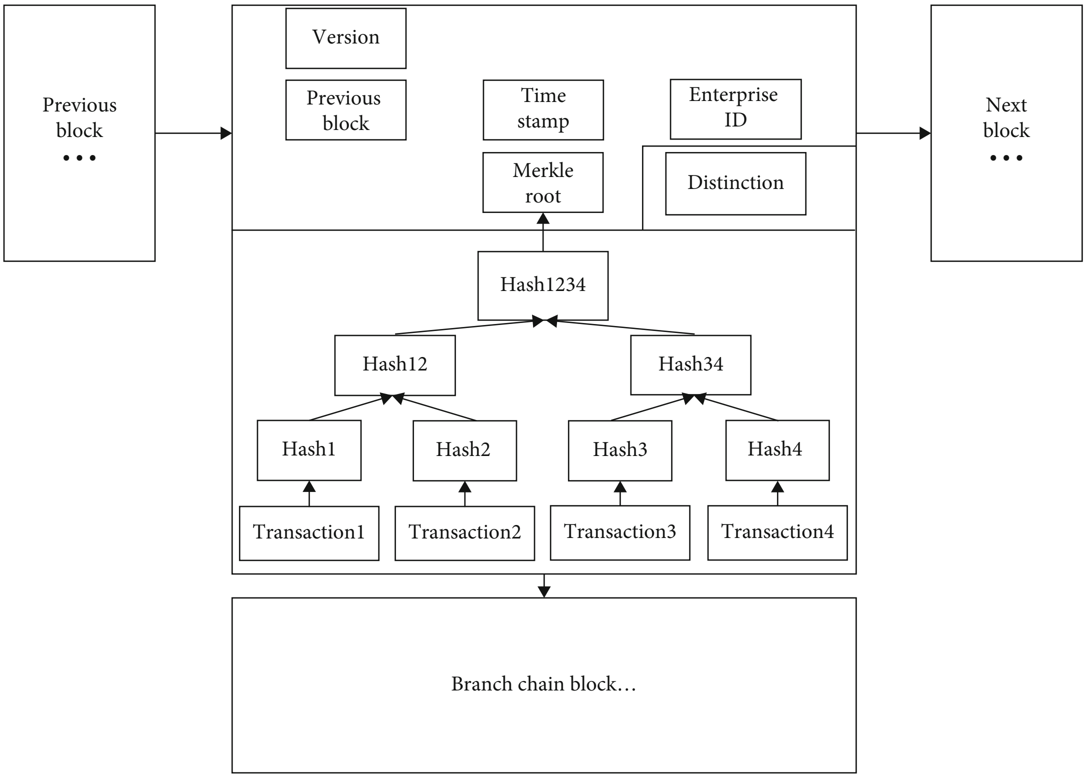


Figure 2: Multibranch block structure.

Encrypt data CT	Drug token	Enterprise ID	Verify hash

Figure 3: The structure of the "transaction."

The witness node accepts the Trans, sorts it according to the company number ID_d in the "transaction," puts it into the data buffer, and waits for packaging. When the transaction in the data buffer reaches a certain number, the current witness node packs the classified transactions and adds them to the corresponding branch chain. The remaining witness nodes verify the current witness node's decision and judge whether there is a classification error. After the verification is passed, the branch chain block is generated successfully and broadcast to the entire network for the update. The above process involves the workflow of the consensus mechanism, and the specific steps will be given in detail in Section 5.4.

5.4. Smart Contract. We use a smart contract called policy tree update contract to automatically update the access policy tree required for attribute-based encryption. The updated access policy tree is also recorded in the blockchain to ensure that it cannot be tampered with. If the leader department of pharmaceutical company needs to update the access strategy tree, it can be achieved through this smart contract. The major work of the access policy tree update contract is formally described in Algorithm 1.

As shown in the algorithm, some departments or drug sellers join or leave the system, the pharmaceutical company expects to update the access policy tree privileges, and then, the smart contract needs to be invoked by the leader node D_m. The leader node D_m needs to take the latest access policy tree $\mathrm{PT} \in \{0, 1\}^*$, the storage address $\mathrm{Dateplace}_{\mathrm{PT}}$ and $\mathrm{PT}'s$ signature $\mathrm{Sign}_{\mathrm{PT}}$ as input to generate $\mathrm{Trans}_{\mathrm{PT}}$ containing the updated access policy tree. Then, it proceeds to the initialization stage, where time is the times that the password can be entered during the payment period, and $\mathrm{Label}_{\mathrm{trans}}$ is the label of $\mathrm{Trans}_{\mathrm{PT}}$ output by the algorithm (Line 1). After the initialization is completed, the signature of the leader node D_m needs to be verified to ensure that D_m is the executor of the contract (Lines 2-4). If the verification is passed, it will start to updating the policy tree. If the current executor's account balance is larger than the PHgas consumed by the transaction, the user needs to enter the account password (Lines 5-9). If the user enters the password correctly within three times, the smart contract will replace the previously stored policy tree address in the previous transaction with the updated $\mathrm{Dateplace}_{\mathrm{PT}}$, calculate the hash fp of the $\mathrm{Dateplace}_{\mathrm{PT}}$, and finally output the updated $\mathrm{Trans}_{\mathrm{PT}}$ (Lines 10-19). The previous access strategy tree address of the system will be changed to $\mathrm{Dateplace}_{\mathrm{PT}}$ after successful payment, and the latest strategy tree will be packaged into transaction $\mathrm{Trans}_{\mathrm{PT}}$ to be recorded in the chain.

```
Input: New policy tree PT, New policy tree's address $\mathbf{Dataplace}_{PT}$, Signature of PT $\mathbf{Sign}_{PT}$
Output: $Trans_{PT}$
initialize: Set $\alpha = H_1(PT)$, $times = 0$, $Label_{trans} = \{policytree\}$
if $(Sign_T, g) = e(\alpha, pk_m)$ then
    $Verifysucess$;
    $Payer \longleftarrow ID_d$;
    if $Balance_i d \geq gap$ then
        Input paymeent password Pw;
        while Pw is not true and time ≤3 do
            time++;
        end while
        if time≤3 then
            $Treeplace_{PT} \longleftarrow Dataplace_{PT}$;
        else return Account lock;
        end if
    else return Insufficient balance;
    end if
end if
$fp \longleftarrow H_2(\alpha)$
$Trans_{PT} \longleftarrow \{Treeplace_{PT}, fp, ID_d, Label_{trans}\}$
return $Trans_{PT}$
```

Algorithm 1: Policy tree update contract.

In addition, it needs to be emphasized that smart contracts are set up under each branch chain; it means each PH can release its smart contracts under its branch chains, such as pharmacy authorization contracts and medical dividend smart contracts. By publishing personalized smart contracts, companies can adjust their business models according to the company status, so that the system is more practical. At the same time, these smart contracts are only valid under the branch chain, avoiding attacks against smart contract vulnerabilities similar to the DAO [40] incident.

5.5. Consensus Mechanisms. We choose the DPoS as the consensus mechanism of our system. In the consensus phase of this scheme, three types of role nodes are involved: ordinary node, candidate node, and witness node. Ordinary nodes are general department nodes and have the right to vote. The candidate nodes are selected from all the leader department nodes of pharmaceutical companies through voting. According to our scoring review mechanism, the weight of each node is calculated and ranked. The top-ranked nodes become witness nodes, and the rest are candidate nodes. Specific steps are as follows:

Voting stage: assume that the number of pharmaceutical companies in the whole network is N_m; that is, there are also N_m leader nodes, and N_T witness nodes need to be selected. Meanwhile, to prevent a large number of malicious nodes, N_T candidate nodes need to be selected. Except for the leader nodes, the rest of the general nodes vote according to their wishes.

Witness election stage: Algorithm 2 shows the witness node election method. The algorithm finally outputs two node sets R_1 and R_2, where R_1 is the witness node set and R_2 is the candidate node set. At the beginning, the system initializes the number of votes for the election node $\{\text{Vote}_i = 0, i \in (0, N_m)\}$ and counts their true votes (Lines 1-6). At the same time, to vote more fairly, weights are added to the algorithm to calculate the final votes. The weight mainly has T_{error} and Count_{ph}. There are two considerations. T_{error} represent the number of failures or errors in generating blocks when the node is used as a witness node, and $T_{\text{error}} = 0$ is set by default. Count_{ph} is the breadth of voting sources. Simply put, it is the number of PHs that you get the votes from. For example, if the remaining preconditions are the same, node A received 80 votes from only one PH, $\text{Count}_{\text{ph}} = 1$, and node B received a total of 40 votes, but these 40 votes came from three different PH, $\text{Count}_{\text{ph}} = 3$, and the final number of valid votes of V_B is greater than that of V_A. This can effectively prevent collusive voting between pharmaceutical companies and improve the fairness of voting. The smart contract calculates and sorts the final votes based on the weight (Lines 7-11). Among them, $\text{Weight}_i = \text{Count}_{\text{ph}}/(r_d + T_{\text{error}})$, r_d can be adjusted by DA as a threshold. According to the voting ranking, the first N_T nodes are elected as witness nodes and the next N_T nodes are candidates (Lines 12-14).

Witness work stage: witness nodes generate blocks in sequence as required, and the generated blocks are verified by other witness nodes. According to DPoS, after the block is verified by $(2/3)N_T + 1$ other witnesses, the block will be added to the blockchain. If the verification is successful, the current block generating node will receive a certain PHgas reward, and the remaining verification nodes will also receive a little PHgas reward. If there is a failure or error in block creation, the DA will review this behavior. The T_{error} of the witness node will be increased by one if it is a malicious behavior or an error can be avoided, and it will be included in the weight in the next cycle of elections.

```
Input: S(set of nodes), $N_m$(number of leading nodes), $N_m$(number of general nodes), $N_T$(number of witness nodes)
Output: $R_1$(set of witness nodes), $R_2$(set of alternate nodes)
initialize: Set $Vote_i = 0$
for $i = 1$ to $N_m$ do
  for $j = 1$ to $N_{sn}$ do
     $Vote_i \longleftarrow Vote_i + Caculate_j$;
  end for
  return $Vote_i$
$Weight_i \longleftarrow (float)(caculateWeight(T_{error}, Count_{ph}))$;
  Real$Vote_i \longleftarrow (Int)(Weight_i * Vote_i)$;
end for
return $RealVote_i$
$N_x^{set} \longleftarrow quickSort(RealVote_i)$;
$R_1 \longleftarrow N_x^{set}(x \in [0, N_T - 1])$;
$R_2 \longleftarrow N_x^{set}(x \in [N_T, 2N_T - 1])$;
return $R_{1,}R_2$
```

Algorithm 2: Witness node election method.

6. Data Access Security

6.1. Access Policy Initialization. The leader department of the pharmaceutical company generates an initial access policy tree according to the actual situation, and the access policy tree structure is shown in Figure 4. The access policy tree mainly has two functions "And" and "Or." If the function implemented by the node is "And" and the number of child nodes is x, the applicant must meet the attributes of x child nodes to successfully execute the decryption algorithm of this layer. If the function implemented by the node is "Or," the applicant only needs to meet the attributes of one of the child nodes to execute the decryption algorithm of this layer. Taking this access policy tree in Figure 4 as an example, the applicant accesses the access policy tree and observes it from bottom to top. In the beginning, the applicant must satisfy the attribute set $\{A_{\text{consumer}}, A_{\text{first}}\}$ or $\{A_{\text{ID}_d}, A_{\text{effective}}\}$; among them, the attribute set $\{A_{\text{consumer}}, A_{\text{First}}\}$ means that consumers who use drugs for the first time meet the requirements, and attribute set $\{A_{\text{ID}_d}, A_{\text{effective}}\}$ means that the valid identity of the applicant must be the department associated with the ID_d.

6.2. Access Policy Storage. Assuming that the drug seller S_A and PH_A have reached a cooperation, S_A become a node in the PH_A's branch chain after the registration is completed, DA will assign the attribute $A_{S_A} \in (0, 1)^*$ to S_A, and D_m will update the structure of the access policy tree according to the attribute A_{S_A} . After that, the leader node D_m needs to update and save the new access policy tree $\text{PT} \in (0, 1)^*$; D_m first saves the access policy tree locally and executes the access policy tree update smart contract mentioned in Section 5. According to Algorithm 1, $\text{Trans}_{\text{PT}} = \{\text{Treeplace}_{\text{PT}}, \alpha, \text{ID}_d, \text{Label}_{\text{PT}}\}$ will be uploaded to the blockchain to ensure that PT and the storage address $\text{Treeplace}_{\text{PT}}$ are not tampered with.

6.3. Data Encryption Stage. D_{sn} is a general node under PH_A and is responsible for drug production. M_i is a piece of production data, and the storage address is Dateplace_{Mi}. D_{sn} inputs the data hash value $H_2(M_i)$ and Dateplace_{Mi} as the message plaintext, and DA will execute the CP-ABE encryption algorithm as follows:

(1) DA backtracks the branch chain of PH_A and finds the latest transaction with Label_{PT}. D_{sn} gets the Trans_{PT} and verifies whether the PH_A's ID is correct and then obtains the access policy tree $\text{PT}_{\text{get}} \in (0, 1)^*$ according to the $\text{Treeplace}_{\text{PT}}$ and verifies that $\alpha = H_1(\text{PT}_{\text{get}})$; if the verification is successful, it means the access policy tree under $\text{Treeplace}_{\text{PT}}$ is valid and usable

(2) DA makes the PH_A's access policy tree $\text{PT}_A = \text{PT}_{\text{get}}$; among them, PT_A's attribute set is A_p and node set $N = \{N_1, N_2, N_3 \cdots N_y\}$, k_N is the threshold value of each node N, and then, arbitrarily select a k-degree polynomial q_N, where $k = k_N - 1$; DA randomly select $s \in Z_p$, where s is the secret value

(3) DA set $q_{\text{root}}(0) = s$ to generate $q_N(0) = q_{\text{parent}N}(\text{index}(N))$ recursively according to the access policy tree, where parent$N$ is the parent node of node N and index(N) is the subscript of N under the tree rooted at parent$N$. D_{sn} obtains the ciphertext: $\text{CT} = (C^{\sim} = M_i * e(g, g)^{\alpha s}, C = h^s, \forall i \in A_p : C_i = g^{q_i(0)}, C_i^* = H_1(\text{att}(i))^{q_i(0)})$, where α, s, h, g have been given in the system setup step, and A_p is a set of attributes containing all attributes. The function att(i) is defined only if i is a leaf node and denotes the attribute associated with the leaf node i in the tree. Finally, D_{sn} packages it into $\text{Trans}_{\text{CT}} = \{\text{CT}, H_2(\text{CT}), \text{PT}_{\text{get}}\}$ and uploads it to the blockchain

6.4. Data Decryption Stage. In the decryption stage, the data applicant may be a patient who purchases the drug or a node

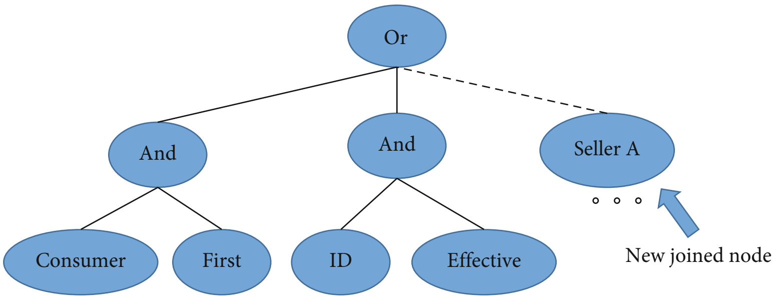


Figure 4: Initial access policy tree.

under the PH. If the applicant is patient P, it will be registered by scanning the drug package, and the system will automatically generate a temporary attribute set $A_u = \{\text{consumer}, \text{first}\}$for the patient; in the second case, the node will directly apply for the private key from DA through its attributes. The specific decryption steps to obtain the private key are as follows:

(1) DA generates a private key for the data applicant. For each attribute in the applicant attribute set A_u, DA chooses $r_j \in z_p^*$ and calculates the applicant's private key as $\text{SK}_u = \{D = g^{(\alpha+r)/\beta}, \forall j \in A_u : D_j = g^r H_1(j)^{r_j}, D_j^* = g^{r_j}\}$

(2) According to the $\{\text{Token}_{\text{drug}}, \text{ID}_d\}$ requested by the data applicant, the system will first lock the corresponding branch chain according to the ID_d and then obtain all relevant drug data ciphertexts in the branch chain according to the $\text{Token}_{\text{drug}}$

(3) The CP-ABE decryption algorithm is executed to decrypt the ciphertext CT: let $n = \text{attr}(i)$, for the leaf node i in the access policy tree and the decryption algorithm $\text{Decrypt}(\text{CT}, D, x_i) = (e(D_i, C_n))/D_i^*, C_n^* = e(g, g)^{rq_x(0)}$. For the nonleaf node i of the access policy tree, the decryption algorithm calculates $\text{Decrypt}(\text{CT}, D, x_i) == e(g, g)^{rs}$. According to the above principles and algorithms, the access policy tree is traversed from bottom to top, and the plaintext $M_i = C^{\sim} /(e(C, D)/e(g, g)^{rs})$ is finally obtained

(4) Finally, the timestamp and the plaintext production data are combined with specific traceability information for consumers to verify the authenticity of the drug. If the data applicant is a patient, to prevent the second use of the drug packaging, the attribute$\{first\}$will be deleted after the first use is completed

7. Scheme Analysis

In this section, we perform a security analysis of our scheme with existing schemes in terms of four aspects: data security, system robustness, supervisibility, and traceability. We also compare the blockchain throughput, data query time, and blockchain consensus consumption of our approach in terms of performance. The security analysis and performance evaluation show that our scheme is secure and efficient.

7.1. Security Analysis. The security of the system will be analyzed. Blockchain and attribute-based encryption provide a strong security guarantee for the system. Compared with the latest solutions in Table 2, our scheme has the advantages of decentralization, data privacy and security, and supervisability. Also, our proposal designs consensus mechanisms and smart contracts to strengthen the safety supervision and system robustness. In summary, the system has the following security features:

(1) *Anticollision attack*: our scheme can effectively prevent collision attacks among different users. Specifically, for the secret value s of attribute-based encryption, the decryption operation $\text{Decrypt}(\text{CT}, D, x_i) == e(g, g)^{rs}$ does not directly derive the secret value, thereby preventing other users from conducting collision attacks and stealing drug production data

(2) *Access policy tree security*: our scheme can effectively prevent the attribute secret key access policy tree from being tampered with or replaced. Assuming that there is a node of PH_A is untrustworthy, it will try to change the access policy tree so that they can obtain the secret key and steal the drug data of other PHs. There may be two types of attacks against access policy trees. The first is access policy tree address tampering. In our scheme, the address of the access policy tree $\text{Treeplace}_{\text{new}}$ is stored in the blockchain and according to the characteristics of the blockchain, the adversary cannot change the address of the access policy tree to another address; the second is to directly change the structure of the access policy tree. When the general node applies for the secret key, the system will find the access policy tree information $\text{Pack}(\text{Treeplace}_{\text{new}}, \text{fp}_T)$ in the blockchain, obtain the T_a of the access policy tree saved under the $\text{Treeplace}_{\text{new}}$, and verify and calculate the equation $H_2(H_1(T_a)) = \text{fp}_T$. Any change to the access policy tree must result in the equation being broken, thereby ensuring that the access policy tree will not be modified

Table 2: Comparison of drug traceability schemes.

Proposal	Architecture	Data confidentiality	Smart contract	Robustness	Supervisability	Traceability
Sinclair et al. [27]	Blockchain-based	×	×	×	×	√
Huang Y. et al. [32]	Blockchain-based	×	×	×	√	√
Jamil et al. [28]	Blockchain-based	×	√	×	×	√
Qi et al. [5]	Centralized	√	×	√	×	√
Ours	MB-BC-based	√	√	√	√	√

Table 3: Registration time.

Operations	Involved entities	Time (ms)
Leader department A registration	LD A/DA	46.7
Leader department B registration	LD B/DA	46.2
Leader department C registration	LD C/DA	46.7
General department A registration	Department A/DA/LD A	57.8
General department B registration	Department B/DA/LD B	59.1
General department C registration	Department C/DA/LD C	57.7

(3) *Nonrepudiation*: in response to problematic data, the corresponding department node of the PH cannot repudiate. The witness node verifies the signature of the node before receiving the "transaction." In addition, the structural characteristics of the blockchain ensure that the "transaction" cannot be tampered with after being on the chain. When the subsequent administration doubts about the production data, the pharmaceutical company cannot deny it

In addition, as a distributed system with a large number of network nodes, system robustness is also one of the indicators of system security. Let us analyze the robustness of the system with some attacks:

(a) *DAO attack*: the DAO attack takes advantage of the fact that a smart contract cannot be changed once it is released and is not controlled by any outside entity. Once a loophole in the smart contract is discovered, it will be attacked. Our schema model can effectively resist DAO attacks. In this scheme, it is assumed that the general nodes of PH are untrustworthy, and they may use the smart contract vulnerability to carry out DAO attacks. Faced with this situation, different from the general blockchain system, each operation of the blockchain node will be attached with its verification signature, to avoid the problem of anonymous operation without accountability. On the other hand, all smart contracts are released on the branch chain. Once loopholes appear, the most serious case will only cause the branch chain of PH to stop operating. After abnormal detection, the system will scrap the branch chain and regenerate a branch chain for pH on the main chain. The branched chain will be restored to the state before the smart contract was issued, avoiding the collapse of the whole blockchain system

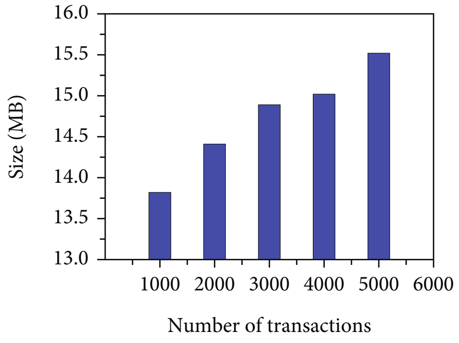


Figure 5: The size of the blockchain system.

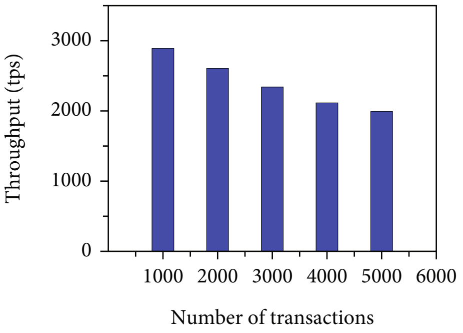
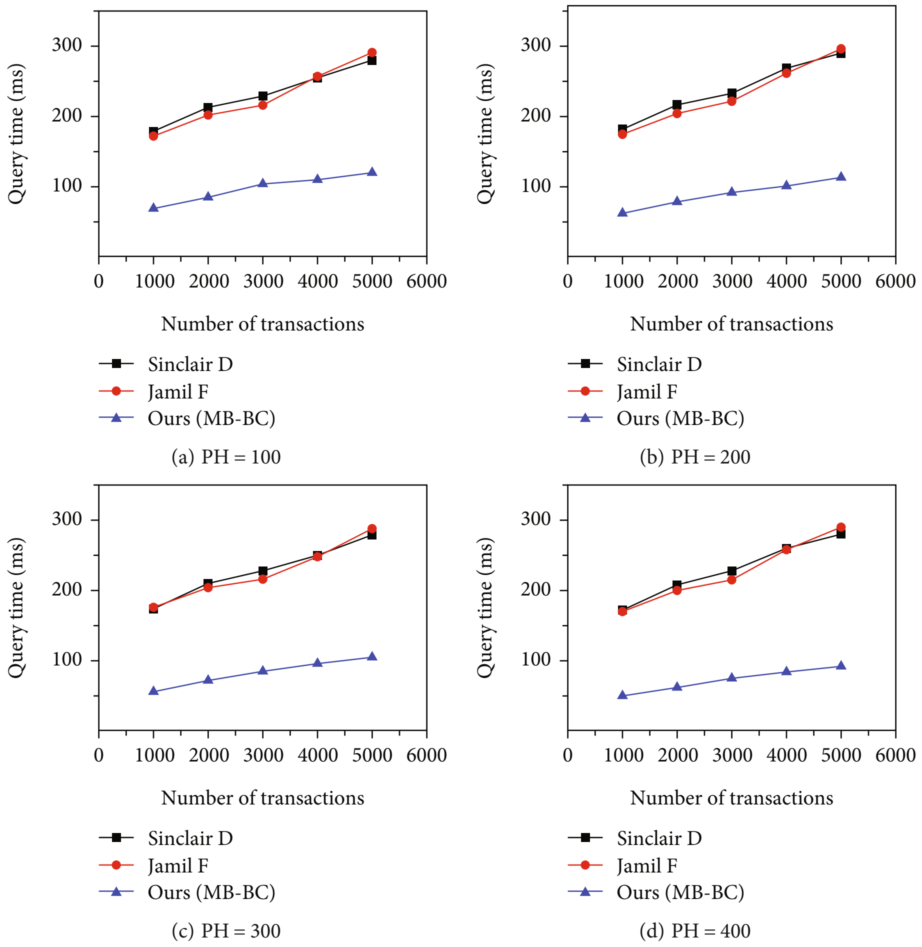


Figure 6: Throughput of the blockchain system.

(b) *Concentration of rights*: for both PoS and DPoS, since the witness node is elected, the rights and interests tend to be concentrated in the hands of a few people. In the common DPoS mechanism, the final witness nodes are always those few nodes, which



(a) PH = 100

(b) PH = 200

(c) PH = 300

(d) PH = 400

Figure 7: Query time of the drug data.

greatly affects the stability of the blockchain system. In this scheme, we have added a review mechanism into the consensus mechanism. In addition to voting, the hard work of the voted node and the source of votes will be counted into the voting proportion. This strategy enhances the fairness of consensus voting and can effectively prevent the problem of concentration of rights

7.2. Performance Evaluation. We simulate patient *P* and pharmaceutical companies PH with Java clients on a laptop with 2.40 GHz Intel(R) Core i5 processors and 8 GB memory. At the same time, we use Java language, choose Spring Boot 2.2.1 for the framework and Postman as the testing tool, and use sockets to implement p2p. The network simply builds a new blockchain structure with the main chain and branch chains. Furthermore, we wrote the smart contract in the proposal on the Ethereum platform using solidity language (a smart contract language). The smart contract was deployed on the blockchain through Truffle platform.

First, we verify the feasibility of the system. We have set up three pharmaceutical companies PH_A, PH_B, and PH_C in the blockchain network, and each pharmaceutical company has a leader node and a general node; the size of each "transaction" is about 1 kb. Table 3 shows the initial registration time of each node in the system. It can be seen from Table 3 that the registration time is very short. The registration time of the general node is slightly longer than that of the leader node. This is mainly because compared with the registration information verification of the leader node, the work was manually reviewed by the system and was not included in the total time. Table 3 shows that the registration time of each node is within the normal range, which is feasible.

The size of the blockchain system is also one of the important indicators of system feasibility. Therefore, we tested the size of the blockchain. After the registration is completed, one main chain and three branch chains will be generated according to the scheme; we test the size of the blockchain under general node *A*. From the test results in Figure 5, as the number of transactions increases, the change in block size is very small. This is because node *A* does not need to save the blocks of the remaining branch chains and it only needs to save the branch chain hash after the update is completed. Therefore, the block size saved by node *A* has no obvious changes. According to the data in Figure 5, taking a general drug shelf life of three years as an example, assuming that PH generates a transaction every three seconds and the assembly line works for 12 hours a day, we can calculate that the data stored on the blockchain will

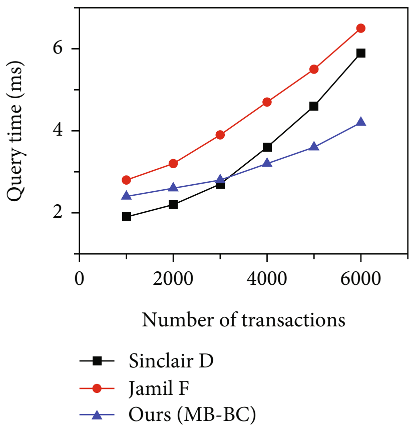


Figure 8: Consensus cost of the blockchain system.

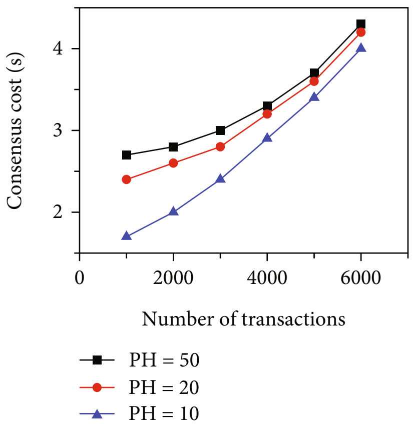


Figure 9: Consensus cost of the blockchain system.

not exceed 15 GB. For modern databases, it is completely acceptable. Therefore, from the perspective of block size, our scheme is completely feasible, too.

In addition, we also tested the throughput of the system in Figure 6. It can be seen from the figure that our system has enough throughput to handle a large number of transactions.

The query time of data in the blockchain is one of the important indicators of the efficiency of the traceability system. As a large number of pharmaceutical companies are involved, here, we simulated the data query efficiency and compared it with the existing solutions. Among them, Sinclair et al.'s [27] scheme is based on the ordinary blockchain traceability system, and Jamil et al.'s [28] scheme improves the blockchain on the basis of the traceability system. All transactions in the experiment belong to the PH randomly, and to prevent extreme situations from happening, the number of transactions of each PH will not exceed one-third of the total number of transactions in the system.

It can be seen from the result that compared with the other two schemes, with the number of transactions in the blockchain increases, the query time will become longer, and the backtracking time of our scheme is much shorter than that of the other two schemes. This is because, in our scheme, we can quickly locate the branch chain where the data is located for backtracking based on the identifier in the "transaction." In addition, from the four pictures in Figure 7 as a whole, with the increase in the number of pharmaceutical companies, the query time of our scheme is more stable than the general blockchain system and will hardly be affected. Therefore, this solution has certain advantages in query time efficiency.

Also, the main time cost for the blockchain system is in the consensus phase. We compared the consensus time consumption in this solution with the other two schemes. We carried the consensus algorithms in scheme [27] and scheme [28] into this system model and operated them independently, and the results obtained are shown in Figure 8.

It can be clearly seen from the figure that the efficiency advantage of this solution is more obvious when faced with a large number of transactions. For the scenario of a drug traceability platform that exists in a large number of pharmaceutical companies, the transaction volume in the system is huge, so it fits this scenario very well.

As shown in Figure 9, changes in the number of PH will also affect consensus cost. The reason can be that when there are too many PHs and the transaction volume is small, the block generation conditions are not met, which leads to a decrease in the efficiency of block generation. When the number of transactions increases, the consensus consumption will stabilize. When the number of PH increases, the system can still operate stably and has little impact on consensus consumption, which can meet system requirements perfectly.

8. Conclusion

In this paper, we proposed a multibranch blockchain (MC-BC) drug traceability and supervision system scheme. MC-BC separated the pharmaceutical companies through branch chains. The structure of the main chain and branch chains was not only conducive to departmental regulatory review but could also greatly reduce the traceability time of drug data. In addition, in this model, we made improvements to DPoS to meet the needs of the drug supply chain by adding review and punishment mechanisms. At the same time, we adopted the combination of CP-ABE technology and smart contracts to realize the privacy of drug data and provided fine-grained access control rights in real time. Meanwhile, experiments and performance evaluations were conducted to prove that our scheme is efficient and feasible.

For future work, we will further improve the trust mechanism and reward mechanism of the blockchain system and expand the existing system functions.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under grant 62072252, in part by the Natural Science Foundation of Shanxi Province (No. 2020JM-537), and in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grants SJCX21_0284 and KYCX21_0790.

References

[1] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K. K. R. Choo, "Security challenges and opportunities for smart contracts in internet of things: a survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12004–12020, 2021.

[2] H. Gao, H. Ji, H. Huang, F. Xiao, and J. Luo, "An immunity passport scheme based on the dual-blockchain architecture for international travel," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5721212, 11 pages, 2022.

[3] 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 of Things Journal*, vol. 4, no. 5, pp. 1634–1646, 2017.

[4] U.S. Food and Drug Administration, *Drug supply chain security act*, http://www.DA.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct.

[5] S. Qi, Y. Zheng, M. Li, Y. Liu, and J. Qiu, "Scalable industry data access control in RFID-enabled supply chain," *IEEE/ACM Transactions on Networking*, vol. 24, no. 6, pp. 3551–3564, 2016.

[6] D. Kapoor, "An overview on pharmaceutical supply chain: a next step towards good manufacturing practice," *Drug Designing & Intellectual Properties International Journal*, vol. 1, no. 2, 2018.

[7] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis et al., "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.

[8] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, and S. Wan, "Safeguarding cross-silo federated learning with local differential privacy," *Digital Communications and Networks*, 2021.

[9] S. Maheswari and U. Gudla, "Secure sharing of personal health records in Jelastic cloud by attribute based encryption," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1–4, Coimbatore, India, 2017.

[10] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3582–3592, 2022.

[11] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet of Things Journal*, vol. 5, no. 7, pp. 4101–4112, 2020.

[12] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: a blockchain-based solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2020.

[13] S. Figorilli, F. Antonucci, C. Costa et al., "A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain," *Sensors*, vol. 18, no. 9, p. 3133, 2018.

[14] Ethereum, https://www.ethereum.org.

[15] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," in *Blockchain Enabled Applications*, pp. 139–149, Apress, Berkeley, CA, USA, 2017.

[16] S. Peng, X. Hu, J. Zhang et al., "An efficient double-layer blockchain method for vaccine production supervision," *IEEE Transactions on Nanobioscience*, vol. 19, no. 3, pp. 579–587, 2020.

[17] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: a survey," *Wireless Networks*, vol. 26, no. 8, pp. 5579–5593, 2020.

[18] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a decentralized currency?," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 54–60, 2014.

[19] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," *Information*, vol. 8, no. 4, p. 137, 2017.

[20] S. Mao, L. Liu, N. Zhang et al., "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6647–6660, 2022.

[21] S. Mao, J. Wu, L. Liu, D. Lan, and A. Taherkordi, "Energy-efficient cooperative communication and computation for wireless powered mobile-edge computing," *IEEE Systems Journal*, vol. 16, no. 1, pp. 287–298, 2022.

[22] X. Tan, J. Zhang, Y. Zhang, Z. Qin, Y. Ding, and X. Wang, "A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network," *Tsinghua Science and Technology*, vol. 26, no. 1, pp. 36–47, 2021.

[23] S. Xu, X. Chen, and Y. He, "EVchain: an anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 845–856, 2021.

[24] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019.

[25] T. Feng, "An agri-food supply chain traceability system for China based on RFID blockchain technology," in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, Kunming, 2016.

[26] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, and P. Lund, "Blockchain: a solution for improved traceability with reduced counterfeits in supply chain of drugs," in *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, pp. 1–5, Ufa, Russia, 2020.

[27] D. Sinclair, H. Shahriar, and C. Zhang, "Security requirement prototyping with hyperledger composer for drug supply chain: a blockchain application," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 158–163, Kuala Lumpur, Malaysia, 2019.

[28] 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, 2019.

[29] B. Alangot and K. Achuthan, "Trace and track: enhanced pharma supply chain infrastructure to prevent fraud," in *International Conference on Ubiquitous Communications and Network Computing*, pp. 189–195, Cham, 2017.

[30] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, Munich, Germany, 2016.

[31] N. Alzahrani and N. Bulusu, "Block-supply chain: a new anticounterfeiting supply chain using NFC and blockchain,," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, New York, NY, USA, 2018.

[32] Y. Huang, J. Wu, and C. Long, "Drugledger: a practical blockchain system for drug traceability and regulation," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1137–1144, Halifax, NS, Canada, 2018.

[33] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 772–777, Lisbon, Portugal, 2017.

[34] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, USA, 2007.

[35] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[36] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[37] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security*, Portorož, Slovenia, 1999.

[38] I. Bentov, C.-T. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.

[39] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: a provably secure proof-of-stake blockchain protocol," *Advances in Cryptology–CRYPTO*, vol. 10401, pp. 357–388, 2017.

[40] S. Falkon, *The Story of the DAO—Its History and Consequences*, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.