IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 3, 2020, accepted October 28, 2020, date of publication November 9, 2020,
date of current version December 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036832

An IoT-Based Traceable Drug Anti-Counterfeiting Management System

CHIN-LING CHEN[1,2,3], YONG-YUAN DENG[3], (Member, IEEE), CHUN-TA LI[4], (Member, IEEE), SHUNZHI ZHU[1], YI-JUI CHIU[5,6], AND PEI-ZHI CHEN[1]

[1]School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
[2]School of Information Engineering, Changchun University of Science and Technology, Changchun 130600, China
[3]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City 41349, Taiwan
[4]Department of Information Management, Tainan University of Technology, Tainan City 71002, Taiwan
[5]School of Mechanical and Automotive Engineering, Xiamen University of Technology, Xiamen 361024, China
[6]State Key Laboratory for Strength and Vibration of Mechanical Structures, Xi'an 710049, China

Corresponding authors: Yong-Yuan Deng (allen.nubi@gmail.com), Chun-Ta Li (th0040@mail.tut.edu.tw), and Shunzhi Zhu (zhusz66@163.com)

This work was supported in part by the Ministry of Science and Technology, Taiwan, R.O.C, under Contract MOST 109-2221-E-324-021, in part by the National Natural Science Foundation of China under Grant 61672442, and in part by the Joint Funds of 5th Round of Health and Education Research Program of Fujian Province under Grant 2019-WJ-41.

ABSTRACT With the rapid development of the social economy, our lives are flooded with all kinds of counterfeit products. The public's attitude of greedy for petty and cheap has encouraged unscrupulous manufacturers to take advantage of the opportunity to provide low-cost counterfeit products, suppress the profits of legitimate manufacturers, and also make the public lose confidence in the quality of the products. At present, the most widely used anti-counterfeiting system based on QR codes on the market. However, existing traceability systems are still mostly built in a centralized manner, and the central agency provides trust guarantees, but the public still has great doubts about the credibility of the central agency. The introduction of blockchain technology can perfectly solve the lack of existing architecture and the environment. In this research, we propose an IoT-based traceable drug anti-counterfeiting management system, a comprehensive plan from drug research and development, certification, production to sales. The framework we propose meets the requirements of information security for data integrity, resistance to replay attacks, irreversible information, and non-repudiation.

INDEX TERMS Anti-counterfeiting, blockchain, data integrity, ECDSA, IoT, non-repudiation.

I. INTRODUCTION

As we known, from fake hairy crabs to fake cigarettes, fake wine, and fake medicines, counterfeit and inferior products have become a tumor in society. According to a survey published by the French Manufacturers Federation (unifab), counterfeit and counterfeit products have accounted for 5 percent of the total world trade, which are more than 110 billion U.S. dollars [1], and the economic losses caused by this are as high as tens of billions of U.S. dollars. Every year, the world's budget for anti-counterfeiting is also a huge number. With the rapid development of the national economy and the continuous improvement of people's living standards, counterfeit and inferior products have increased day by day, causing great damage to the market economy and affecting the quality of people's integrity. To solve this problem, anti-counterfeiting technology has received extensive attention.

At present, the most widely used anti-counterfeiting system based on QR codes on the market, but it appears that it has the following five defects: (1) unscrupulous merchants can directly steal QR codes of genuine products, then make thousands copies of the code; (2) illegal merchants can forge a similar serial number by analyzing the contents of each column of the serial number of the genuine product, thus they can forge or copy a database of the genuine product; (3) scan the QR code then can immediately jump to the corresponding web page (or the official homepage of the merchant, enter the relevant query information, they can get

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

the information of the product, etc.); (4) malicious merchant can modify the link to forge a malicious website similar to the authentic website, and pretending to be genuine merchants to deceive consumers; (5) merchants have the authority to change the database, thus merchants can manipulate the database by themselves, making online verification no longer credible [2]–[6].

In order to promote the healthy development of the market economy, effective anti-counterfeiting technology is urgently needed to prevent the current vandalism, and blockchain technology is the first choice. Blockchain technology is essentially a decentralized database maintained collectively. It has the characteristics of high reliability and high confidentiality and has a good prospect in effectively solving the trust problem between the two parties. Credit is the basis for the generation and maintenance of social relations between people and organizations. Currently, people mainly use regulations, systems, laws, contracts, etc. to restrict credit issues. Due to many subjective factors, these methods cannot solve the credit problem. The decentralization of the blockchain allows all users who join the blockchain to participate in the data authenticity verification, thus eliminating the shortcomings of a single authentication center in the traditional authentication system [7]–[10].

Blockchain mainly relies on two cryptographic methods: digital signatures and cryptographic hash functions. The immutability of the blockchain makes it form a decentralized database that cannot be tampered with or forged; its decentralized operation greatly improves transparency, security, and efficiency. It uses mathematical puzzles as the basis of trust and uses asymmetric encryption algorithms to ensure the security of transactions. As a decentralized database, the blockchain records all transactions of the blockchain from the creation block to the current block. Compared with the traditional database, the blockchain is decentralized, non-receivable, anonymous, and auditable [11]–[15].

The rest of this article is organized as follows. The second part is the descriptions of the related works. The third part is the introduction of the preliminary knowledge and threat model. The fourth part is the proposed IoT-based traceable drug anti-counterfeiting management system. The fifth part shows the analysis of security and characteristics. Finally, the fifth part is the conclusion of this research.

II. RELATED WORKS

Traceability and integrity are always discussed for complex supply chain issues. Food traceability has been one of the emerging blockchain applications in recent years for improving the areas of anti-counterfeiting and quality assurance. Blockchain technology has the potential to address these challenges through providing a tamper-proof audit trail of supply chain events and data associated with a product lifecycle, false data generated by the supply chain entities becomes immutable once recorded on the blockchain. On the other hand, the Internet of Things (IoT) technology is also involved to observe, track, and monitor products, activities, and processes via networks for supply chain applications. In recent years, [16]–[18] has been applied blockchain technology to the drug supply chain to prevent counterfeit drugs.

In order to solve the problem of counterfeit drugs, the pharmaceutical giant Merck applied for a patent in December 2016 to use blockchain to track goods flowing in the supply chain [19]. The patent outlines a method of using blockchain to store information about an item (in this case, a single product), and update the information when the product moves from the origin, and a distributed network can be used to store information to verify the authenticity of the product. In other words, the focus of the patent application is anti-counterfeiting. This technology ensures safe and reliable data integrity and avoids data damage or loss due to accidental or deliberate deletion.

Previous studies have been conducted by scholars [20]. The combination of the two characteristics of non-falsification of blockchain technology and traceability of transactions can completely eradicate the problems of counterfeit and inferior drugs in the process of drug research and development, production, and transportation in the supply chain. It has the following characteristics:

First, the production process is recorded in the chain. Record the operation of each production process from raw materials to drugs, use handheld devices to record production and inspection information, and at the same time transmit the encryption code generated after recording the information to the equipment in the next production link, to record all the information of the production link.

Second, the drug packaging process. In this link, a customized labeling device is used to generate a pair of identification codes, one part can be directly identified, and the other part is covered by a coating. The essence of the identity code is to generate paired keys in batches through an asymmetric encryption algorithm: the public key is used for drug circulation and recording drug information; the private key is covered with a coating and used for end consumers to scan the code after purchase.

Third, finished product inspection and anti-counterfeiting code assignment. In the finished product inspection process, the company writes the drug qualification certificate, anti-counterfeiting identification code, and other information into the drug identification code. After completing the finished product inspection, the employees use handheld devices or set up automatic assembly line equipment to encrypt the anti-counterfeiting information and packaging records with the company's private key to the blockchain and time stamps for storage, and cannot be forged or tampered with.

Fourth, records of inbound and outbound information. When the medicines are packaged in and out of the warehouse, use the conveyor belt mobile code scanning recorder to scan, and superimpose the inbound and outbound information on the identity code of the drug, and the identification code of a single drug corresponds to the information in the identity code of the whole box of drugs. And at the same time, the in-and-out information is transmitted to the

warehouse management system in real-time and stored on the blockchain.

Fifth, consumers verify authenticity. The end consumer scans and recognizes through the WeChat scan code or APP drug identification code. The decrypted information is called through the API to directly display part of the desensitization data of the drug and calculates based on the integrity and authenticity of the information to obtain the possibility that the drug is genuine. At the same time, this link can be connected to corporate marketing plans and data analysis systems.

Although some scholars have put forward some suggestions for drug anti-counterfeiting [15]–[18], [21], they still lack a comprehensive plan from drug research and development, certification, production to sales. Therefore, this article proposes a traceable drug anti-counterfeiting management system based on the Internet of Things. The drug manufacturer starts by contacting the raw material supplier to develop a new drug and then is approved by the drug administration until the drug distributor conducts terminal sales. The information of all the drug circulation process is protected by the blockchain on the chain to protect the data. The signature and seal approval cannot be tampered with privately by interested persons, so the legality of the data can be verified by a third party at any time to achieve the purpose of the anti-counterfeiting of drugs.

The rest of this article is organized as follows. The second part is the introduction of the preliminary knowledge and threat model. The third part is the proposed IoT-based traceable drug anti-counterfeiting management system. The fourth part shows the analysis of security and characteristics. Finally, the fifth part is the conclusion of this research.

III. PRELIMINARY KNOWLEDGE AND THREAT MODEL

A. ECDSA DIGITAL SIGNATURE

In the field of cryptography, the Elliptic Curve Cryptography Digital Signature Standard (ECDSA) [22] provides a variant of the standard digital signature algorithm (DSA). Like general elliptic curve cryptography, the bit size of the public key required by ECDSA is about twice the size of the security level. For example, to achieve a security level of 80 bits, the size of the ECDSA public key needs to be 160 bits, and the size of the DSA public key must be at least 1024 bits to achieve the same 80-bit security level.

The signature and verification process of ECDSA is as follows:

Suppose A wants to send a message to B. Initially, both parties must reach a consensus on the curve parameters (CURVE, G, n). In addition to the field equation of the curve, the base point G on the curve and the multiplication order n of the base point G is also required. In addition, A also needs a private key d_A and a public key Q_A, where $Q_A = d_A G$. If the message A wants to send is m, A needs to choose a random value k between [1, n-1], calculate $z = h(m)$, $(x_1, y_1) = kG$, $r = x_1 \bmod n$, $s = k^{-1}(z + rd_A) \bmod n$, and send the ECDSA signature pair (r, s) together with the original message m to B. After receiving the signature pair (r, s) and the original message m, B will verify the correctness of the ECDSA signature. B first calculates $z' = h(m)$, $u_1 = z's^{-1} \bmod n$, $u_2 = rs^{-1} \bmod n$, $(x_1', y_1') = u_1 G + u_2 Q_A$, $r \stackrel{?}{=} x_1' \bmod n$, and if it passes the verification, then B confirms that the ECDSA signature and message m sent by A are correct.

B. BLOCKCHAIN SMART CONTRACT

The smart contract was first proposed by the interdisciplinary legal scholar Nick Szabo [23] in 1995. Its definition is as follows: A smart contract is a set of commitments defined in digital form, including contract participants. Contract participants can execute the agreed agreement through smart contracts. Blockchain can achieve collaboration and trust between multiple business entities through smart contracts, thereby expanding the scope and depth of mutual cooperation between parties.

With the vigorous development of the pharmaceutical industry and global trade, the research and development, manufacturing, and distribution of medicines are no longer under the full control of a single or a small number of manufacturers. The production and sales of medicines are bound to be extremely closely related to the supply chain. Nowadays, the supply chain has applied blockchain technology extensively, achieving the characteristics of transparency and open tracking and verification. If the design and production of drugs are combined with blockchain technology, the drug manufacturer and the medicinal raw material supplier will agree on the supply of raw materials through smart contracts, and the drug manufacturer and the drug distribution distributor will also agree on the distribution and sale of drugs through smart contracts. The history of drug production and circulation can be traced completely, and a third party can verify the drug at any time to achieve the effect of drug anti-counterfeiting.

C. THREAT MODEL

1) UNABLE TO ENSURE DATA INTEGRITY ISSUES

For any message transmitted in an unencrypted network environment, malicious attacks can be carried out in a modified form. This results in that the information delivered to the receiver is not the original information delivered by the sender, and the integrity of the data transmission is damaged. For example, the attacker wants to cause the drug manufacturer to misunderstand the sales status of a certain drug, so the attacker intercepts the drug sales status transmitted by the drug distributor to the drug manufacturer, and fakes the legitimate drug distributor to try to transmit incorrectly messages to the drug manufacturer.

2) DRUG COUNTERFEITING AND DRUG SAFETY ISSUES

If a message transmitted on the Internet is not signed by a digital signature, the recipient will not be able to confirm whether the message has been forged, and the sender of the

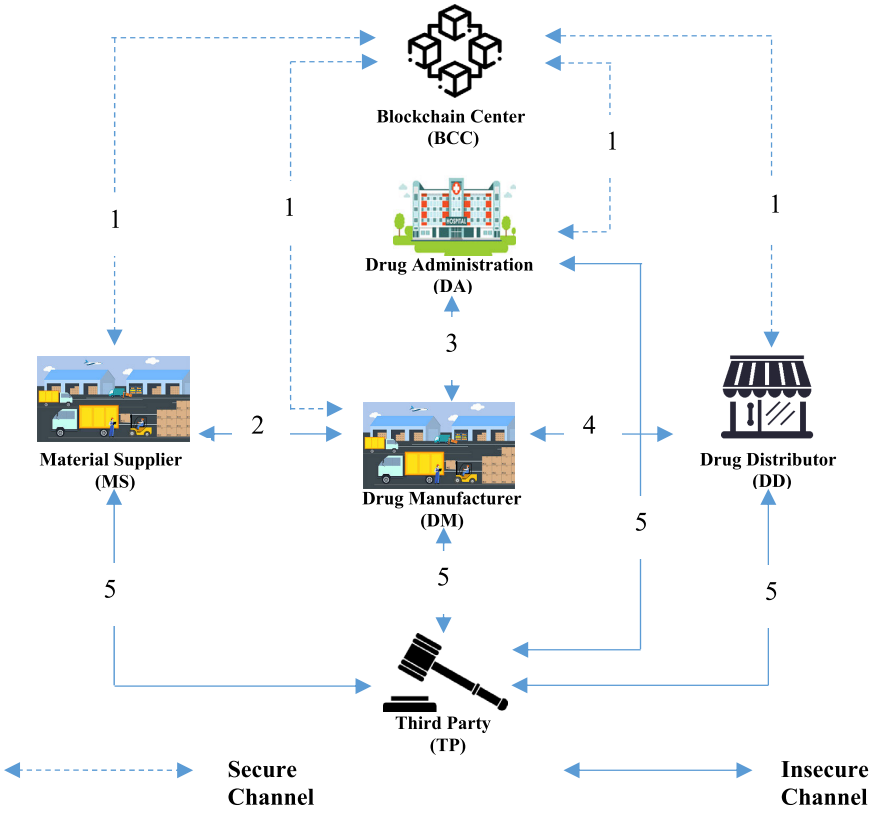

FIGURE 1. System architecture diagram.

message can deny that the message has been sent afterward. For example, if a certain drug is sold on the market, it does not have a marketing authorization approved by the drug administration, nor a production certificate approved by a drug manufacturer. When a patient has a negative risk due to taking the drug, the drug administration can deny that the drug has been approved for marketing, and the drug manufacturer can also deny that it has manufactured the drug.

3) DATA TRANSMISSION REPLAY ATTACK ISSUES

Even if the transmitted messages are signed and verified by digital signatures, the lack of protection by the time stamp mechanism during the transmission of the messages will have a serious impact on the overall drug design and production system. We can assume that the drug manufacturer sends an order request for raw materials to the raw material supplier, and the attacker intercepts the legal message sent by the drug manufacturer to the raw material supplier and repeatedly transmits this ordering demand to the raw material supplier. The content of the transmitted message has the legal digital signature of the drug manufacturer, but due to the lack of a timestamp mechanism, the raw material supplier will recognize that the drug manufacturer has sent multiple orders for raw materials, which will reduce the mutual trust between the drug manufacturer and the raw material supplier. It will also increase the operational risks and losses of drug manufacturers and raw material suppliers.

4) UNABLE TO PROVIDE TRACKING MANAGEMENT ISSUES

In the traditional supply chain circulation process, independent information management systems may be used between any two roles. Therefore, a large amount of manpower is required to integrate supply chain data, and even cannot provide overall supply chain data integration. If blockchain technology is not applied to the supply chain, it is impossible to provide an overall automated integration architecture. The system cannot automatically record drug design, production, and sales data, and cannot provide national drug identification code integration services. When issues related to drug quality and drug safety occur, third-party verifiers will not be able to verify the correctness and legitimacy of data at each stage based on the drug's production history and confirm the responsibility relationship between roles.

IV. OUR PROPOSED SCHEME

A. SYSTEM STRUCTURE

In this research, we propose to use the Elliptic Curve Cryptography Digital Signature Standard (ECDSA) to design an IoT-based traceable drug anti-counterfeiting management system. As shown in Figure 1 below, the application of blockchain technology to a complete drug production and

circulation history, which allows a third party to verify the complete production history of the drug at any time to achieve the anti-counterfeiting effect of the drug. The roles in the environment include Blockchain Center (BCC), Drug Administration (DA), Material Supplier (MS), Drug Manufacturer (DM), Drug Distributor (DD), and Third-Party (TP).

Step 1: This step is the registration stage of each role in the system. All drug administration, material suppliers, drug manufacturers, and drug distributors need to register with the blockchain center to obtain the public and private keys for ECDSA signature.

Step 2: When a drug manufacturer wants to market a new drug, it will enter the drug development and trial phase. The drug manufacturer will request the material supplier to provide production raw materials for the development of new drugs, and the material supplier will return a confirmation message of the content of the drug raw materials. The message contains the identification code of the drug raw materials.

Step 3: After the drug manufacturer completes the drug development and testing phase, it will enter the drug inspection and approval phase. The drug manufacturer will provide the drug-related trial data and drug information signed with a private key, and sent to the drug administration for the drug administration to conduct drug testing and analysis. If the drug administration approves the listing of the drug, the drug approval certificate issued by the drug administration will be returned.

Step 4: After the drug manufacturer obtains the drug marketing authorization, the drug will be mass-produced and the unique identification code of the drug will be marked. According to international standards, the first half of the unique identification code is the classification code approved by drug administration, and the second half is the drug production serial number defined by the drug manufacturer. The drug manufacturer will sign the drug information, drug unique identification code, and drug approval certificate with a private key and send it to the drug distributor. The drug distributor will send the medicines to medical institutions and pharmacies, and finally, deliver the medicines to the patients.

Step 5: All third-party verifiers, such as hospitals, pharmacies, patients, patient family members, inspection agencies, etc., can use the public keys of drug administration, material supplier, drug manufacturer, and drug distributor to verify the blockchain value and the drug approval certificate. After that, they can verify the complete production history and legality of the drug. The third-party can verify the expiration date of the drug by checking the signature information of the drug manufacturer and drug distributor. The third-party checks the signature information of the drug manufacturer and material supplier to confirm whether the raw material content is correct. The third-party checks the signature information of the drug manufacturer, drug administration, and the drug approval certificate to verify the marketing authorization of the drug.

B. NOTATION TABLE

The general table of notations in this study is defined as follows:

q	A k-bit prime number
$GF(q)$	Finite group q
E	The elliptic curve defined on finite group q
G	A generating point based on the elliptic curve E
ID_x	A name representing identity x
k_x	A random value on elliptic curve
(r_x, s_x)	Elliptic curve signature value of x
(x_x, y_x)	An ECDSA signature message of x
M_{x-y}	A message from x to y
ID_{BC}	The index value of blockchain message
BC_x	Blockchain message of x
TS_x	Timestamp message of x
ID_{MUI}	Identification code of pharmaceutical raw materials
ID_{UI}	The unique identification code of the drug
$Cert_D$	Drug approval certificate issued by the drug administration
h	Hash function
$A \stackrel{?}{=} B$	Verify whether A is equal to B

C. THE INITIAL PHASE

In the initial stage of the system, the blockchain center will generate some basic parameters and disclose these common parameters to the material supplier, the drug administration, the drug manufacturer, and the drug distributor.

Step 1: The blockchain center chooses a k bits prime number p, and generates elliptic curve related parameters $(F_p, E/F_p, G, P)$.

Step 2: The blockchain center discloses relevant public parameters $(F_p, E/F_p, G, P)$ to all drug administration, material suppliers, drug manufacturers, and drug distributors.

D. SMART CONTRACT INITIALIZATION

The research plan uses the blockchain technology based on the Internet of Things, starting with the drug manufacturer purchasing raw materials from the raw material supplier, and then the drug manufacturer sends the drug and related documents to the drug administration for review. If the drug is approved by the drug administration, the certificate will be issued to the drug manufacturer. The drug manufacturer will formally produce the drug, perform the unique identification code of the drug following national regulations, and finally send it to the drug distributor for sale. In the process of drug production and circulation, some key information will be stored and verified through blockchain technology and can be verified by a third-party verifier. The key information of these blockchains will be defined in the smart contract.

```
struct dmms smart contract
dmmsinf{
        string dmms_id;
        string dmms_detail;
}
struct msdm smart contract
msdminf{
        string msdm_id;
        string msdm_detail;
        string msdm_mui;
        string msdm_date;
}
struct dmda smart contract
dmdainf{
        string dmda_id;
        string dmda_detail;
}
struct dadm smart contract
dadminf{
        string dadm_id;
        string dadm_detail;
        string dadm_cert;
}
struct dmdd smart contract
dmddinf{
        string dmdd_id;
        string dmdd_detail;
        string dmdd_cert;
        string dmdd_ui;
        string dmdd_date;
        string dmdd_cost;
}
struct dddm smart contract
dddminf{
        string dddm_id;
        string dddm_detail;
}
string keypairs;
string count;
```

E. SYSTEM ROLE REGISTRATION PHASE

At this stage, the material supplier, the drug administration, the drug manufacturer, and the drug distributor register with the blockchain center and obtain the public and private keys for the ECDSA signature. The system role X can represent material suppliers, drug administration, drug manufacturers, and drug distributors. The registration process is shown in Figure 2.

Step 1: System role X generates a name ID_X, and sends it to the blockchain center.

Step 2: The blockchain center generates an ECDSA private key d_X based on the role X, calculates

$$Q_X = d_X G \tag{1}$$

If the identity of the registered role is verified, the smart contract xins will be triggered, the content of which is as follows:

```
function insert x smart
contract xins (
string x_id, string x_detail) {
        count ++;
        x[count].id = id;
        x[count].detail =
detail;
}
string x_keypairs;
```

Then the blockchain center will transmit ID_X, (d_X, Q_X) to role X.

Step 3: The role X will store the key (d_X, Q_X).

F. DRUG DEVELOPMENT AND TRIAL PHASE

When the drug manufacturer wants to conduct drug research and development, it will request the material supplier to provide drug raw materials for the drug manufacturer to conduct drug development and production. The raw material content and production date of the drug are both signed and confirmed by both drug manufacturers and material suppliers and recorded on the blockchain, which can be publicly checked and verified. The process of drug development and trial phase is shown in Figure 3.

Step 1: The drug manufacturer generates a random value k_{DM-MS}, calculates

$$z_{DM-MS} = h(ID_{DM}, M_{DM-MS}, TS_{DM-MS}, ID_{BC}) \tag{2}$$

$$(x_{DM-MS}, y_{DM-MS}) = k_{DM-MS} G \tag{3}$$

$$r_{DM-MS} = x_{DM-MS} \bmod n \tag{4}$$

$$s_{DM-MS} = k_{DM-MS}^{-1}(z_{DM-MS} + r_{DM-MS} d_{DM}) \bmod n \tag{5}$$

And sends ID_{DM}, M_{DM-MS}, TS_{DM-MS}, (r_{DM-MS}, s_{DM-MS}), ID_{BC} to the material supplier.

Step 2: The material supplier first uses

$$TS_{NOW} - TS_{DM-MS} \leq \Delta T \tag{6}$$

to confirm whether the time stamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{DM-MS} = h(ID_{DM}, M_{DM-MS}, TS_{DM-MS}, ID_{BC}) \tag{7}$$

$$u_{DM-MS1} = z'_{DM-MS} s_{DM-MS}^{-1} \bmod n \tag{8}$$

$$u_{DM-MS2} = r_{DM-MS} s_{DM-MS}^{-1} \bmod n \tag{9}$$

$$(x'_{DM-MS}, y'_{DM-MS}) = u_{DM-MS1} G + u_{DM-MS2} Q_{DM} \tag{10}$$

$$x'_{DM-MS} \stackrel{?}{=} r_{DM-MS} \bmod n \tag{11}$$

If the verification is passed, the drug manufacturer will get the relevant drug raw material request information and trigger the smart contracts dmmsins and dmmschk. The content is as follows:

```
function insert smart contract
dmmsins(
string dmms_id, string
dmms_detail) {
        count ++;
        dmms[count].id = id;
        dmms[count].detail =
detail;
}
sign string dm_key (dmms_id,
dmms_detail);
```

```
verify string dm_key
(dmms_id, dmms_detail);
function check smart contract
dmmschk(
string dmms_id, string
dmms_detail) {
        return dmms_id.exist;
        return
dmms_detail.exist;
}
```

The material supplier calculates

$$BC_{DM-MS} = h(r_{DM-MS}, s_{DM-MS}) \tag{12}$$

(ID_{BC}, BC_{DM-MS}) will also be uploaded to the blockchain center. Then the material supplier generates a random value k_{MS-DM} and calculates

$$z_{MS-DM} = h(ID_{MS}, M_{MS-DM}, TS_{MS-DM}, BC_{DM-MS}, ID_{MUI}, ID_{BC}) \tag{13}$$

$$(x_{MS-DM}, y_{MS-DM}) = k_{MS-DM} G \tag{14}$$

$$r_{MS-DM} = x_{MS-DM} \bmod n \tag{15}$$

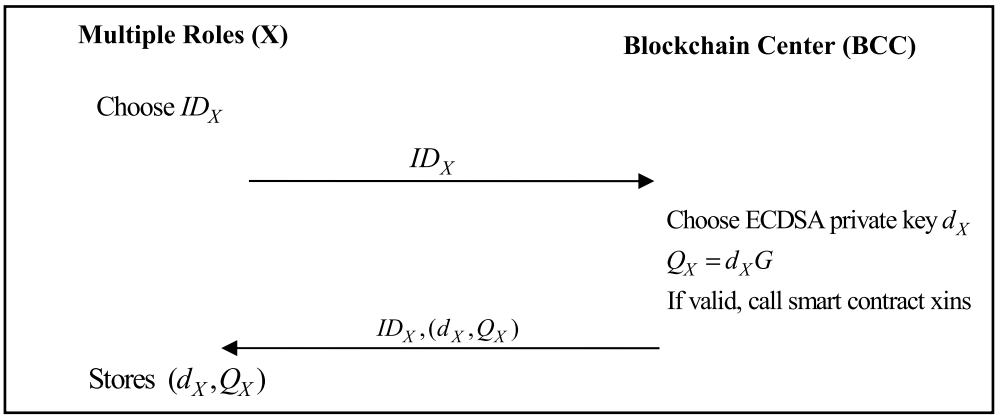

FIGURE 2. Each role of the system registers with the blockchain center.

$$s_{MS-DM} = k_{MS-DM}^{-1}(z_{MS-DM} + r_{MS-DM} d_{MS}) \bmod n \quad (16)$$

And sends ID_{MS}, M_{MS-DM}, TS_{MS-DM}, (r_{MS-DM}, s_{MS-DM}), BC_{DM-MS}, ID_{MUI}, ID_{BC} to the drug manufacturer.

Step 3: The drug manufacturer first uses

$$TS_{NOW} - TS_{MS-DM} \leq \Delta T \quad (17)$$

to confirm whether the timestamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{MS-DM} = h(ID_{MS}, M_{MS-DM}, TS_{MS-DM}, BC_{DM-MS}, ID_{MUI}, ID_{BC}) \quad (18)$$

$$u_{MS-DM1} = z'_{MS-DM} s_{MS-DM}^{-1} \bmod n \quad (19)$$

$$u_{MS-DM2} = r_{MS-DM} s_{MS-DM}^{-1} \bmod n \quad (20)$$

$$(x'_{MS-DM}, y'_{MS-DM}) = u_{MS-DM1} G + u_{MS-DM2} Q_{MS} \quad (21)$$

$$x'_{MS-DM} \stackrel{?}{=} r_{MS-DM} \bmod n \quad (22)$$

If the verification is passed, the content and production date of the relevant drug materials provided by the material supplier will be obtained, and the smart contracts msdmins and msdmchk will be sent. The content is as follows:

```
function insert smart contract
msdmins(
string msdm_id, string
msdm_detail,
string msdm_mui, string
msdm_date) {
   count ++;
   msdm[count].id = id;
   msdm[count].detail = detail;
   msdm[count].mui = mui;
   msdm[count].date = date;
}
sign string ms_key (msdm_id,
msdm_detail,
msdm_mui, msdm_date);
```

```
verify string ms_key
(msdm_id, msdm_detail,
msdm_mui, msdm_date);
function check smart contract
msdmchk(
string msdm_id, string
msdm_detail,
string msdm_mui, string
msdm_date) {
   return msdm_id.exist;
   return msdm_detail.exist;
   return msdm_mui.exist;
   return msdm_date.exist;
}
```

The drug manufacturer calculates

$$BC_{MS-DM} = h(r_{MS-DM}, s_{MS-DM}) \quad (23)$$

(ID_{BC}, BC_{MS-DM}) will also be uploaded to the blockchain center.

G. DRUG TESTING AND APPROVAL PHASE

When the drug manufacturer completes the drug development and trial phase, it will provide the drug-related test data to the drug administration for the drug administration to conduct drug testing and analysis. The medicinal properties and approval certificate of the drug are both signed and confirmed by both drug manufacturer and drug administration. The process of drug testing and approval phase is shown in Figure 4.

Step 1: The drug manufacturer generates a random value k_{DM-DA}, calculates

$$z_{DM-DA} = h(ID_{DM}, M_{DM-DA}, TS_{DM-DA}, BC_{MS-DM}, ID_{BC}) \quad (24)$$

$$(x_{DM-DA}, y_{DM-DA}) = k_{DM-DA} G \quad (25)$$

$$r_{DM-DA} = x_{DM-DA} \bmod n \quad (26)$$

$$s_{DM-DA} = k_{DM-DA}^{-1}(z_{DM-DA} + r_{DM-DA} d_{DM}) \bmod n \quad (27)$$

And sends ID_{DM}, M_{DM-DA}, TS_{DM-DA}, (r_{DM-DA}, s_{DM-DA}), BC_{MS-DM}, ID_{BC} to the drug administration.

Step 2: The drug administration first uses

$$TS_{NOW} - TS_{DM-DA} \leq \Delta T \quad (28)$$

to confirm whether the timestamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{DM-DA} = h(ID_{DM}, M_{DM-DA}, TS_{DM-DA}, BC_{MS-DM}, ID_{BC}) \quad (29)$$

$$u_{DM-DA1} = z'_{DM-DA} s_{DM-DA}^{-1} \bmod n \quad (30)$$

$$u_{DM-DA2} = r_{DM-DA} s_{DM-DA}^{-1} \bmod n \quad (31)$$

$$(x'_{DM-DA}, y'_{DM-DA}) = u_{DM-DA1} G + u_{DM-DA2} Q_{DM} \quad (32)$$

$$x'_{DM-DA} \stackrel{?}{=} r_{DM-DA} \bmod n \quad (33)$$

If the verification is passed, the relevant drug test data provided by the drug manufacturer will be obtained, and the

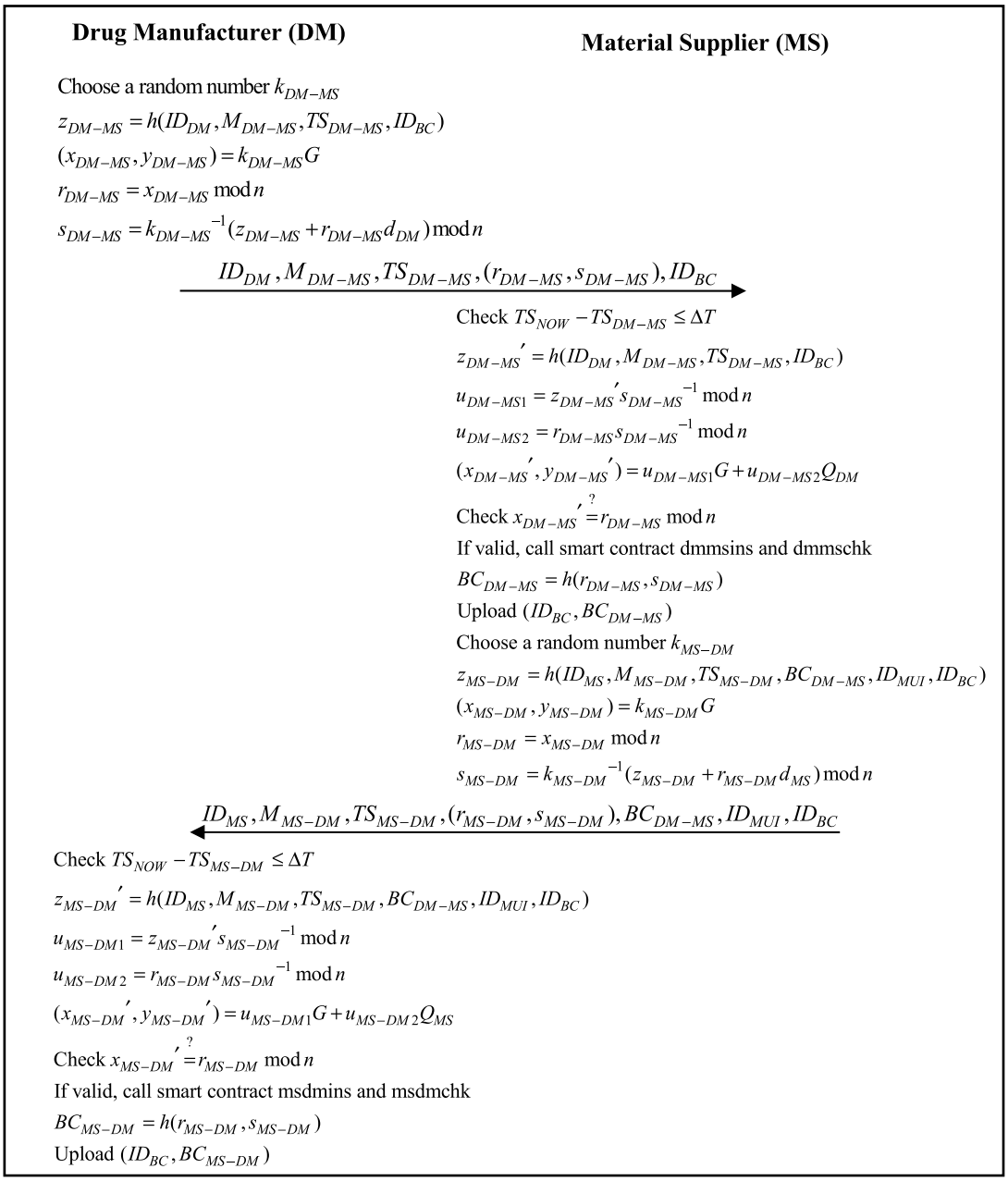

FIGURE 3. Drug development and trial phase.

smart contracts dmdains and dmdachk will be triggered. The content is as follows:

```
function insert smart contract
dmdains(
string dmda_id, string
dmda_detail) {
        count ++;
        dmda[count].id = id;
        dmda[count].detail =
detail;
}
sign string dm_key (dmda_id,
dmda_detail);
```

```
verify string dm_key
(dmda_id, dmda_detail);
function check smart contract
dmdachk(
string dmda_id, string
dmda_detail) {
        return dmda_id.exist;
        return
dmda_detail.exist;
}
```

The drug administration calculates

$$BC_{DM-DA} = h(r_{DM-DA}, s_{DM-DA}) \tag{34}$$

(ID_{BC}, BC_{DM-DA}) will also be uploaded to the blockchain center. Then the drug administration generates a random value k_{DA-DM}, calculates

$$z_{DA-DM} = h(ID_{DA}, M_{DA-DM}, TS_{DA-DM}, BC_{DM-DA}, Cert_D, ID_{BC}) \tag{35}$$

$$(x_{DA-DM}, y_{DA-DM}) = k_{DA-DM}G \tag{36}$$

$$r_{DA-DM} = x_{DA-DM} \bmod n \tag{37}$$

$$s_{DA-DM} = k_{DA-DM}^{-1}(z_{DA-DM} + r_{DA-DM}d_{DA}) \bmod n \tag{38}$$

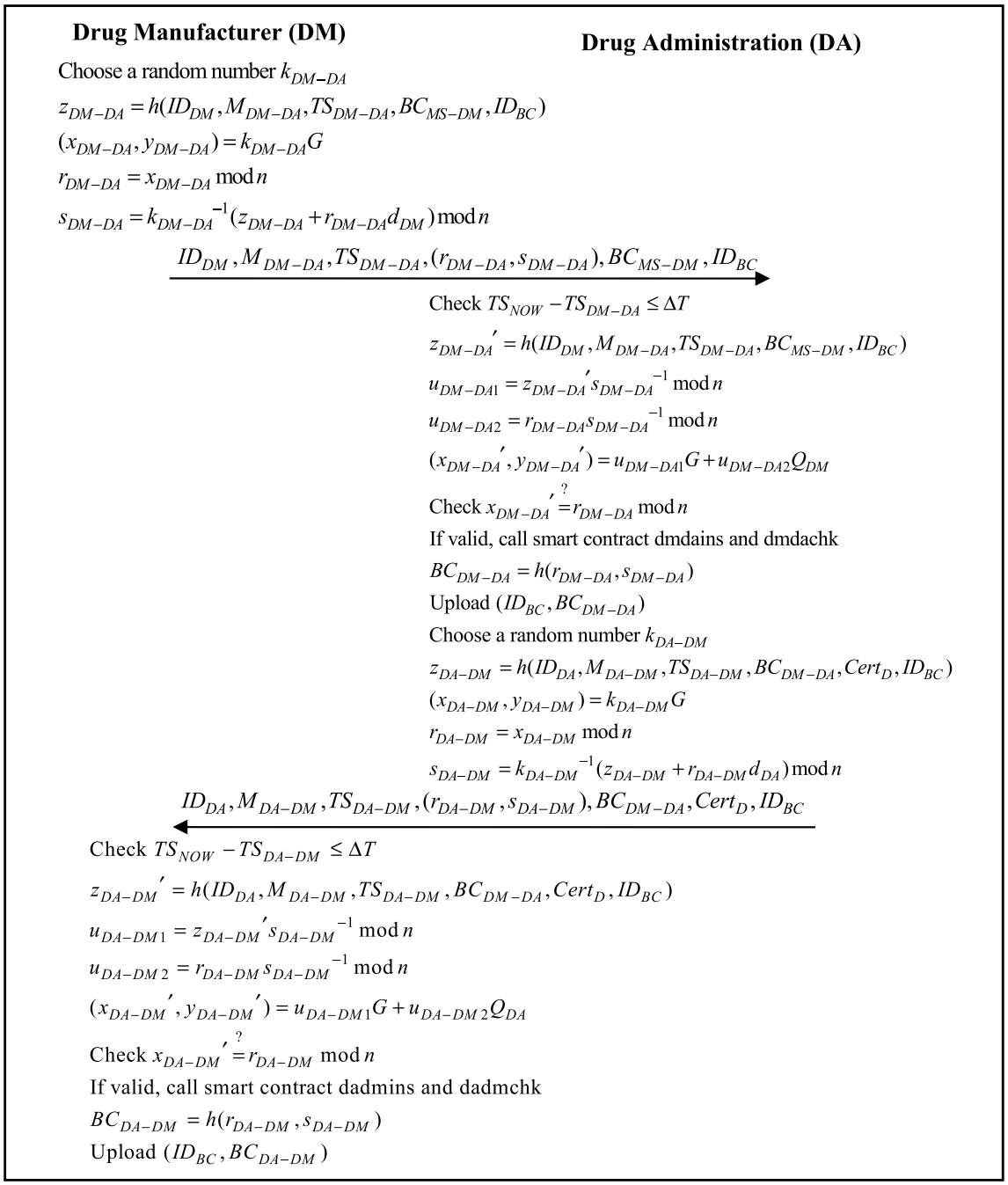

FIGURE 4. Drug testing and approval phase.

And sends ID_{DA}, M_{DA-DM}, TS_{DA-DM}, (r_{DA-DM}, s_{DA-DM}), BC_{DM-DA}, $Cert_D$, ID_{BC} to the drug manufacturer.

Step 3: The drug manufacturer first uses

$$TS_{NOW} - TS_{DA-DM} \le \Delta T \tag{39}$$

to confirm whether the timestamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{DA-DM} = h(ID_{DA}, M_{DA-DM}, TS_{DA-DM}, BC_{DM-DA}, Cert_D, ID_{BC}) \tag{40}$$

$$u_{DA-DM1} = z'_{DA-DM} s_{DA-DM}^{-1} \bmod n \tag{41}$$

$$u_{DA-DM2} = r_{DA-DM} s_{DA-DM}^{-1} \bmod n \tag{42}$$

$$(x'_{DA-DM}, y'_{DA-DM}) = u_{DA-DM1}G + u_{DA-DM2}Q_{DA} \tag{43}$$

$$x'_{DA-DM} \stackrel{?}{=} r_{DA-DM} \bmod n \tag{44}$$

If the verification is passed, the relevant drug approval information provided by the drug administration will be obtained, and the smart contracts dadmins and dadmchk will be triggered. The content is as follows:

```
function insert smart contract
dadmins(
string dadm_id, string
dadm_detail,
string dadm_cert) {
        count ++;
        dadm[count].id = id;
        dadm[count].detail =
detail;
        dadm[count].cert =
cert;
}
sign string da_key (dadm_id,
dadm_detail, dadm_cert);
```

```
verify string da_key (dadm_id,
dadm_detail,
dadm_cert);
function check smart contract
dadmchk(
string dadm_id, string
dadm_detail,
string dadm_cert) {
        return dmda_id.exist;
        return
dmda_detail.exist;
        return dmda_cert.exist;
}
```

The drug manufacturer calculates

$$BC_{DA-DM} = h(r_{DA-DM}, s_{DA-DM}) \tag{45}$$

(ID_{BC}, BC_{DA-DM}) will also be uploaded to the blockchain center.

H. DRUG PRODUCTION AND DISTRIBUTION PHASE

After the drug is approved by the drug administration, the drug manufacturer will provide the drug to the drug distributor for sale. The sales method and expiration date of the drug are both signed and confirmed by both drug manufacturers and drug distributor and are recorded on the blockchain, which can be publicly checked and verified. The process of drug production and distribution phase is shown in Figure 5.

Step 1: The drug manufacturer generates a random value k_{DM-DD}, calculates

$$z_{DM-DD} = h(ID_{DM}, M_{DM-DD}, TS_{DM-DD}, BC_{DA-DM}, Cert_D, ID_{UI}, ID_{BC}) \tag{46}$$

$$(x_{DM-DD}, y_{DM-DD}) = k_{DM-DD}G \tag{47}$$

$$r_{DM-DD} = x_{DM-DD} \bmod n \tag{48}$$

$$s_{DM-DD} = k_{DM-DD}^{-1}(z_{DM-DD} + r_{DM-DD}d_{DM}) \bmod n \tag{49}$$

And sends $ID_{DM}, M_{DM-DD}, TS_{DM-DD}, (r_{DM-DD}, s_{DM-DD})$, $BC_{DA-DM}, Cert_D, ID_{UI}, ID_{BC}$ to the drug distributor.

Step 2: The drug distributor first uses

$$TS_{NOW} - TS_{DM-DD} \leq \Delta T \tag{50}$$

to confirm whether the time stamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{DM-DD} = h(ID_{DM}, M_{DM-DD}, TS_{DM-DD}, BC_{DA-DM}, Cert_D, ID_{UI}, ID_{BC}) \tag{51}$$

$$u_{DM-DD1} = z'_{DM-DD}s_{DM-DD}^{-1} \bmod n \tag{52}$$

$$u_{DM-DD2} = r_{DM-DD}s_{DM-DD}^{-1} \bmod n \tag{53}$$

$$(x'_{DM-DD}, y'_{DM-DD}) = u_{DM-DD1}G + u_{DM-DD2}Q_{DM} \tag{54}$$

$$x'_{DM-DD} \stackrel{?}{=} r_{DM-DD} \bmod n \tag{55}$$

If the verification is passed, the relevant drug distribution information provided by the drug manufacturer will be obtained, and the smart contracts dmddins and dmddchk will be obtained, and the smart contracts dmddins and dmddchk will be triggered. The content is as follows:

```
function insert smart contract
dmddins(
string dmdd_id, string
dmdd_detail,
string dmdd_cert, string
dmdd_ui,
string dmdd_date, string
dmdd_cost) {
   count ++;
   dmdd[count].id = id;
   dmdd[count].detail = detail;
   dmdd[count].cert = cert;
   dmdd[count].ui = ui;
   dmdd[count].date = date;
   dmdd[count].cost = cost;
}
sign string dm_key (dmda_id,
dmda_detail,
dmdd_cert, dmdd_ui,
dmdd_date, dmdd_cost);
```

```
verify string dm_key
(dmda_id, dmda_detail,
dmdd_cert, dmdd_ui,
dmdd_date, dmdd_cost);
function check smart contract
dmddchk(
string dmdd_id, string
dmdd_detail,
string dmdd_cert, string
dmdd_ui,
string dmdd_date, string
dmdd_cost) {
   return dmdd_id.exist;
   return dmdd_detail.exist;
   return dmdd_cert.exist;
   return dmdd_ui.exist;
   return dmdd_date.exist;
   return dmdd_cost.exist;
}
```

The drug distributor calculates

$$BC_{DM-DD} = h(r_{DM-DD}, s_{DM-DD}) \tag{56}$$

(ID_{BC}, BC_{DM-DD}) will also be uploaded to the blockchain center. Then the drug distributor generates a random value k_{DD-DM}, calculates

$$z_{DD-DM} = h(ID_{DD}, M_{DD-DM}, TS_{DD-DM}, BC_{DM-DD}, ID_{BC}) \tag{57}$$

$$(x_{DD-DM}, y_{DD-DM}) = k_{DD-DM}G \tag{58}$$

$$r_{DD-DM} = x_{DD-DM} \bmod n \tag{59}$$

$$s_{DD-DM} = k_{DD-DM}^{-1}(z_{DD-DM} + r_{DD-DM}d_{DD}) \bmod n \tag{60}$$

And sends $ID_{DD}, M_{DD-DM}, TS_{DD-DM}, (r_{DD-DM}, s_{DD-DM})$, BC_{DM-DD}, ID_{BC} to the drug manufacturer.

Step 3: The drug manufacturer first uses

$$TS_{NOW} - TS_{DD-DM} \leq \Delta T \tag{61}$$

to confirm whether the timestamp is valid, and then verify the correctness of the ECDSA signature, calculates

$$z'_{DD-DM} = h(ID_{DD}, M_{DD-DM}, TS_{DD-DM}, BC_{DM-DD}, ID_{BC}) \tag{62}$$

$$u_{DD-DM1} = z'_{DD-DM}s_{DD-DM}^{-1} \bmod n \tag{63}$$

$$u_{DD-DM2} = r_{DD-DM}s_{DD-DM}^{-1} \bmod n \tag{64}$$

$$(x'_{DD-DM}, y'_{DD-DM}) = u_{DD-DM1}G + u_{DD-DM2}Q_{DD} \tag{65}$$

$$x'_{DD-DM} \stackrel{?}{=} r_{DD-DM} \bmod n \tag{66}$$

If the verification is passed, the relevant drug sales status provided by drug distributor will be obtained, and the

smart contracts dddmins and dddmchk will be triggered. The content is as follows:

```
function insert smart contract
dddmins(
string dddm_id, string
dddm_detail) {
        count ++;
        dddm[count].id = id;
        dddm[count].detail =
detail;
}
sign string dd_key (dddm_id,
dddm_detail);
```

```
verify string dd_key (dddm_id,
dddm_detail);
function check smart contract
dddmchk(
string dddm_id, string
dddm_detail) {
        return dddm_id.exist;
        return
dddm_detail.exist;
}
```

The drug manufacturer calculates

$$BC_{DD-DM} = h(r_{DD-DM}, s_{DD-DM}) \tag{67}$$

(ID_{BC}, BC_{DD-DM}) will also be uploaded to the blockchain center.

I. THIRD-PARTY VERIFIER VERIFICATION PHASE

When the third-party verifier (such as hospitals, pharmacies, patients, patients' family members, inspection agencies, etc.) has doubts about the production history of the drug, they can verify the certificate of the drug at any time, as well as the signature message of material supplier, drug manufacturer, and drug distributor. The third-party verifier calculates and compares blockchain data through the signature message to confirm the legality of the drug. The third-party verifier verification phase is shown in Figure 6.

Step 1: Third-party verifiers such as hospitals, pharmacies, patients, patient's family members, inspection agencies, etc. can download the certificate, signature, and blockchain data of the drug through, ID_{BC}, and then the third-party verifier verifies

$$BC_{DD-DM} \stackrel{?}{=} h(r_{DD-DM}, s_{DD-DM}) \tag{68}$$

and

$$BC_{DM-DD} \stackrel{?}{=} h(r_{DM-DD}, s_{DM-DD}) \tag{69}$$

If the verification fails, the expiry date of the drug is tampered with by the drug distributor.

Step 2: If the signature between the drug manufacturer and the drug distributor, and the blockchain data are verified, the third-party verifier will verify

$$BC_{DA-DM} \stackrel{?}{=} h(r_{DA-DM}, s_{DA-DM}) \tag{70}$$

and

$$BC_{DM-DA} \stackrel{?}{=} h(r_{DM-DA}, s_{DM-DA}) \tag{71}$$

And verify the drug certificate $Cert_D$ through the public key of the drug administration. If the verification fails, the certificate is forged by the drug manufacturer and the drug is not approved by the drug administration.

Step 3: If the drug certificate $Cert_D$, the signature between the drug manufacturer and the drug administration, and the blockchain data are verified, the third-party verifier will verify

$$BC_{MS-DM} \stackrel{?}{=} h(r_{MS-DM}, s_{MS-DM}) \tag{72}$$

and

$$BC_{DM-MS} \stackrel{?}{=} h(r_{DM-MS}, s_{DM-MS}) \tag{73}$$

If the verification fails, the material content of the drug is tampered with by the material supplier.

Step 4: If the signature between the drug manufacturer and the material supplier, and the blockchain data are verified, the blockchain data has been fully verified, and the third-party verifier can confirm that the drug is legal.

V. SECURITY AND FEATURE ANALYSIS

A. DATA INTEGRITY

In this research, we use the Elliptic Curve Cryptography Digital Signature Standard (ECDSA) to sign the transmitted message to ensure data integrity. Let's take the drug manufacturer and the material supplier as an example. When the drug manufacturer wants to transmit a message to the material supplier, the drug manufacturer will generate an ECDSA signature value (r_{DM-MS}, s_{DM-MS}). The attacker cannot know the private key of the drug manufacturer. Even if the transmission content is altered, the correct ECDSA signature values (r_{MS-DM}, s_{MS-DM}), (r_{DM-DA}, s_{DM-DA}), (r_{DA-DM}, s_{DA-DM}), (r_{DM-DD}, s_{DM-DD}) and (r_{DD-DM}, s_{DD-DM}). From the above description, we can see that this study uses ECDSA signature technology to ensure the integrity of data transmission between characters.

1) SCENARIO

The attacker intercepts the drug sales status sent by the drug distributor to the drug manufacturer, and fakes a legitimate drug distributor to try to send an incorrect message to the drug manufacturer.

2) ANALYSIS

The attacker will be unable to succeed because even if the attacker modifies the content of the message M_{DD-DM} sent by the drug distributor to the drug manufacturer, the attacker cannot sign the ECDSA with the private key of the drug distributor. After receiving the message, the drug manufacturer will immediately check the integrity of the transmitted data. The drug manufacturer will find that the message content M_{DD-DM} does not match the signature value (r_{DD-DM}, s_{DD-DM}), and the attacker's attack fails.

B. ANTI-COUNTERFEIT DRUGS

Whether it is a legal drug manufacturer or an illegal person, it is possible to produce fake drugs that have not been approved by the drug administration, which affects the lives and health of the people. This plan uses a certificate mechanism to avoid this situation. When hospitals, pharmacies, patients, patients' family members, inspection agencies, etc.

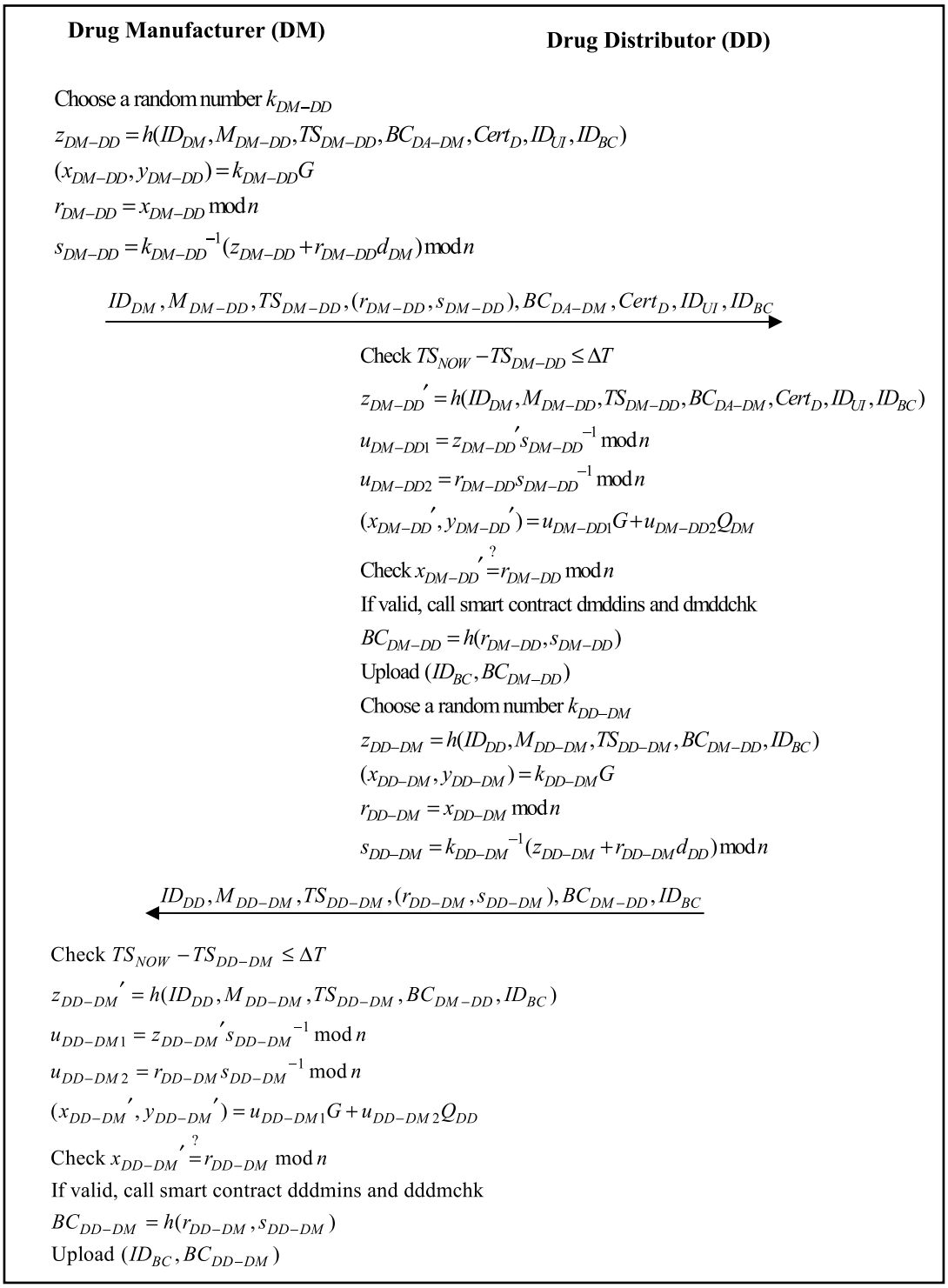

FIGURE 5. Drug production and distribution phase.

have doubts about the drug, they can verify the certificate $Cert_D$ of the drug at any time to confirm the legality of the drug. The certificate $Cert_D$ is signed by the drug administration with its private key. Whether it is a legal drug manufacturer or an illegal person, it is not possible to sign the ECDSA with the drug administration's private key. When the verifier examines that the certificate $Cert_D$ of the drug does not match the actual drug information, it can be known that the drug has been counterfeited.

C. RESIST REPLAY ATTACKS

Even if the attacker cannot pretend to be a legitimate role to attack, he/she may still intercept the content of the legitimate message first, and then retransmit the message to achieve

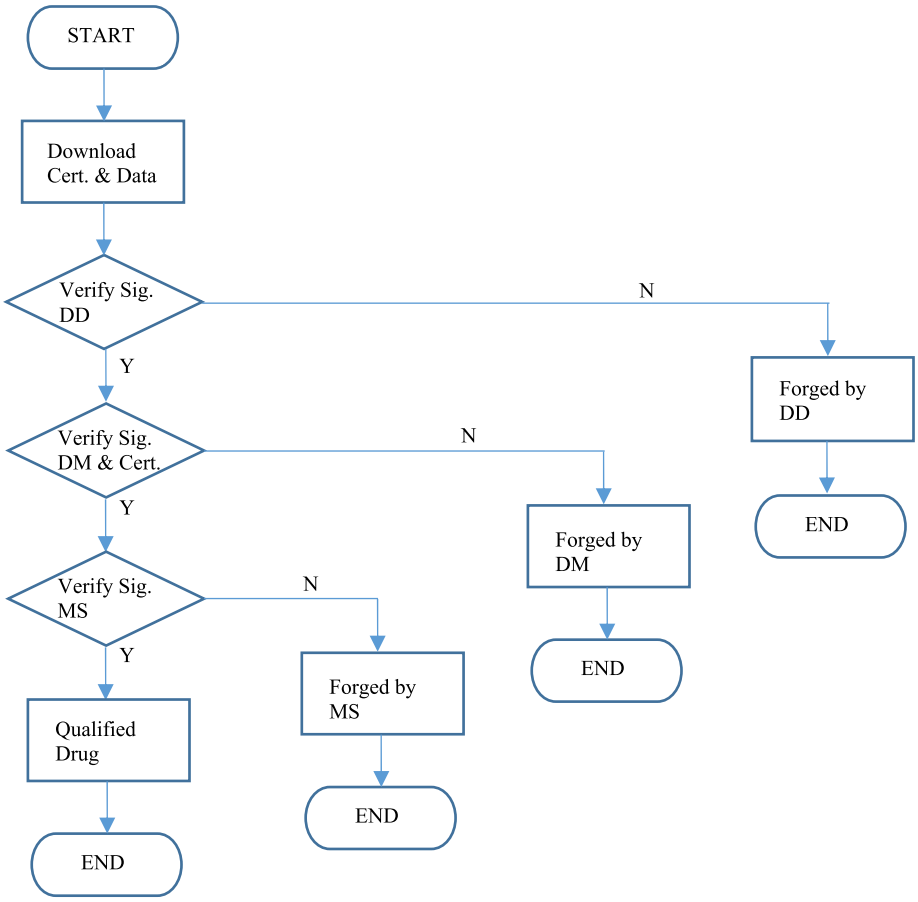

FIGURE 6. The third-party verifier verification phase.

its interference purpose. In our proposed scheme, a timestamp mechanism is added to the communication between any two characters. With time stamp messages TS_{DM-MS}, TS_{MS-DM}, TS_{DM-DA}, TS_{DA-DM}, TS_{DM-DD}, and TS_{DD-DM}, the attacker's replay attack can be resisted. For example, the attacker tried to disrupt the order information of the pharmaceutical raw materials of the drug manufacturer and the material supplier, intercepting the legal transmission content of the drug manufacturer to the material supplier, and then resending the message to the material supplier. The material supplier will check the time stamp message TS_{DM-MS} to confirm whether the timestamp is valid $TS_{NOW} - TS_{DM-MS} \leq \Delta T$. Even if the attacker changes the time stamp data since the drug manufacturer has added the time stamp TS_{DM-MS} to the signature, the material supplier checks the timestamp TS_{DM-MS} does not match the signature value (r_{DM-MS}, s_{DM-MS}), the attacker's replay attack will fail.

D. MESSAGE IS IRREVERSIBLE

In our proposed method, the key message content transmitted between each role is first subjected to hash function calculation, and then the ECDSA signature is performed to achieve the irreversible characteristics of the message. Message after hash function operation:

$$
\begin{aligned}
z_{DM-MS} &= h(ID_{DM}, M_{DM-MS}, TS_{DM-MS}, ID_{BC}) \\
z_{MS-DM} &= h(ID_{MS}, M_{MS-DM}, TS_{MS-DM}, BC_{DM-MS}, \\
&\quad ID_{MUI}, ID_{BC}) \\
z_{DM-DA} &= h(ID_{DM}, M_{DM-DA}, TS_{DM-DA}, \\
&\quad BC_{MS-DM}, ID_{BC}) \\
z_{DA-DM} &= h(ID_{DA}, M_{DA-DM}, TS_{DA-DM}, \\
&\quad BC_{DM-DA}, Cert_D, ID_{BC}) \\
z_{DM-DD} &= h(ID_{DM}, M_{DM-DD}, TS_{DM-DD}, \\
&\quad BC_{DA-DM}, Cert_D, ID_{UI}, ID_{BC}) \\
z_{DD-DM} &= h(ID_{DD}, M_{DD-DM}, TS_{DD-DM}, \\
&\quad BC_{DM-DD}, ID_{BC})
\end{aligned}
$$

The attacker cannot reverse the original message content, so the proposed protocol achieves the irreversible characteristics of the message.

E. NON-REPUDIATION

The content of the message sent by each role is signed by the role of its ECDSA private key. After the receiver receives the message, it will verify the message with the sender's public

TABLE 1. Non-repudiation of the proposed scheme.

Item / Phase	Signature value	Sender	Receiver	Signature verification
Drug development and trial phase	(r_{DM-MS}, s_{DM-MS})	DM	MS	$x_{DM-MS}{}' \stackrel{?}{=} r_{DM-MS} \bmod n$
	(r_{MS-DM}, s_{MS-DM})	MS	DM	$x_{MS-DM}{}' \stackrel{?}{=} r_{MS-DM} \bmod n$
Drug testing and approval phase	(r_{DM-DA}, s_{DM-DA})	DM	DA	$x_{DM-DA}{}' \stackrel{?}{=} r_{DM-DA} \bmod n$
	(r_{DA-DM}, s_{DA-DM})	DA	DM	$x_{DA-DM}{}' \stackrel{?}{=} r_{DA-DM} \bmod n$
Drug production and distribution phase	(r_{DM-DD}, s_{DM-DD})	DM	DD	$x_{DM-DD}{}' \stackrel{?}{=} r_{DM-DD} \bmod n$
	(r_{DD-DM}, s_{DD-DM})	DD	DM	$x_{DD-DM}{}' \stackrel{?}{=} r_{DD-DM} \bmod n$

key. If the message is successfully verified, the sender will not deny the content of the message is transmitted. Table 1 is an undeniable description of each role in this program.

F. PUBLICLY VERIFIABLE

This research uses blockchain technology, combined with ECDSA digital signatures, to design an IoT-based traceable drug anti-counterfeiting management system, which has the characteristics of public verification. Let us take the message transmitted by the drug manufacturer and the material supplier as an example. When the drug manufacturer sends a message signed with ECDSA to the material supplier, the material supplier will first verify the correctness of the time stamp and the signature, and then generate the blockchain message $BC_{DM-MS} = h(r_{DM-MS}, s_{DM-MS})$, and use ID_{BC} as an index to upload the blockchain data to the blockchain center. The material supplier will then send the blockchain data BC_{DM-MS} to the next character after it is signed by ECDSA. That is to say, after verifying the correctness of the time stamp and signature for each role that receives the message, it also verifies the correctness of the blockchain data generated by the previous role. Therefore, the solution we proposed achieves the characteristics of public verification through blockchain technology and ECDSA digital signature.

G. AUTOMATED MANAGEMENT

At present, many countries in the world have proposed a set of drug identification code coding and management principles for their pharmaceutical industry. This drug identification code is usually divided into two parts. The first part is the drug classification code managed by the country's drug administration, and the second part is the drug production serial number managed by the drug manufacturer. The two parts are combined, which form the unique identification code of the drug. Through the consistent coding principle, the drug can be quickly checked, classified, and transported when it is circulating on the market, reducing human intervention and processing, and achieving the goal of automated drug management.

H. COMPUTATION COST ANALYSIS

Table 2 is the computation cost analysis of all stages and roles in this scheme. We analyze the drug testing and approval phase with the highest computational cost. The drug manufacturer requires 7 multiplication operations, 3 hash function operations, 2 comparison operations, and 3 signature operations. The drug administration requires 7 multiplication operations, 3 hash function operations, 2 comparison operations, and 3 signature operations in the drug testing and approval phase. The method we proposed has a good computational cost.

I. COMMUNICATION COST ANALYSIS

The communication cost analysis of each phase in this scheme is shown in Table 3. We assume that the ECDSA key and signature are 160 bits, the hash function calculation is 160 bits, and the rest of the message length such as ID

TABLE 2. Computation cost analysis of this scheme.

Phase \ Role	BCC	DM	MS	DA	DD
System role registration phase	$1T_{Mul}$	N/A	N/A	N/A	N/A
Drug development and trial phase	N/A	$7T_{Mul}+3T_H$ $+2T_{Cmp}+2T_{Sig}$	$7T_{Mul}+3T_H$ $+2T_{Cmp}+2T_{Sig}$	N/A	N/A
Drug testing and approval phase	N/A	$7T_{Mul}+3T_H$ $+2T_{Cmp}+3T_{Sig}$	N/A	$7T_{Mul}+3T_H$ $+2T_{Cmp}+3T_{Sig}$	N/A
Drug production and distribution phase	N/A	$7T_{Mul}+3T_H$ $+2T_{Cmp}+2T_{Sig}$	N/A	N/A	$7T_{Mul}+3T_H$ $+2T_{Cmp}+3T_{Sig}$

T_{Mul} : Multiplication operation
T_H : Hash function operation
T_{Cmp} : Comparison of operation
T_{Sig} : Signature operation

TABLE 3. Communication cost analysis of this scheme.

Phase \ Item	Message length	Rounds	3.5G (14 Mbps)	4G (100 Mbps)	5G (20 Gbps)
System role registration phase	480 bits	2	0.034 ms	0.005 ms	0.024 us
Drug development and trial phase	1520 bits	2	0.109 ms	0.015 ms	0.076 us
Drug testing and approval phase	1760 bits	2	0.126 ms	0.018 ms	0.088 us
Drug production and distribution phase	1840 bits	2	0.131 ms	0.018 ms	0.092 us

and time stamp is 80 bits. We analyze the drug production and distribution phase with the highest communication cost. The message sent by the drug manufacturer to the drug distributor includes 3 ECDSA keys and signatures, 1 hash function operation, and 5 other messages. The message sent by the drug distributor to the drug manufacturer includes 2 ECDSA keys and signatures, 1 hash function operation, and 4 other messages. The total communication cost in the drug production and distribution phase is 1840 bits, which takes 0.131 ms under 3.5 G (14 Mbps) communication environment, 0.018 ms under 4 G (100 Mbps) communication environment, and it takes 0.092 us under 5 G (20 Mbps) communication environment. The solution we proposed has excellent performance [24].

TABLE 4. Feature comparison of drug supply chain WORKS.

Feature \ Scheme	Wazid et al. [18]	Haq et al. [19]	Tseng et al. [20]	Sylim et al. [21]	Our proposed scheme
Blockchain architecture	No	Yes	Yes	Yes	Yes
Data integrity	Yes	No	No	Yes	Yes
Anti-counterfeit drugs	Yes	Yes	Yes	Yes	Yes
Resist replay attacks	Yes	No	No	No	Yes
Message is irreversible	Yes	Yes	No	Yes	Yes
Non-repudiation	No	No	No	No	Yes
Publicly verifiable	No	Yes	Yes	Yes	Yes
Automated management	No	Yes	Yes	Yes	Yes
Complete supply chain process	No	Yes	Yes	Yes	Yes

J. FEATURE COMPARISON

Table 4 is the feature comparison of the scheme proposed by other scholars with this scheme.

VI. CONCLUSION

With the rapid development of the social economy, our lives are flooded with all kinds of counterfeit products. The public's attitude of greedy for petty and cheap has encouraged unscrupulous manufacturers to take advantage of the opportunity to provide low-cost counterfeit products, suppress the profits of legitimate manufacturers, and also make the public lose confidence in the quality of the products. At present, many fresh foods in the society have provided traceability services of production history, providing consumers with inquiries and confirmation of the production process of the product. In addition to food, counterfeit drugs, and vaccines or lack of production management will pose a major threat to the safety of patients' medication. Existing traceability systems are still mostly built in a centralized manner, and the central agency provides trust guarantees, but the public still has great doubts about the credibility of the central agency. Although traditional information technology can provide partial solutions to the above problems, it cannot solve all the problems. The introduction of blockchain technology can perfectly solve the lack of existing architecture and the environment.

In this research, we propose an IoT-based traceable drug anti-counterfeiting management system, a comprehensive plan from drug research and development, certification, production to sales. The drug manufacturer starts by contacting the raw material supplier to develop a new drug and then is approved by the drug administration until the drug distributor conducts terminal sales. All information about the drug circulation process is uploaded on the blockchain and the data is signed by each role, thus it cannot be tampered with privately by interested people. Therefore, the legality of the data can be verified by a third party at any time, and the complete production history of the drug can be traced to achieve the purpose of the anti-counterfeiting of the drug and ensure drug safety. The framework we propose meets the requirements of information security for data integrity, resistance to replay attacks, irreversible information, and non-repudiation. Through the integration of the Internet of Things and blockchain technology, in addition to achieving the main purpose of the anti-counterfeiting of drugs, it has also achieved the goal of automated management of the overall supply chain.

REFERENCES

[1] J. Mondiale *Anti-Contrefaçon 2017: Le Marché des Médicaments Contrefaits*. [Online]. Available: https://www.unifab.com/journee-mondiale-anti-contrefacon-2017/
[2] M. Qi, J. Chen, and Y. Chen, "A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC," *Comput. Methods Programs Biomed.*, vol. 164, pp. 101–109, Oct. 2018.
[3] D. Puthal, R. Ranjan, A. Nanda, P. Nanda, P. Jayaraman, and A. Y. Zomaya, "Secure authentication and load balancing of distributed edge datacenters," *J. Parallel Distrib. Comput.*, vol. 124, pp. 60–69, Feb. 2019.
[4] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.
[5] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1983–2001, 2016.
[6] A. H. Moon, U. Iqbal, and G. M. Bhat, "Implementation of node authentication for WSN using hash chains," *Procedia Comput. Sci.*, vol. 89, pp. 90–98, Jan. 2016.
[7] V. Odelu, A. K. Das, and A. Goswami, "An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card," *J. Inf. Secur. Appl.*, vol. 21, pp. 1–19, Apr. 2015.
[8] P. Gope and A. K. Das, "Robust anonymous mutual authentication scheme for n-Times ubiquitous mobile cloud computing services," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1764–1772, Oct. 2017.
[9] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Gener. Comput. Syst.*, vol. 68, pp. 74–88, Mar. 2017.
[10] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC," *Comput. Commun.*, vol. 110, pp. 26–34, Sep. 2017.
[11] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.-R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.
[12] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.
[13] B. Lin, W. Guo, N. Xiong, G. Chen, A. V. Vasilakos, and H. Zhang, "A pretreatment workflow scheduling approach for big data applications in multicloud environments," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 3, pp. 581–594, Sep. 2016.
[14] Y. Yang, X. Zheng, V. Chang, S. Ye, and C. Tang, "Lattice assumption based fuzzy information retrieval scheme support multi-user for secure multimedia cloud," *Multimedia Tools Appl.*, vol. 77, no. 8, pp. 9927–9941, Apr. 2018.
[15] L. Guo and H. Shen, "Efficient approximation algorithms for the bounded flexible scheduling problem in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 12, pp. 3511–3520, Dec. 2017.
[16] I. Haq and O. Muselemu, "Blockchain technology in pharmaceutical industry to prevent counterfeit drugs," *Int. J. Comput. Appl.*, vol. 180, no. 25, pp. 8–12, Mar. 2018.
[17] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-W. Liao, "Governance on the drug supply chain via gcoin blockchain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, p. 1055, May 2018, doi: 10.3390/ijerph15061055.
[18] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Res. Protocols*, vol. 7, no. 9, Sep. 2018, Art. no. e10163, doi: 10.2196/10163.
[19] *Are You Still Only Detecting or Are You Already Avoiding Counterfeits?* [Online]. Available: https://www.merckgroup.com/en/research/innovation-center/highlights/blockchain.html
[20] B. Geng, "Yi liao ling yu qu kuai lian ying yong mo shi ji mian lin tiao zhan tan tao," *Ability Wisdom*, 2018, pp. 234–235.
[21] 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.
[22] W. Han and Z. Zhu, "An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem," *Int. J. Commun. Syst.*, vol. 27, no. 8, pp. 1173–1185, Aug. 2014.
[23] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process," *Technol. Forecasting Social Change*, vol. 144, pp. 1–11, Jul. 2019.
[24] M. J. Marcus, "5G and 'IMT for 2020 and beyond' [spectrum policy and regulatory issues]" *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 2–3, Aug. 2015.