Hindawi
Complexity
Volume 2024, Article ID 9842389, 1 page
https://doi.org/10.1155/2024/9842389

Retraction

Retracted: Intelligent Digital Currency and Dynamic Coding Service System Based on Internet of Things Technology

Complexity

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Li and X. Jing, "Intelligent Digital Currency and Dynamic Coding Service System Based on Internet of Things Technology," *Complexity*, vol. 2020, Article ID 6647039, 16 pages, 2020.

Hindawi
Complexity
Volume 2020, Article ID 6647039, 16 pages
https://doi.org/10.1155/2020/6647039

Research Article

Intelligent Digital Currency and Dynamic Coding Service System Based on Internet of Things Technology

Shanshen Li[1] **and Xin Jing**[2]

[1]*School of Economics and Management, Xi'an Shiyou University, Xi'an 710065, Shaanxi, China*
[2]*Law School, Shanghai University of Finance and Economics, Shanghai 200433, China*

Correspondence should be addressed to Xin Jing; jingxin@163.sufe.edu.cn

Received 22 October 2020; Revised 28 November 2020; Accepted 30 November 2020; Published 22 December 2020

Academic Editor: Zhihan Lv

The amazing rise of digital currency is not only favored by investors but also attractive to lawbreakers for its anonymity and decentralization. This paper mainly discusses the intelligent digital currency and dynamic coding service system based on Internet of Things technology. In this paper, the RDCAR algorithm is used to realize the routing discovery process of the wireless network. When the intermediate node receives the RREQ message, first of all, to avoid the loop, it checks whether the same RREQ message has been introduced. If it has received it, it will discard it. Otherwise, it will cache the message and attach its own neighbor node list to the signal-to-noise ratio of the channel link, update the RREQ message, and broadcast it. The payment cipher is managed by the bank. When the user opens an account, the bank registers and sends it to the user. The key is generated by the algorithm chip, and the public key is kept in the bank background server. When the bill is delivered to the bank, the bank inputs all the elements on the bill on the counter terminal and transmits it to the verification machine for verification through the bank network. If the verification is correct, it indicates that the bill is indeed issued by the customer, and all bill elements are correct, and payment can be made. The node operation protocol of public chain and alliance chain maintains the operation of the Internet of Things system. The nodes of alliance chain generate new blocks according to the interval of 30 s. When the node fails to complete the block generation within 30 s, it will rotate to the next node. The mkfile command is used to generate 16b, 1 KB, 1 MB, and 1 GB files as input. The peak speed of the encoding service system is about 370 mb/s. The results show that the system designed in this study is robust and suitable for complex trading environment.

1. Introduction

With the rise of the wave of digital currency in recent years, some underlying technologies related to it, such as blockchain technology and distributed accounting methods, also show broad application prospects. Digital currency is moving from theory to reality, and its feasibility and security are being tested. As a typical application of the Internet of Things in the financial economy, the Bitcoin system has attracted much attention due to its decentralized, open, and transparent characteristics. Various cryptocurrencies such as Monero coins and dark coins emerge in endlessly. In addition, central banks and commercial banks in various countries have also used the underlying advanced technology of Bitcoin as a reference, planning to carry out research on legal digital currency, so as to improve the national digital financial system. This shows that the future development of digital currency has broad prospects, but the accompanying digital currency security and privacy issues have become increasingly prominent.

The amazing growth of encrypted digital currency is not only favored by investors but its anonymity and decentralization are also quite attractive to criminals. Although some countries have considered introducing digital currency regulatory policies, the attitudes of different countries are different. Facing the diversified needs of people's life and work, research and deployment of legal digital currency are urgently needed. However, unlike Bitcoin's non-real-time, lightweight transaction information, small transaction volume, and low sensitivity, legal digital currency is circulated

throughout the country and the world, and its security and privacy issues are more prominent, and legal digital currency and its related applications should be suitable for more complex international environments. Therefore, how to strengthen the robustness of the legal digital currency system and build a harmonious credit society by learning from the security and privacy protection measures of the Bitcoin system and Bitcoin wallet is the research direction of our future work. Digital currency is backed by national credit, which can synchronize online and offline to the greatest extent, and maximizes the convenience and security of transactions.

Utilizing the advantages of distributed architecture and proximity to end users, fog/edge computing can provide faster response and higher quality of service for IoT applications. Lin et al. believed that the Internet of Things based on fog/edge computing will become the future infrastructure for the development of the Internet of Things. In order to develop the IoT infrastructure based on fog/edge computing, they first studied the architecture related to the IoT, supporting technologies and issues, and then explored the integration of fog/edge computing and the IoT. They gave a comprehensive overview of the Internet of Things in terms of system architecture, supporting technology, security, and privacy issues and studied the integration of fog/edge computing with the Internet of Things and applications. Their research lacks data [1]. In order to overcome the scalability problem of the traditional IoT architecture, Sun et al. proposed a novel method for mobile edge computing. At the same time, they proposed a layered fog computing architecture in each fog node to provide flexible IoT services while maintaining user privacy; each user's IoT device is associated with the proxy VM (located in the fog node), and proxy VM collects, classifies, and analyzes the raw data stream of the device, converts it into metadata, and then transmits the metadata to the corresponding application VM (owned by the IoT service provider). Each application VM receives corresponding metadata from a different proxy VM. Their research lacks practice [2]. Yang et al. believed that the Internet of Things (IoT) is ubiquitous in our daily lives. In order to protect the security of IoT devices, they have conducted a lot of research work to deal with these problems and find better ways to eliminate these risks, or at least minimize its impact on user privacy and security requirements. Their investigation consists of four parts. The most relevant limitations of IoT devices and their solutions will be discussed first. Then, the classification of IoT attacks will be introduced. Secondly, it will focus on the mechanism and architecture of authentication and access control. Finally, the security issues in different layers will be analyzed. Their research process is too complicated [3]. Yaqoob et al. discussed the architecture of the Internet of Things. In this case, first of all, they investigate, focus on, and report on the recent major research progress in the IoT architecture and then classify the IoT architecture and design a taxonomy based on important parameters (such as applications, supporting technologies, business goals, architecture requirements, network topology, and IoT platform architecture types). They identified and outlined the key requirements of the future IoT architecture and discovered and introduced some outstanding case studies on the Internet of Things. Finally, they listed and outlined the future research challenges. Their research has no practical significance [4].

This research mainly discusses the intelligent digital currency and dynamic coding service system based on the Internet of Things technology. This research is mainly based on the RDCAR algorithm to realize the route discovery process of the wireless network. When the intermediate node receives the RREQ message, first, to avoid loops, check whether the same RREQ message has been introduced. If it is received, discard it. Otherwise, buffer the message and append its own neighbor node list, corresponding to the signal-to-noise ratio of the channel link, and update RREQ message and broadcast it. The payment cipher is managed by the bank. When the user opens an account, the bank registers and sends it to the user, and the key is generated by the algorithm chip, and the public key is stored in the bank's back-end server. When the bill is delivered to the bank, the bank enters the various elements of the bill on the counter terminal and transmits it to the verification machine through the bank network for verification. If the verification is correct, it indicates that the bill is indeed issued by the customer, and the bill elements are correct, so you can make payment. The public chain and alliance chain node operation agreement maintains the operation of the Internet of Things system. The alliance chain node generates new blocks at a time interval of 30 s. When the node cannot complete the block generation within 30 s, it will rotate to the next node.

2. Dynamic Coding Service System

2.1. Internet of Things. The IoT paradigm is expected to completely change the way we live and work through a large number of new services based on the seamless interaction between a large number of heterogeneous devices. After decades of creation of the concept of the Internet of Things, in recent years, various communication technologies have gradually emerged, reflecting the diversity of application fields and communication requirements. At present, this heterogeneity and fragmentation of the connectivity landscape hinder the full realization of the vision of the Internet of Things by posing some complex integration challenges. In this case, the emergence of 5G cellular systems with truly ubiquitous, reliable, scalable, and cost-effective connection technologies is considered to be a potential key driver of the yet-to-be-emerging global Internet of Things. Similar to how humans use the Internet, devices will become the main users of the Internet of Things (IoT) ecosystem. Therefore, device-to-device (D2D) communication is expected to become an inherent part of the Internet of Things. Devices will automatically communicate with each other without any centralized control and cooperate in a multihop manner to collect, share, and forward information. The ability to collect relevant information in real time is the key to leveraging the value of the Internet of Things because such information will be transformed into intelligence, which will help create a

smart environment. Ultimately, the quality of the information collected depends on the intelligence of the device. In addition, these communication devices will operate with different networking standards and may encounter intermittent connections with each other, and many of them will be limited by resources. These features bring some networking challenges that traditional routing protocols cannot solve. Therefore, devices will need intelligent routing protocols to be intelligent. Nowadays, the development of traditional business models has become more and more mature, and people use them to guide various e-commerce activities [5, 6]. The Internet of Things (IoT) is an innovative revolution on the Internet and has become a new platform for e-commerce [7].The flow of static timing constraints is shown in Figure 1.

2.2. Positive Impact of Digital Currency. For many people, the concept of digital currency is abstract and confusing. Having confidence in intangible assets without government or precious metal support is a daunting task. However, the rapid spread of smartphones and tablets, the rapid transformation of cross-border banking, and the emergence of non-card real-time payments have made digital payments commonplace. First of all, it has a positive impact. Digital currency creates a relatively novel concept and model, which can improve transaction convenience and reduce transaction costs, promotes the progress and development of shared finance, and decentralizes the digital currency embedded payment system mainly from its own; the system allows users to directly carry out peer-to-peer transactions without resorting to financial units, which can improve transaction efficiency and reduce transaction costs. At the same time, its lower transaction costs will have an impact on traditional payment systems and promote banks and other financial institutions to continuously improve their service quality and reduce transaction costs. Secondly, digital currency can allow people who have not created an account in a financial unit to carry out noncash payments, and the speed is very fast, and the cost is low. Therefore, digital currency has a positive impact on the popularization of finance, especially for those who are relatively backward in finance. In regions and countries, the benefits it brings are also very large [8, 9]. Digital currency can realize network transfer with the help of mobile phones and so on, and the recipient only needs to obtain digital currency to exchange activities with it [10]. When there is no code perception, it is shown in Figure 2, and when there is code perception, it is shown in Figure 3.

2.3. Verify Algorithm. The Verify algorithm uses a layered verification mechanism to verify whether the hidden transaction amount is correct [11, 12]. Specifically, it will be stated in Verify-I that the payer has enough bitcoins; that is, the payee must be convinced that the input of the transaction is greater than the output. Then, the recipient verifies that the transaction amount promised by the wallet is equal to the actual transaction amount in Verify-II. In the commitment phase, the wallet will make a commitment to both the bitcoin deposit amount $b1$ and the bitcoin transaction amount $b2$ $(b < 2 \le b1)$. In addition, the wallet will also promise the difference between $b1$ and $b2$. In the verification phase, the correctness of the commitment value is checked in two steps: (1) the difference between the input amount $b1$ and the output amount $b2$ is always positive and (2) the promise made by the payee to the correct transaction amount is always the same as the promise value c of the wallet [13]. Online wallet calculates $F1$ and $F2$ and sends $(F2, F3)$ to the payee:

$$\begin{aligned} F1 &= h_1^{m-a} h_2 \bmod n, \\ u(t) &= u_i(t-\Delta t) R^L(\Delta t) + u_i(t) \sum_{i=1}^{n} (t+\Delta t)(t-\Delta t), \\ e_0(\lambda, T) &= \frac{5\pi \mathrm{HC}}{\lambda^6} \frac{1}{e^{(hc/\lambda KT)}} - \frac{hc}{e}. \end{aligned} \tag{1}$$

Recipient calculation is as follows:

$$\begin{aligned} U &= \frac{h1}{F_3} = h_1^{\beta} h_2^{-r\alpha^2 - q_1\alpha - q_2} \bmod n, \\ F_2 &= \frac{1}{Q} \sum_{\omega \in Q} \exp\left\{-\frac{U(z)}{T}\right\} \delta(z-\omega), \\ M &= T[x, y, p(x, y), f(x, y)]. \end{aligned} \tag{2}$$

If the check passes, the recipient can trust $m \ge \alpha$. At this stage, my country's main basis for this supervision is only this notice, and there is no other effective document [14, 15]. Moreover, the measures of my country's regulatory authorities are mainly aimed at preventing financial risks and money laundering crimes. The protection of financial consumers is mainly based on the principle of "risk yourself." The overall rules are relatively rough. The filing system for trading platforms is not a licensing system. This has led to the obligation of financial institutions and digital cryptocurrency trading platforms to be limited to popularizing industry knowledge and risk disclosure, accepting irregular administrative inspections, and so on [16] and make substantive requirements for deeper content such as the entry barriers of the trading platform, network security, information disclosure, and fund management. As a result, the chaos in the digital cryptocurrency market has not been curbed, and even with the emergence of ICOs, lawsuits for digital cryptocurrency continue to increase [17, 18]. Recipient calculation is as follows:

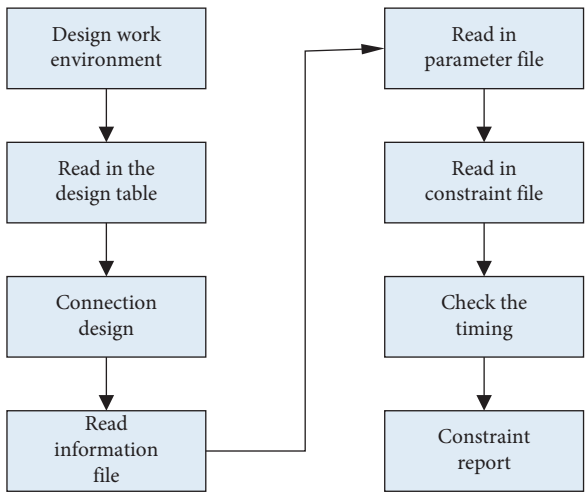

Figure 1: Flow of static timing constraints.

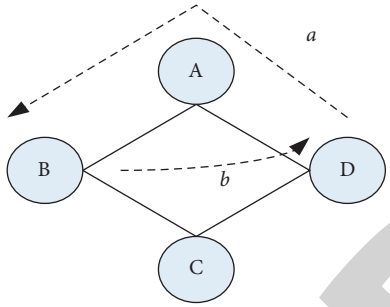

Figure 2: No coding perception.

$$c = \frac{c_1}{c_2'} = h1^{b1-b2'} h2^{r1-r2},$$

$$c_1 = -2\left(r_{ui} - \sum_{f=1}^{F} p_{uf} q_{if}\right) + 2p_{uf}, \tag{3}$$

$$c_2 = \frac{\sum_{i\in I}(h_1 - \overline{r_u}) \times (h_2 - r_u)}{\sqrt{\sum_{i\in I}(r_{ui} - \overline{r_u})^2 \sum_{i\in I}(r_{vi} - \overline{r_v})^2}}.$$

Verify that c is equal to c'. If there is any error in the verification process, the payee returns 0 and rejects the transaction [19]. If the verification is successful, the payee returns 1, and then the online wallet broadcasts the encrypted transaction and sends the digital currency amount to the payee account [20, 21].

2.4. Code-Aware Routing Algorithm. In wireless networks, the quality of the channel is the key to the successful transmission of data, which is generally measured by the signal-to-noise ratio [22]. The channel quality has great differences in different links of the actual network [23, 24].

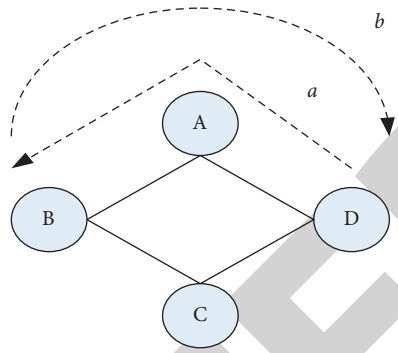

Figure 3: Coding-aware.

$$h = \sum_{i=1}^{n} co_i h_{\min} + \sum_{i=1}^{n} co_i,$$

$$D_1^K = P(x_i \in x_k, y_i = 1) = \sum_i x \in x_k(i), \tag{4}$$

$$D_{-1}^K = P(x_i \in x_k, y_i = -1) = \sum_i x \in x_k D_{-1}.$$

The final strong classifier is as follows:

$$H(x) = \sin g\left(\sum_{t=1}^{T} h_t(x) - \text{threshold}\right). \tag{5}$$

If you want to transmit under poor channel quality, you must choose a relatively low transmission rate. There are many broadcasting situations in network coding. When broadcasting to various downstream nodes, the signal-to-noise ratio of each single link in the broadcasting link is different [25]. Choosing a suitable broadcasting transmission rate can make the throughput efficiency reach during this broadcast maximum. The coding-aware routing algorithm based on rate selection is expressed as follows:

$$M = \min_{l\in L}\left\{M_l | M_l = \frac{H_l * H_l'}{R_l}\right\},$$

$$\text{MIQ}_s(c) = \text{MQ}_s(c) + \sum_{t\in c} \text{MQ}_s(i),$$

$$\text{MIQ}_d(c) = \text{MQ}_d(c) + \sum^{t\in c} \text{MQ}(l), \tag{6}$$

$$\text{CRM}_J = \frac{1 + \text{MIQ}_d(l)}{1 - P_t}.$$

Among them, M is a unicast or broadcast link on the entire link L for data packet transmission. When the data

link layer successfully transmits a data packet, the routing layer initiates a transmission [26].

$$\text{Angle}(a, r) = \arccos\left(\frac{a \bullet r}{|a| * |r|}\right),$$

$$\min\left(E^2\right) = \sum_{k=1}^{N} \left[y'(k) - y(k)\right]^2, \tag{7}$$

$$s = \{x_1, y_1\}, (x_2, y_2), \ldots, (x_N, y_N).$$

The probability of successful data packet transmission on the data link layer is as follows:

$$p_i^j = \sum_{k=1}^{5} \left(1 - p_{1i}^j\right)^{k-1} p_{1i}^j,$$

$$\text{CRM}_L = \sum_{I \in L} \text{CRM}_J,$$

$$F^2(s, v) = \frac{1}{s} \sum_{i=1}^{s} \{Y[N - (v - N_s) + i] - y_v(i)\}^2, \tag{8}$$

$$P_{n,j} = \frac{p_{n,t}}{p_{n,t-1}} - 1,$$

$$P_j = \frac{p_{n,t}}{p_{n,t-1}}.$$

That is, the probability of starting a routing layer transmission is p_i^j. The process of the Verify algorithm generating code is shown in Figure 4.

3. Dynamic Coding Service System Experiment

3.1. System Framework Design. The system is divided into four parts: the background server, the foreground management system, the foreground business system, and the cipher. The back-end server is equivalent to a certification authority CA, which stores the user's certificate information and completes the actual verification process. It is generally the server of the head office. The front-end management system is the management program on the front-end computer of the branch, which manages the user account information, the issuance and management of the user password, the management of the operator and the log query, and so on. The front desk business system is a business management program on the front-end computer of the branch. It uses the information on the check and the payment password to verify the authenticity of the check and generally provides services for the bank transfer system. The cipher is a handheld device used by the user, which is issued to the user by the bank to implement the user-side algorithm in hardware, including the generation of the key and the generation of the payment password. The system framework is shown in Figure 5.

3.2. Cipher. The encryption chip integrates RSA and SHA-1 algorithms and saves the user's key. There are two types of chips: A slice is mainly a public key algorithm, which is used in the payment password verification subsystem, and B slice is mainly a private key algorithm, which is used in the payment cipher used by the account opening unit. The payment cipher adopts the B-chip arithmetic chip to make a handheld device to manage the user's account and key and generate payment password. The payment cipher is managed by the bank. When the user opens an account, the bank registers and sends it to the user, and the key is generated by the algorithm chip, and the public key is stored in the bank's back-end server.

3.3. Password Management. The payment cipher is issued by the bank to the customer who opens an account with the bank and downloads the account number of the customer with the bank and the corresponding account key in it. When the customer uses the account to issue a bill, enter the bill number, bill type, amount, and other information on the payment cipher and use the payment cipher to automatically calculate a string of numbers. This number is closely related to the payer account number, receiver account number, bill type, bill number, amount, and date of signing and is called the payment password. The customer fills in the number on the bill as the digital seal of the bill. When the bill is delivered to the bank, the bank enters the various elements of the bill on the counter terminal and transmits it to the verification machine through the bank network for verification. If the verification is correct, it indicates that the bill is indeed issued by the customer, and the bill elements are correct, so you can make payment.

3.4. Calculate the Plaintext Format of Payment Password. The format of the 48-byte plaintext data PLAIN_TXT input to the B slice when the payment password is generated is shown in Table 1. After the chip output is converted, it is a 19-digit integer plus 1 identification bit to form a 20-digit payment password output. The plaintext format of the payment password is shown in Table 1.

3.5. Design of the Alliance Chain. System initialization completes the generation of system parameters and the initial state of the blockchain; transaction verification and forwarding are the process of sharing information among alliance chain members, ensuring that nodes reach consensus on the same basis; the consensus process includes the specific process of node interaction in CPBFT; transaction confusion is responsible for after the transaction is confirmed, and the transaction is processed before being sent to the public chain node to remove the transaction relationship information to protect transaction privacy; the final transaction traceability is the process of internal supervision of the system. The communication between nodes in the alliance chain uses encrypted channels to prevent information leakage when the communication transmits the plaintext and completes transactions.

3.6. Choice of Algorithm. The Verify algorithm aims to check that the difference $b1 - b2$ between the input amount and the

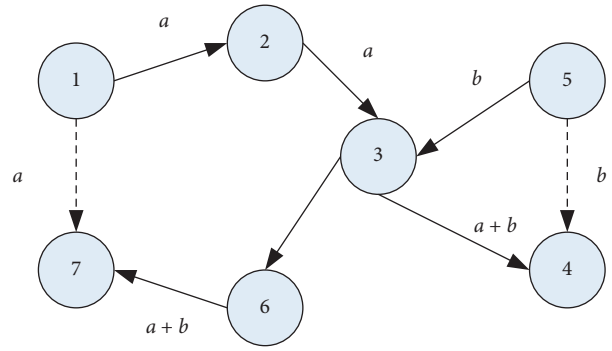

Figure 4: The process of the Verify algorithm to generate code.

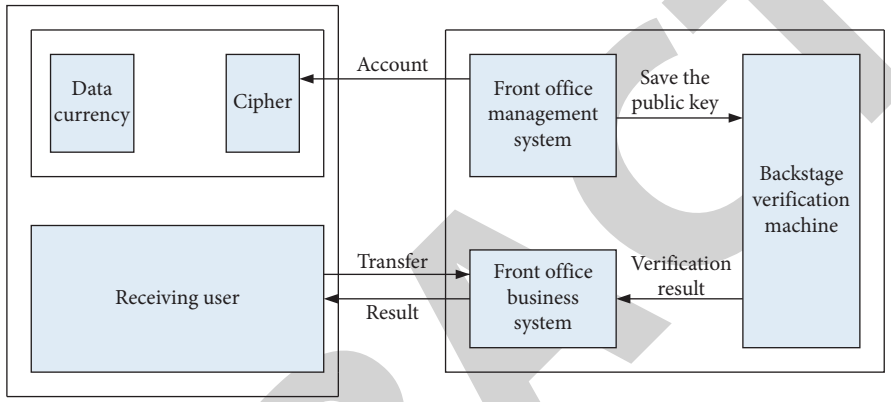

Figure 5: System framework.

Table 1: Plaintext format of the payment password.

ACCU	16	Account, compressed BCD code
Service	4	Business type, 0×31–0×35
Date	4	Date, compressed BCD code
Ticket_ num	8	Voucher number, compressed BCD code
Balance	9	Amount, in minutes, compressed BCD code

output amount of the transaction is always positive, and the output amount $b2$ is the transaction amount specified by the payee. The algorithm first confirms that the promised secret value is always positive. To this end, the payer commits to the difference between the input amount and the output amount of the transaction. Then, use the range proof method to convince the payee to believe that the promised secret value is always positive. Secondly, because the recipient knows the correct transaction amount $b2$ in advance, he also needs to use the correct transaction amount and some auxiliary evidence $c1$ and $r2$ to verify that the final commitment value is equal to the commitment value c made by the wallet. We call this two-step verification method a layered verification mechanism. If the algorithm returns 1, the protocol goes to the next step.

3.7. Operation Process Design. The peer relationship between public chain nodes and alliance chain nodes in the system is just different in processing messages. Together, these two parts can be regarded as servers. The user's wallet is the client and sends operation requests to the server. After each part of the system starts running, it performs related functions according to the protocol designed in chapter 4. When there is no user to send a transaction, the blockchain node automatically runs the consensus process in a loop to maintain the consistency of the system and waits to process the sent transaction information. After the user sends the transaction, it is collected and processed by the alliance chain nodes, including verification transactions, packaged transactions, and transaction confusion, and finally the confirmed transactions are confused and broadcasted to the public chain nodes to complete the complete transaction confirmation and recording process. When the system initiates the traceability, the entire process only occurs between the alliance chain nodes. The traceability initiating node initiates a request to other alliance chain nodes including the supervision node. The other alliance chain nodes in the figure include more than one node, and the request is judged separately, and the supervised node obtains the user identity after recovering the

key. The design values of running nodes are shown in Table 2. The running process is shown in Figure 6.

3.8. Implementation of Routing Algorithm. The route discovery process of RDCAR is as follows:

(1) The source node initiates the route discovery process of the wireless network by broadcasting a route request (RREQ) message . In our algorithm, the routing request message needs to include the following messages: neighbor nodes within the range of the source node, high channel quality signal-to-noise ratio, and the path that has been transmitted.

(2) The intermediate node receives the RREQ message; first to avoid loops, check whether the same RREQ message has been introduced and discard it if it is received; otherwise, it will buffer the message and attach its own neighbor node list, corresponding to the signal noise of the channel link, and then update the RREQ message and broadcast it.

(3) When the RREQ arrives at the destination node, the destination node sends a route reply request (RREP) message to the source node. This is a unicast message that contains information on this unicast path.

(4) When the intermediate node receives the RREP message, it selects a value from the set of rates supported in the 802.11 protocol, calculates the expected number of transmissions based on the stored signal-to-noise ratio information, selects the appropriate rate, updates the neighbor node list, and finally calculates the smallest metric value. Then, add this information to RREP. Take out the RREQ path in the cache and compare it with the upstream path set in the RREP. Use the conditions of the encoding node above to check whether there is an encoding opportunity for the new stream. If it exists, calculate the metric value of the broadcast link. Add the minimum metric value to RREP, and continue forwarding the cached path until it reaches each source node.

(5) Maintain routing regularly, update routing messages, and reselect the most appropriate path for the current distributed flow. The realization of the routing algorithm is shown in Figure 7.

3.9. IoT Node Operation. The public chain and alliance chain node operation agreement maintains the operation of the Internet of Things system. The alliance chain node generates new blocks at a time interval of 30 s. When the node cannot complete the block generation within 30 s, it will rotate to the next node. Similar rules are also used in the public chain to generate block rights maintenance system operation.

3.10. Realization of User Transfer Process. The transfer behavior takes place in the user's wallet, and the user first verifies his identity using the wallet. The user's login name and corresponding password are stored locally, and the password retains the value after MD5 calculation. During the login process, compare whether it is the same as the previously saved record. After the user logs in, the wallet will check whether the user has an identity certificate issued by the authentication server in the system. Only transactions sent by users registered in the system will be received by the alliance chain node. When the user does not store the identity certificate in the node, the wallet will prompt user complete the authentication. Users can use the wallet to initiate transfers, and they can also query the status of the account. Transfers between users need to use the public key as the address to receive the transfer. In fact, the public key is associated with the payment transaction so that the currency obtained in the payment transaction is used. When making a payment, you can prove your ownership of the currency through the private key corresponding to the public key and pass the cryptographic algorithm without the need to pass a centralized credit institution. The generated payment address will be displayed, and the corresponding private key will be stored in the file by the wallet and used in the transaction. The payment address can be sent to other users in the digital currency system by means of communication outside the system.

After sending the transaction, the user needs to wait for the alliance chain node and the public chain node to perform a series of operations and finally store the relevant transfer-in and transfer-out transactions in the public chain block. The wallet has stored the label and content of the complete transaction for a period of time. By comparing the data stored in the public chain, you can check whether the transaction you initiated has been written to the block and confirmed by multiple blocks. To initiate a transfer, users need to use their USOT as the payment method, provide the corresponding private key, send currency to the public key provided by the other party, and provide one or more public key addresses of their own as the change address. The total amount of currency in the USOT provided by the transaction initiator cannot be less than the payment amount. If the balance cannot be exactly equal, the excess amount will be sent to the change address and returned to the payer.

3.11. Traceability and Transaction Disclosure. Traceability is initiated and completed internally by the alliance chain, and the result of the transaction traceability can be seen in the end. The goal of retroactive transactions is generally a transfer-out transaction because the initiator of a complete transaction on the transfer-out exchange is the owner of the transfer-out transaction address, and the identity of the initiator can be queried. If no one spends it for a transfer-in transaction, it cannot get the owner of the transaction. When searching for a transaction, according to the query transaction serial number, it traverses the plaintext of transaction information saved in the block, finds the block containing the same serial number, decrypts the transaction, finally finds the transaction, and displays the complete record in the transaction.

3.12. System Test and Implementation. This system runs under Windows and uses Java language for programming.

Table 2: Design values of operating nodes.

Constraint content	Settings (ns)
Input delay	3.1
Output delay	3.0
Clock jitter and skew	3.2
Drive capability	3.2

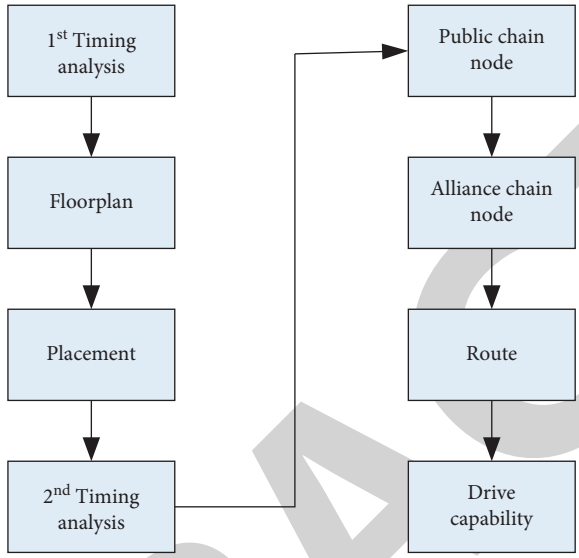

Figure 6: Running process.

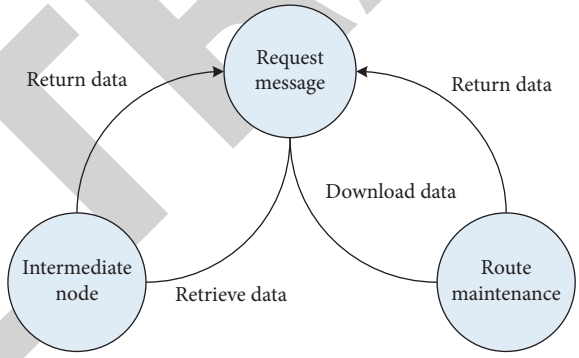

Figure 7: Implementation of the routing algorithm.

The machine configuration for system testing is shown in Table 3. This system uses the JPBC (Java Pairing-Based Cryptography) library. JPBC is a Java package based on the paired cryptography library function (PBC). JPBC completely breaks away from the dependence of PBC, realizes the pair operation completely based on Java, and puts aside the limitations of the platform itself. This system uses it as the basic support library for cryptography. In addition to the basic upload and download function files, this system mainly includes the following types of files that generate user keys, generate keyword ciphertexts and secret doors, and implement keyword encryption and search. CLPEKS.java is used to implement various algorithms. CLPEKS Pub Params.java is used to store public parameters, Service and Client Key Interface java is an interface class for client and server keys, CLPEKS Secret Key.java and CLPEKS Client Key java store server and client keys, respectively, and CLPEKS Cipher text.java and CLPEKS Trap door.java store ciphertext and secret door, respectively.

4. Analysis of Dynamic Coding Service System

4.1. Algorithm Performance Analysis. The performance test mainly includes two aspects. On the one hand, the algorithm performance changes under different matrix sizes, that is, when N is different; on the other hand, the performance differs between the test algorithm and the SM2 algorithm. First, test the performance of the algorithm when different matrix sizes are different, that is, when N is different. When the test N is 4, 8, 16, 32, and 64, the number of signatures and

Table 3: Machine configuration during the system test.

Project	Value
Operating system	Microsoft Windows 7 Ultimate
Version	6.1.7601 Service Pack1 internal version 7601
System type	x64-based PC
Processor	Intel8CoreTM i3-2310M
CPU	2.10 GHz
RAM capacity	8 GB

verifications per second by the algorithm and the experimental results retain two significant digits. The performance of the algorithm at different matrix sizes is shown in Table 4. It can be seen from Table 4 that with the increase in the matrix size, the performance of algorithm signature and verification is gradually decreasing. The reason is that the larger the matrix size, the more cycles in the GeneratePrivateKey and Public Key Derivation GeneratePublicKey methods. At the same time, the performance of the verification algorithm drops faster because the loop of the GeneratePublicKey method in the verification process contains the accumulation of elliptic curve points which takes longer. However, although the performance of the algorithm decreases as the matrix size N increases, the security of the algorithm will increase as N increases. Next, test the performance difference between this algorithm and the standard SM2 signature algorithm. When the test matrix size $N = 64$, the number of signatures and verifications per second of this algorithm and the SM2 algorithm are the same. The initialization of the private key matrix SKM and the public key matrix PKM will only be performed once, so this part of the time is not calculated. From an algorithm perspective, the performance difference between the two algorithm signatures (or signature verification) is the time it takes to derive the key from the matrix. The performance difference of the signature of the two algorithms is greater than the performance of the verification. This is because the calculation of the private key corresponding to the public key in the private key derivation algorithm (the private key class contains the public key) will involve the elliptic curve dot product operation. The dot multiplication operation takes a long time. It can be seen from Table 4 that when the matrix size is $N = 64$, the signature and verification efficiency of this algorithm are both close to half of the efficiency of the SM2 algorithm, and the performance difference is due to the secret key of the proxy signature private key and the proxy verification public key derived from overhead. On the whole, performance has been lost, but according to the safety analysis of this algorithm, the overall safety limit of the system has been increased from 1 to 33. After that, the SM2 hash algorithm and this research algorithm are tested for performance comparison. Use the mkfile command to generate 16B, 1 KB, 1 MB, and 1 GB files in sequence as input. After 10 tests, according to the test results, as the length of the input message increases, the computational efficiency of SM2 and this research show an upward trend first and then reach a peak. The peak algorithm speed of SM2 is around 100 MB/s, and the peak algorithm speed of RDCAR is around 370 MB/s. On the whole, the efficiency of the algorithm in this study is higher than that of SM2. This is not because of the gap in the algorithm itself but because the bottom layer of the Go algorithm is implemented in assembly, which is more efficient. The performance analysis of the algorithm at different matrix sizes is shown in Figure 8. Before the simulation is carried out, it is necessary to specify specific voltage values for the power signal and ground as shown in Table 5.

4.2. Dynamic Coding Analysis. Use simulation tools to simulate the RDCAR routing algorithm. We take the network model of the grid graph and distribute 25 nodes in the range of $100 \times 100\ m^2$, and the communication range of each node is 20 m. 11 streams are randomly generated in the network. The purpose of our experiment is to compare RDCAR, DCAR protocol, and COPE coding protocol. Since there is no DCAR protocol and COPE coding protocol, there is no rate-aware algorithm, so the rate of DCAR and COPE cannot be automatically adjusted. Let's take a look at the coding opportunities and throughput. Under different speeds and signal-to-noise ratios, compare the coding opportunities and throughput of RDCAR. The rates of COPE and DCAR we used here are the same, so the difference in coding opportunities is enough to reflect the difference in throughput. At the same time, the increase in coding opportunities will lead to the increase in throughput, so the number of coding opportunities can reflect the size of throughput. The simulation shows the comparison of coding opportunities at different rates in a low channel capacity environment. We can see that in the actual situation of about 5 to 10 dB, the channel quality is very poor and the packet loss rate is quite high. DCAR and COPE use a minimum of 12 mbps, and DCAR and COPE use 24 mbps for coding opportunities. Our RDCAR uses a rate selection algorithm, so it will use a lower transmission rate to ensure the number of successes on a poor link and use a higher transmission rate on a better link to increase throughput. We found that DCAR adopts coding-aware routing scheme and can actively discover coding opportunities. Therefore, under the same circumstances, no matter what transmission rate is used, it is better than COPE. When the channel environment of 5 to 10 dB is poor, compared with the two cases of 12 mbps and 24 mbps, using 12 mbps to guarantee the transmission rate, the coding opportunity and throughput are better than those of 24 mbps. The medium quality channel ranges from 10 to 20 dB. Since under medium channel quality, a certain transmission success rate can be guaranteed even when 48 mbps is used again, and we can see that as the transmission rate increases, under the premise of ensuring a

Table 4: Algorithm performance at different matrix sizes.

Algorithm	$N=4$	$N=8$	$N=16$	$N=32$	$N=64$
Signature	221.72	262.47	251.89	239.81	219.78
Check	245.10	227.27	224.72	189.39	155.28

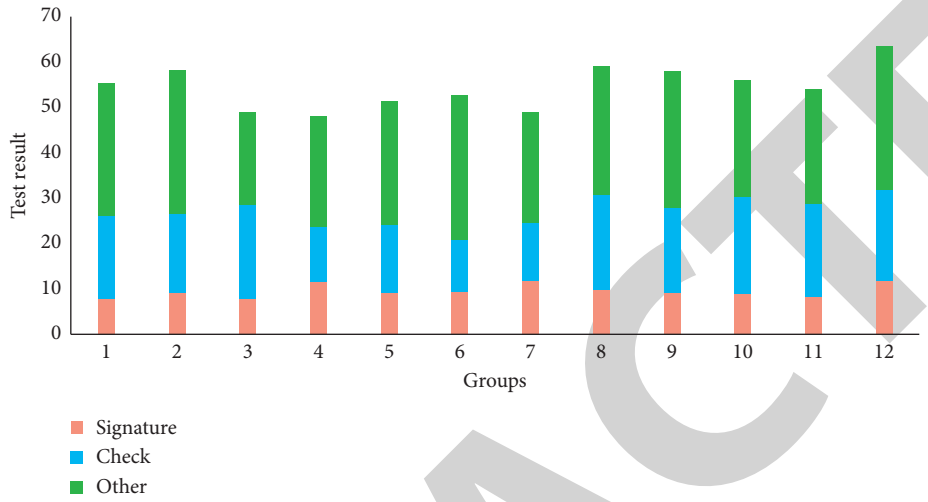

Figure 8: Algorithm performance analysis at different matrix sizes.

Table 5: Before the simulation, you need to specify specific voltage values for the power signal and ground.

Net name	Voltage value (V)
AWCC1V8	1.8
DD RYTT	075
GND	1.2
YCC1V2	1.8
YCC1V8	33

certain transmission probability, the coding of COPE and DCAR opportunities and throughput gradually approach RDCAR. Due to the high channel quality, the success rate of information transmission is very high, and the main factor that affects coding opportunities and throughput is the transmission rate. Therefore, we can see that in Figure 9, when DCAR and COPE only use low-speed channels, the low transmission rate guarantees success rate is no longer applicable but greatly affects the transmission efficiency, making the coding opportunity and throughput smaller. DCAR and COPE use medium-speed channels. It can be seen that the coding efficiency of RDCAR is still far behind when using 24 mbps. The transmission rate of RDCAR in our actual simulation is about 48 mbps. Therefore, we found in subsequent experiments that if 48 mbps high-speed transmission is used, the coding opportunities of DCAR and RDCAR are quite close, and there is a certain gap between COPE and DCAR. The coding situation monitored by different transmission rates is shown in Table 6. The learning step length of the RDCAR algorithm is shown in Table 7. The original high-frequency coded signal collected by using the oscilloscope is shown in Figure 10.

4.3. Function Analysis. The model proposed in this study not only includes the antitampering, traceability, and decentralization characteristics of transactions in the existing digital currency system but also adds supervisable attributes to the system to enhance the system's ability to protect user privacy. The performance test is divided into two aspects. On the one hand, it tests the performance changes of the algorithm under different matrix sizes, that is, N; on the other hand, it tests the performance comparison between this algorithm and the standard SM2 signature algorithm. During the test, first create a plaintext byte array and assign values, then create a key byte array and assign values, create an encryption instance by calling sm4.NewCipher (key), and then call c.Encrypt to calculate the encryption result. Then, call c.Decrypt to calculate the decryption result. The performance of the algorithm changes when the test matrix size N is different. When the test N is 8, 16, 32, and 64, calculate the number of signature tests and verification times of the algorithm per second. The result of functional analysis is shown in Figure 11. Since authorization generation and authorization verification will only occur once when the system is initialized, this part of the time is not calculated. In

Figure 9: Comparison of encoding opportunities at different rates.

Table 6: Coding situation monitored by different transmission rates.

Project	Infeasible area	Feasible region	Near real POF
5 dB	(0.10, 0.20)	(0.40, 0.55)	(0.30, 0.45)
10 dB	(0.10, 0.10)	(0.70, 0. 70)	(0.60, 0.64)
12 mbps	(0.10, 0.20)	(0.40, 0. 50)	(0.24, 0.27)
24 mbps	(0. 10, 0.20, 0.10)	(30, 0.7, 0.25)	(0.12, 0.31, 0. 67)
36 mbps	(0.20, 0.50, 0 60)	(70, 0.7, 0. 50)	(0.50, 0.77, 0.37)
48 mbps	(0.20, 0.50, 0.60)	(70, 0.7, 0.50)	(0.50, 0.77, 0.37)

Table 7: Learning step size of the RDCAR algorithm.

Number of learning samples	Number of test samples	Number of hidden nodes	Learning step
100	50	8	0.005, 0.005
100	50	8	0. 005, 0. 005

terms of privacy protection, the complete transaction records are encrypted and stored. Only after initiating the traceability of the transaction and voting by the members of the alliance chain, can the transaction plaintext be viewed by the special members of the alliance chain. After completing a consensus, the alliance chain broadcasts a batch of transfer-in and transfer-out transactions, hiding multiple pieces of information belonging to the same complete transaction in a large amount of similar information and avoiding the leakage of user privacy in the process of information interaction. The public transaction records stored in the public chain for query, because of truncation and confusion, lose the traceable transaction relationship information and have the unlinkability of the transaction output required by the digital currency public chain data. The data stored in the alliance chain node have the most restrictive restrictions on access rights. During the normal operation, the alliance chain node only has the write permission, and the verification function in the system is completed by the data in the public chain block. In terms of supervisable attributes, when there is a need for the system to trace the transaction, the alliance chain node initiates a transaction traceability application, and the nodes can understand the reason for initiating the traceability outside the system, and then the supervisory authority node is responsible for restoring the key and decrypting the traceability. Transaction records finally obtain the identities of relevant transaction participants through the identity verification server. But, only after a USOT is spent, the consortium chain can obtain its owner's identity signature through a transaction request from a public chain user. If a USOT has not been spent, its owner cannot be known. In order to increase the supervisable properties of the system, this research adds three parts of the supervision agency, identity authentication server, and encrypted storage to the Internet of Things system. When there is no need to initiate traceability, the supervisory agency only participates in the consensus process as a participant in the alliance chain, and only when it needs to

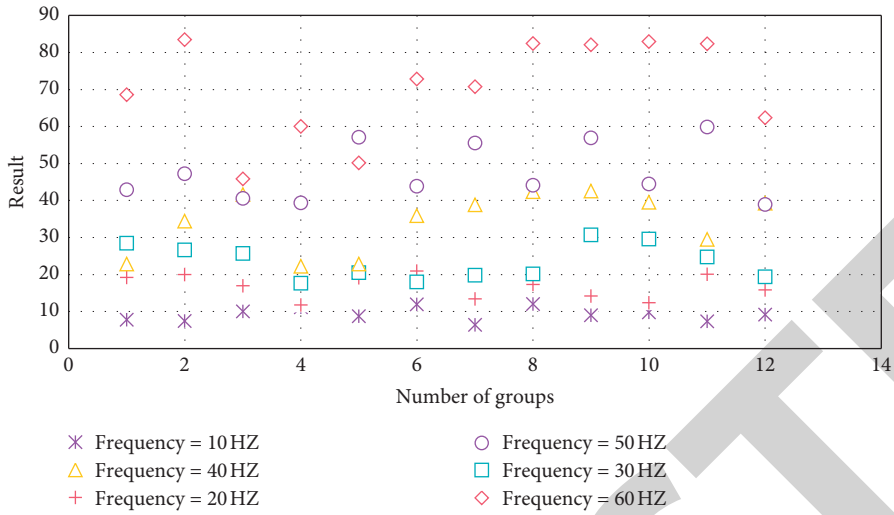

Figure 10: The original high-frequency coded signal collected by using an oscilloscope.

trace the transaction, can it act as a trusted secret shared share collector to decrypt data. The identity authentication server issues identity certificates to registered users, which can trace the transaction to a clear user and achieve thorough supervision. The addition of supervisory attributes reduces the degree of decentralization of the system, but it does not damage the Internet of Things from the user's perspective. The original intention of the design is that the members and data of the alliance chain and the public chain do not rely on centralized credit, and it can also achieve better protection for users. When a user loses an account or transaction certification document such as an identity certificate, he can protect his account through the identity authentication server and the system. Encrypted storage is to prevent consortium chain members from leaking transaction information after being attacked. The function of the regulatory agency has affected the decentralized structure, and it has also become a security weakness that the system may be attacked. The use of secret sharing to a certain extent prevents the possibility of stealing transaction data with the regulatory agency as the target, and only alliance chain members agree to restore only when the key is the supervisory authority which has the ability to decrypt data. The test results after changing the maximum number of learning times are shown in Table 8. The regulatory error is shown in Table 9.

4.4. Security Analysis. The issuance of legal digital currency requires the transformation of the payment system infrastructure. As a digital form of currency, legal digital currency needs to adopt extremely high technology in any link of circulation to reduce the degree of operational risk. Once the legal digital currency infrastructure is destroyed, it will cause the entire financial system to suffer losses. The system security results are shown in Figure 12. The analysis of legal digital currency has to deal with a large number of transactions, and the most mature distributed ledger technology cannot fully meet the requirements of the central bank's payment system. In its fiat digital currency project, the Bank of Canada uses distributed ledger technology (DLT) to build a payment system, but the performance of distributed ledger technology is not optimistic. According to the report, it is difficult to use distributed ledger technology for transaction systems to process a large amount of instantaneous transaction data. After the official issuance of legal digital currency, it faces far more requirements than Bitcoin in terms of importance and transaction scale. The payment infrastructure established by the central bank must meet the transaction needs of the society. The issuance of legal digital currency will have a profound impact on the payment system of the entire country. Therefore, the construction of the payment system must consider the requirements of scalability, compatibility, and transaction throughput. This article divides the attacks faced by the supervisable digital currency model into three types according to their sources: attacks from outside the system, attacks from alliance chain nodes, and attacks from public chain nodes. In terms of the most basic security of digital currency transactions, the system uses identity certificates and signatures to ensure that attackers cannot forge identities to steal other people's assets; transactions in the system are based on USOT and use a unique public key as an address. The corresponding private key can be unlocked for payment. The purpose of the attack from outside the system is to destroy the function of the system and make the digital currency system unable to operate normally. The target of the attack may be a node in the system or a communication network. Due to the distributed nature of the blockchain, attacking a node in the system will not affect the operation of the system, but when an attacker has the ability to attack multiple nodes, the alliance chain as the core of the system must ensure that the node that stops working cannot exceed 1/3 of the system. Since the public chain uses DPoS as a consensus mechanism, during the election cycle, those nodes that are made public due to the operation of the system are likely to become targets for system attackers. Therefore, in order to ensure that the system does not stop running, it is necessary to

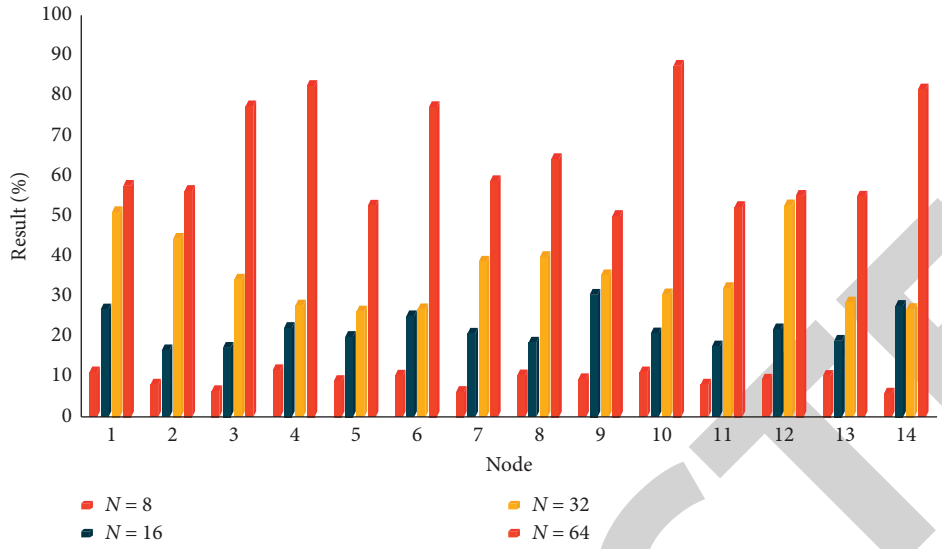

Figure 11: Functional analysis results.

Table 8: Test results after changing the maximum number of learning.

Maximum number of studies	Best accuracy rate (%)	Worst accuracy rate (%)	Average accuracy (%)
10000	66	56	60
20000	66	60	62

Table 9: Regulatory errors.

Target location	Right in front	Upper left	Top right	Right rear
Maximum positioning error of X-axis (cm)	1	1	1	1
Maximum positioning error of Y-axis (cm)	2	1	1	2

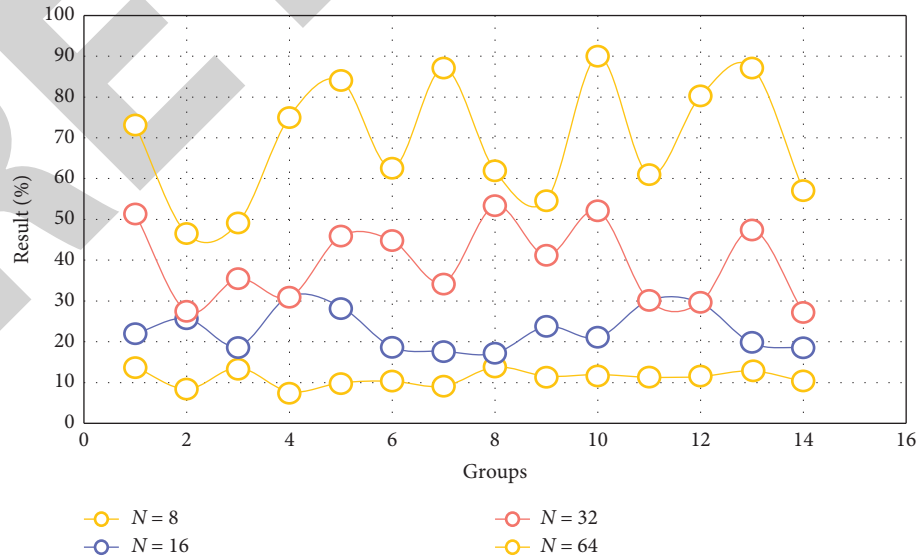

Figure 12: System security results.

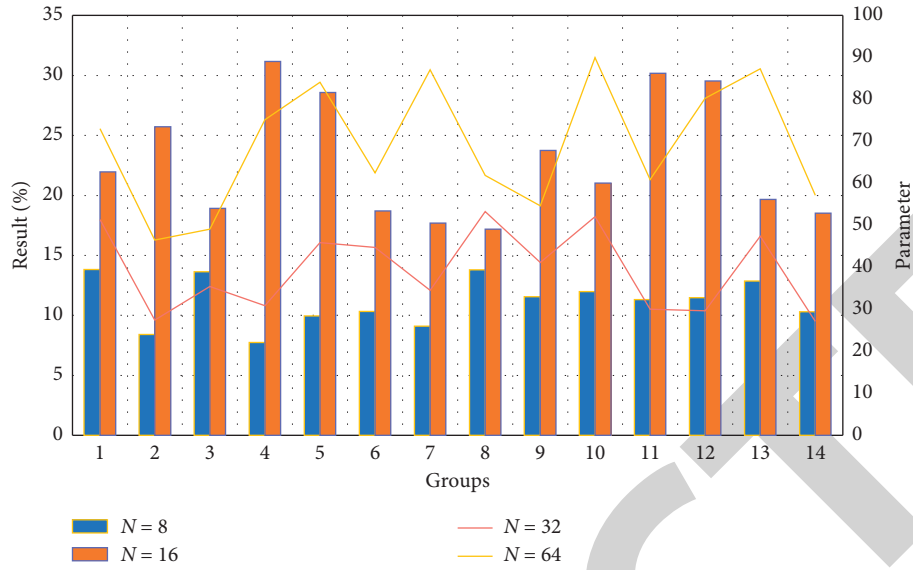

Figure 13: Efficiency analysis results.

ensure that the system attackers are all before destroying the current witness node, complete a new round of witness node voting. Attacks from within the system are generally through the creation of system inconsistencies such as the fork of the Internet of Things to achieve double-spending by tampering or canceling transaction records. The CPBFT consensus mechanism adopted by the alliance chain does not have the possibility of forks of the Internet of Things. When the number of colluding attackers does not exceed the threshold, it can prevent double-spending attacks. Although there may be forks in the public chain, only attackers account for more than 50% of the total number of nodes to ensure the success of the attack. The real-name registration mechanism in the background also reduces the possibility of launching and succeeding from inside the system. Digital currency can record and check transaction information and information of both parties, can accurately reflect the implementation of monetary policy, and can strengthen financial management. The transaction record of digital currency cannot be tampered with, can completely record the transactions of each participant, and can form a unified distributed ledger in the entire digital currency system. Through the review of transaction information and the supervision of digital currency circulation, the national regulatory agency can accurately grasp the monetary policy and credit policy in real time, and then scientifically and comprehensively calculate the policy implementation status, and adjust relevant policies in time according to changes in the situation; It can promote the publicity, openness, and integrity of digital currency transactions as a whole by establishing an overlying public credit system.

4.5. Efficiency Analysis. Intermediaries such as digital currency trading platforms or traditional financial institutions and certain nonfinancial industries which are likely to participate in the flow of digital currency transactions should keep records and report suspicious transactions. The specific methods include conducting due diligence on customer identity and storing customer identity information. The public key address, account, transaction nature, date, and amount involved in the transaction are helpful for monitoring transactions, recording suspicious transaction information, and combining the information on the blockchain ledger for more accurate recording. In order to prevent unqualified financial institutions from participating in the payment and settlement system, the access system sets specific conditions so that only payment and settlement participants who meet the corresponding conditions are allowed to be the counterparty of payment and settlement. The efficiency analysis result is shown in Figure 13. As the transparency and intensity of supervision have been greatly improved and the legal digital currency relies on advanced Internet technology, it can better identify the relevant conditions of financial institutions involved in payment and settlement and strengthen prudential supervision. The consensus mechanism used in the public chain part of the system is DPoS, and the consortium chain part uses CPBFT. Both consensus mechanisms are based on voting. The system state is determined according to the choice of the majority of nodes in the system, without the need for additional proof of work. The computational overhead of the system mainly occurs in the verification and encryption of transactions. In the process of verifying the block, each alliance chain node needs to encrypt and compare the transactions packaged into the block. This process uses a public key cryptographic algorithm, which has a high time complexity. Each node has basically the same demand for computing power, and there will be no system security problems and decentralized performance caused by the concentration of computing power. To achieve consistency within the alliance chain, nodes need to broadcast multiple times to achieve information interaction between the two. The communication complexity is $O(n)$, where n is the number of nodes. The system is

Table 10: The correlation coefficient matrix of the independent variables.

X variable Y variable	INF	LNC	LNY	R	P	V
INF	1.000	−0.129	−0.132	0.730	0.180	−0.470
LNC	−0.129	1.000	0.999	−0.473	−0.363	0.876
LNY	−0.132	0.999	1.000	−0.473	−0.352	0.878.
R	0.730	−0.473	−0.473	1.000	0.707	−0.670
P	0.180	−0.363	−0352	0.707	1.000	−0.287
V	0.470	0.876	0.878	−0.670	−0.287	1.000

Table 11: Time series unit root test results.

Variable	(c, t, n)	ADF inspection value	Critical value	Conclusion
$\ln y$	(0, 0, 0)	6.962	−1.966	Smooth
$\Delta \ln y$	$(c, 0, 0)$	−2.998	−1.956	Nonstationary
Inf	$(c, 0, 0)$	−1.627	−1.956	Nonstationary
Δinf	$(c, 0, 0)$	−3.809	−1.956	Smooth
p	$(c, 0, 0)$	−0.182	−1.956	Nonstationary
Δp	$(c, 0, 0)$	−3.898	−1.956	Smooth

designed so that each participant can control multiple nodes proportionally. The more the number of nodes, the stronger the antiattack ability of the system, but the communication overhead will also increase. The system maintains two blockchains at the same time. Compared with a single chain system, the communication between some nodes of different systems is increased. If the nodes of the alliance chain and the public chain communicate with each other, the complexity of the communication is $O(n, m)$, where n is the number of nodes in the alliance chain, mm is the number of nodes in the public chain, and m may be multiples of n, so the pair can be appropriately relaxed. The communication requirements between two blockchain nodes can reduce the communication complexity to $O(m)$. The supervisable digital currency system uses CPBFT and DPoS improved in this research. The characteristics of these two consensus mechanisms are that the block generation interval is short and the system transaction throughput is high, so there is no system bottleneck caused by increasing the system scale in the consensus mechanism. The correlation coefficient matrix of the independent variables is shown in Table 10. The unit root test results of the time series are shown in Table 11.

5. Conclusion

This research mainly discusses the intelligent digital currency and dynamic coding service system based on the Internet of Things technology. To a certain extent, digital currency can help save currency issuance and circulation costs, improve the effectiveness of monetary policy, accelerate the pace of development to a cashless society, and adopt effective methods for promotion and application. It is expected that digital currency will be widely used by all people, thereby contributing to building a robust and efficient new financial system. At the same time, the current status of the use of digital currencies at home and abroad is also analyzed. The digital currency market is frequently traded. According to the traditional trading market, digital currency is an active market, but the currency value stability of digital currency is poor.

This research is mainly based on the RDCAR algorithm to realize the traceability of the route discovery process of the wireless network initiated and completed within the alliance chain, and finally the results of the transaction traceability can be seen. The goal of retroactive transactions is generally a transfer-out transaction because the initiator of a complete transaction on the transfer-out exchange is the owner of the transfer-out transaction address, and the identity of the initiator can be queried. If no one spends it for a transfer-in transaction, it cannot get the owner of the transaction. When searching for a transaction, according to the query transaction serial number, it traverses the plaintext of transaction information saved in the block, finds the block containing the same serial number, decrypts the transaction, finally finds the transaction, and displays the complete record in the transaction.

When the intermediate node receives the RREQ message, first, to avoid loops, check whether the same RREQ message has been introduced. If it is received, discard it. Otherwise, buffer the message and append its own neighbor node list, corresponding to the signal-to-noise ratio of the channel link, and update RREQ message and broadcast it. The payment cipher is managed by the bank. When the user opens an account, the bank registers and sends it to the user, and the key is generated by the algorithm chip, and the public key is stored in the bank's back-end server. When the bill is delivered to the bank, the bank enters the various elements of the bill on the counter terminal and transmits it to the verification machine through the bank network for verification. If the verification is correct, it indicates that the bill is indeed issued by the customer, and the bill elements are correct, so you can make payment. The public chain and alliance chain node operation agreement maintains the operation of the Internet of Things system. The alliance chain node generates new blocks at a time interval of 30 s. When the node cannot complete the block generation within 30 s, it will rotate to the next node.

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 Social Science Foundation of Shaanxi Province of China under grant no. 2019D009 and the Shaanxi Province of China, Department of Education Project of Philosophy and Social Sciences Key Research Base under grant no. 19JZ052.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] X. Sun and N. Ansari, "EdgeIoT: mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.

[3] Y. Yang, L. Wu, G. Yin, H. Zhao, and L. Li, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[4] I. Yaqoob, E. Ahmed, I. A. T. Hashem et al., "Internet of things architecture: recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10–16, 2017.

[5] O. Bello and S. Zeadally, "Intelligent device-to-device communication in the internet of things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1172–1182, 2016.

[6] M. M. Zuberi and R. Levin, "Schumpeter's revenge: the gale of creative destruction: digital currencies and blockchain technology," *Banking & Financial Services Policy Report*, vol. 35, no. 5, pp. 1–8, 2016.

[7] M. I. Mehar, C. L. Shier, A. E. Giambattista et al., "Understanding a revolutionary and flawed grand experiment in blockchain," *Journal of Cases on Information Technology*, vol. 21, no. 1, pp. 19–32, 2019.

[8] D. S. Gong, "Financial transactions in ATM machines using speech signals," *International Journal of Engineering Research and Applications*, vol. 7, no. 1, pp. 25–28, 2017.

[9] F. Balo, "Internet of things: a survey," *International Journal of Applied Mathematics Electronics and Computers*, vol. 4, no. 2016, pp. 104–110, 2016.

[10] M. R. Palattella, M. Dohler, A. Grieco et al., "Internet of things in the 5G era: enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[11] A. V. Torsner and R. Buyya, "Fog computing: helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[12] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.

[13] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[14] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[15] M. Amadeo, J. C. Campolo, A. D. MolinaroCorujo, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the internet of things: challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, 2016.

[16] Y. Iera and J. Wen, "The IoT electric business model: using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[17] Z. Longchao, Y. X. Jianjun, and Y. Limei, "Research on congestion elimination method of circuit overload and transmission congestion in the internet of things," *Multimedia Tools and Applications*, vol. 76, no. 17, pp. 18047–18066, 2017.

[18] J. W. Xue, X. K. Xu, and F. Zhang, "Big data dynamic compressive sensing system architecture and optimization algorithm for internet of things," *Discrete and Continuous Dynamical Systems-Series S*, vol. 8, no. 6, pp. 1401–1414, 2017.

[19] H. S. Dhillon, H. Huang, and H. Viswanathan, "Wide-area wireless communication challenges for the internet of things," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 168–174, 2017.

[20] A. Ouaddah, A. A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[21] M. Nitti, G. V. Pilloni, and L. Atzori, "The virtual object as a major element of the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1228–1240, 2016.

[22] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 99, pp. 601–628, 2018.

[23] D. Zhang, L. T. Yang, M. Chen, S. Zhao, M. Guo, and Y. Zhang, "Real-time locating systems using active RFID for internet of things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1226–1235, 2016.

[24] K. Sood, Y. S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for internet-of-things: a review," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 453–463, 2016.

[25] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: the internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, 2016.

[26] J. Bernal Bernabe, A. F. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: multidimensional trust-aware access control system for the internet of Things," *Soft Computing*, vol. 20, no. 5, pp. 1763–1779, 2016.