Double Chain Blockchain Based on Improved Virginia Algorithm

Yibo Cao, Yuyang Cheng*, Chunyu Yang, Anqi Zhan, Chuxiao Xu
North China University of Technology, Beijing, Beijing, China
*Corresponding author’s e-mail: 18152010616@mail.nuct.edu.cn

Abstract: As more and more people accept Bitcoin, block chain technology has received extensive attention and research. Block chain is a decentralized open dean technology that combines data blocks with the chain structure in chronological order, and combines encryption, protocol mechanisms, and smart contracts. Block chain technology has the characteristics of decentralization, high security, difficult information tampering, traceability, and transparency. Therefore, more and more companies and institutions are focusing on block chain technology research. In the wide application of block chain technology, the current centralized transaction model of e-commerce has gradually exposed some problems, such as the obvious monopoly trend of third-party platforms caused by the excessive central power, the difficulty of cross-border transactions, and the insecurity of user privacy information. Difficulties in accountability for transaction disputes, numerous phishing websites, and proliferation of fakes. Moreover, the current block chain transactions lack legal supervision and protection, transaction efficiency is low, smart contract functions are limited and difficult to understand, and block chain is highly professional and difficult to be accepted by the general public. Based on this, this article proposes a product anti-counterfeiting traceability system using a dual-chain block chain based on an improved Virginia algorithm, analyzes the security of the traceability system, and verifies the feasibility of the system through simulation experiments. The further combination of chain block chain technology and product security field provides reference and reference.

1. Introduction

In 2008, Satoshi Nakamoto published the paper "Bitcoin: A Perto Peer Electronic Cash System", and the block chain technology, which has become the core technology of Bitcoin, has gradually entered people's attention. The development of the block chain can be compared with the development of the Internet itself [1]. In the future, finance-the Internet will be formed on the Internet, which is based on the block chain, and its precursor is Bitcoin, that is, folk traditional finance. Starting from the chain and industrial chain (near field communication network), the Bitcoin series started from the public chain (wide area network), all showing the same concept of digital assets, and finally converging with an intermediate balance [2]. In China, the research of block chain technology started relatively late, especially the development model was relatively fast in 2016. On January 20th, the People's Bank of China Digital Currency Seminar was held in Beijing. The meeting proposed to clarify the issuance of the central bank as soon as possible, and the digital currency plan to issue its own digital currency as quickly as possible [3]. In the same year, the China Block chain Research Association, the Basic Contract of the Dean of the China Distributed Master Account, the Financial Block chain Cooperation Association and the Central Bank Digital Currency Research Institute were established [4]. In this case, the number of Chinese block chain research literature also shows a rapid growth trend.
With the passage of time, blockchain technology continues to improve, and its application scenarios are no longer limited to cryptocurrencies, but are more widely used in fields such as electronic voting, medical care, charity, and distributed ledgers [5]. In the foreseeable future, blockchain technology will be more complete and its application scenarios will be more extensive. In many application scenarios of blockchain, product information traceability has gradually become an important application scenario [6]. For the lack of effective supervision in the blockchain, many experts and regulatory agencies have begun to pay attention to this issue. However, a unified supervision method has not been formed to deal with this problem. However, at present, the development time of the blockchain is relatively short, and there are many problems that are not perfect. For example, due to the original design purpose of the blockchain, the completed transactions and the included smart contracts are not subject to legal supervision[7].

The Virginia algorithm is one of the most common algorithms in the multi-table cipher classical encryption algorithm based on a single "Caesar cipher" extended [8]. The principle is to use a string combined with the Virginia phalanx. Each key character is used to encrypt ordinary text characters. The first key character can encrypt the first ordinary text character, and the second key is a way to encrypt the second ordinary text character. If the key text is all used, can be used again [9]. In order to better apply the blockchain in e-commerce activities, establish a dual-chain blockchain structure and use a professional supervision system to supervise blockchain transactions. It is proposed to establish a smart contract market on the chain of custody, strengthen the supervision and review of smart contracts, ensure the consistency of their actual functions and description functions, and facilitate users to choose appropriate smart contracts to use [10]. It also improved the Virginia algorithm of stream encryption technology, and used it in conjunction with the ECC Elliptic Curve Cryptograph to guarantee the intellectual property rights of smart contracts and other electronic commodities. Utilizing the low energy consumption characteristics of public key encryption, while increasing the security of the double-chain block chain, it hardly increases the efficiency burden.

2. Algorithm establishment

2.1 Improved Virginia algorithm
Stream cipher is widely used in network communication because it is a simple, fast, and low-cost encryption queue. Veneer cipher is one of the well-known stream ciphers. It encrypts messages by using a series of different Caesar ciphers based on the key letters. To facilitate calculations, the keys and the letters as in the plain text are converted into corresponding numbers 0-25. Therefore, the cipher text space is 26.

Use the key \( K \) to encrypt the plaintext:
\[
C_i = EK(P_i) = (P_i + K_i) \mod 26
\]
(1)

Use the key \( K \) to decrypt the cipher text:
\[
P_i = DK(C_i) = (C_i - K_i) \mod 26
\]
(2)

Where \( P = P_1P_2...P_n \) is plaintext, \( C = C_1C_2...C_n \) is ciphertext, and \( K = K_1K_2...K_n \).

The time complexity of this algorithm is \( O(1) \), and the space complexity is \( O(1) \).

By adding the number of characters, the frequency of a single letter can be reduced. The Virginia password library can be modified from the original 26 characters to an alpha-qwerty (ASCII code table) password, which consists of 92 characters, including numbers and others Common symbols that can be typed from the keyboard. The formula description of the extended version is similar to the original encryption method. It's just that it uses modulo92 instead of modulo26, and the cipher text \( C \) has also been expanded at the same time, making it more difficult to crack. The encryption and decryption process after expanding the ciphertext space becomes:

Encryption:
\[
EK(P_1P_2...P_m) = (P_1 + K_1, P_2 + K_2, ..., P_m + K_m)(\mod 92)
\]
(3)

Decrypt:
\[
DK(C_1C_2...C_m) = (C_1 - K_1, C_2 - K_2, ..., C_m - K_m)(\mod 92)
\]
(4)
First, a key with a short length is generated, and then a logical operation formula is calculated to generate a sufficiently long key. If the generated key is not repeated, or its length is longer than the plain text, it is difficult to find the regularity of the key, and it is difficult to obtain the key through frequency analysis to decrypt the plain text. Then the algorithm will be like an OTP password. It is also difficult to crack, so the plaintext will be safe.

2.2 ECC elliptic curve encryption algorithm
Cryptography is divided into symmetric and asymmetric encryption algorithms according to whether the keys $K_1$ and $K_2$ are the same.

When $K_1 \neq K_2$, it is an asymmetric encryption algorithm. ECC encryption, hashing and other algorithms are commonly used in block chain to encrypt information, and mathematical problems are used to increase the difficulty of attacks and protect plaintext information from being stolen.

The ECC elliptic curve equation is formula (5), which is a plane curve, generally represented by the letter E.

$$y^2 + m_1xy + m_3y = x^3 + m_2x^2 + m_4x + m_6 \quad (5)$$

The encryption process of the elliptic curve uses a special equation (6), which is a curve defined on a finite field $E_p$.

$$y^2 = x^3 + mx + n \mod p \quad (6)$$

Where $p$ is a prime number, $m$ and $n$ are non-negative integers, $m, n, x, y \in E_p$ and $m < p \& n < p$, satisfying formula (7):

$$4m^3 + 27n^2 \mod p \neq 0 \quad (7)$$

2.3 Advantages and disadvantages of the algorithm
Advantages: The key technology of selective encryption is to distinguish between meaningful and meaningless image regions. This is because a small error in a meaningful image area will bring about a huge change to the original image, and changing the meaningless area will not cause too many side effects. Therefore, only the meaningful image data needs to be encrypted, which can reduce the amount of calculation. Use two paths to encrypt separately, and then multiply the obtained results for diffusion. The first path uses the saw tooth linear filling curve containing the key $k$ and the pixel values after the POI selection to form a matrix. The second path uses nonlinear chaotic mapping to generate a theoretically undecipherable encrypted $K$ matrix. Multiplying the matrices obtained by the two paths is theoretically safer.

Disadvantages: The data to be transmitted is large, not only the cipher text, but also the position matrix of the point selected by the POI. The key $k$ generated by the first path of images of different sizes is limited. Therefore, the key of the first path is relatively weak, and it may be deciphered if the idea of divide and conquer is used for analysis. Although generating the encrypted $K$ matrix is complicated and difficult to decipher this path, it is clear that the only thing that really affects the encryption process is the encrypted $K$ matrix. What needs to be deciphered is only a matrix. As for how the matrix came from, you may not care about it.

3. Modeling method

3.1 Smart contract model
Smart contracts require a unified market-based management to formulate unified development and regulatory standards to improve security. It is necessary to increase legal supervision, and before the smart contract is formally put into use, its functions need to be verified in multiple rounds to reduce transaction risks. Supervise and manage this smart contract market by using the supervisory nodes in the double-chain block chain chain.

The smart contract owner A gets the sum value $V_m$ and generates a random number $P$ ($P \neq 0$), which is secret and can be discarded and cannot be disclosed. Then generate a random number $q$ ($q > 3$ and random numbers $P$ and $q$ are relatively prime, $q < \max(V_i)$) calculation:
\( E(V_m) = PV_m \mod q \) \hspace{1cm} (8)

Among them, \( V_m \) is the number to be verified, which is confidential. The random number \( P \) is also secret. The random number \( q \) and the calculation result \( E(V_m) \) are public. The smart contract owner sends the calculated value \( E(V_m) \) to the verification node.

The verification node generates a secret random number \( R \), which is calculated by node 1:

\( E(V_1) = RV_1 \mod q \) \hspace{1cm} (9)

Node 1 sends the calculation result to node 2. When the number of nodes \( i > 1 \), iterative calculations are performed in sequence:

\( E(V_i) = (E(V_{i-1}) + RV_i) \mod q \) \hspace{1cm} (10)

Because the calculation results are evenly distributed, the subsequent node \( V_i \) cannot know the specific value of the previous \( V_{i-1} \) through calculation. When the nth node is calculated, the result is obtained:

\( E(V_n) = (E(V_{n-1}) + RV_n) \mod q = (E(V_{n-2}) + RV_{n-1} + RV_n) \mod q = \ldots =
(\sum_{i=2}^{n} R) \mod q = RV_n \mod q \) \hspace{1cm} (11)

Smart contract owner calculation:

\( E(V_m) = PE(V_n) \mod q = PRV_m \mod q \) \hspace{1cm} (12)

Verification node calculation:

\( E(V_n) = RE(V_m) \mod q = PRV_m \mod q \) \hspace{1cm} (13)

Return to formula (8), regenerate random numbers and perform \( T \) times of verification. If the values of \( E(V_m) \) and \( E(V_n) \) are equal every time, it proves that the smart contract calculation result \( V_m \) is correct.

4. Evaluation results and research

It can be seen from Table 1 that the block chain is compared between the single-chain and the double-chain block chain. The use of Virginia algorithm in the double-chain block chain can protect the privacy of the node account and protect the account. Data will not be stolen or leaked, etc., causing losses to enterprises or individuals.

| structure               | characteristic   | Number of accounts owned by each node | Number of information exchanges | Transaction processing number (times/s) | Number of transaction requests (times/s) |
|-------------------------|------------------|-------------------------------------|---------------------------------|----------------------------------------|----------------------------------------|
| Single strand           | 200 nodes without privacy protection | 1000                               | \( 3.46 \times 10^8 \)            | 1160                                   | \( 1.16 \times 10^{10} \)               |
| Double-chain block chain| 30 nodes with privacy protection   | 50                                  | \( 7.76 \times 10^6 \)            | 111                                    | \( 5.79 \times 10^4 \)                 |

For nearly 300 years, the Veneer password was considered unbreakable, but in the end the password was successfully deciphered by analyzing the frequency of letters in the cipher text. Because the plaintext to be encrypted is much longer than the key, the key will eventually encrypt the same letters that were previously encrypted. This forms a repetitive pattern of letter combinations. If the letters in the cipher text are evenly distributed, the attack will be ineffective. This article uses \( (K1: \text{true}) \) as the key to encrypt an English article, and calculates the letter frequency of the obtained cipher text. Experimental results show that the improved encryption algorithm almost reaches the goal of even distribution of cipher text letters. The experimental data is shown in Figure 1.
Figure 1 shows that although the key length is only 4 letters, the letter frequency of the obtained cipher text is still almost evenly distributed. Compared with not using algorithmic encryption, the frequency of letters appearing is relatively even, which can ensure the protection of customers' personal private data and privacy protection of enterprises' private information in industries operating under dual-chain block chain technology.

Block chain can combine encryption algorithms and zero-knowledge proofs to ensure account privacy and security, allowing users to be free of nationality restrictions, and cross-border transactions are convenient, safe, and cost-effective. Although the current block chain technology is developing rapidly, but to truly apply it to e-commerce, which has a wide range of impacts, the characteristics of block chain without supervision and legal protection will facilitate criminals, not conducive to management, and not conducive to legality. Of consumers defend their rights.

It can be seen from Figure 2 that adopting the improved Virginia algorithm double-chain block chain structure and mutual supervision can simplify the application structure, and adopt different hardware facilities according to the requirements of the chain to reduce costs. The two chains can be operated in parallel, and the operation efficiency is greatly improved. It can not only maintain the advantages of the original definition of the block chain, but also improve transaction speed and scalability, reduce delays, and increase profit models, thereby attracting more users to participate in the block chain, increasing the scale of the distributed architecture, and further improve safety.
5. Conclusion
Cryptography is a key technology to protect transaction security and information privacy in online business transactions. This chapter first gives an overview of commonly used encryption algorithms, analyzes the advantages and disadvantages of different encryption algorithms, mainly introduces the stream encryption algorithm used in this article and the commonly used ECC elliptic curve encryption algorithm in the block chain, and explains the improvement of Virginia. The application of algorithms in double-chain block chain technology is still in the initial stage of exploration, and its applicable product types need to be further analyzed, and there are still some security problems in the integration with IoT technology. The next step will continue to refine the details of the combination of the two and improve the product traceability system.

References
[1] Boccardi V, Paolacci L, Remondini D, et al. Cognitive Decline and Alzheimer's Disease in Old Age: A Sex-Specific Cytokinome Signature[J]. Journal of Alzheimer's Disease, 2019, 72(3):911-918.
[2] Ebhota V C, Isabona J, Srivastava V M. Investigation and Comparison of Generalization Ability of Multi-Layer Perceptron and Radial Basis Function Artificial Neural Networks for Signal Power Loss Prediction[J]. International Journal on Communications Antenna and Propagation, 2019, 9(1):46-54.
[3] Yannibelli V, Pacini E, Monge D, et al. A Comparative Analysis of NSGA-II and NSGA-III for Autoscaling Parameter Sweep Experiments in the Cloud[J]. Scientific Programming, 2020, 2020(6):1-17.
[4] Feng L, Zhang H, Tsai W T, et al. System architecture for high-performance permissioned blockchains[J]. Frontiers of Computer ence, 2019, 13(006):1151-1165.
[5] Dai W. Platform modelling and scheduling game with multiple intelligent cloud-computing pools for big data[J]. Mathematical and Computer Modelling of Dynamical Systems, 2018, 24(5):506-552.
[6] J.H. Núez-Moreno, Walworth J, Pond A, et al. Effect of nitrogen rates on 'Western' pecan tree development[J]. Acta horticulturae, 2018, 10974(1217):103-110.
[7] Mohamed B, Noureddine A, Adnene C. Secured Cloud Computing for Medical Data Based on Watermarking and Encryption[J]. Iet Networks, 2018, 7(5):294-298.
[8] Brad, Reid. Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city[J]. Computing reviews, 2018, 59(3):186-186.
[9] Anderson M. Quantum cryptography needs a reboot: A failed security product could someday power large-scale quantum computing - [News][J]. IEEE Spectrum, 2019, 56(10):9-10.
[10] Bechoff A, Tomlins K I, Chijioke U, et al. Variability in traditional processing of gari: a major food security product from cassava[J]. Food Chain, 2019, 8(1):39-57.