Hash Algorithm Optimization for Long-span Digital Currency Transactions based on Multi-constraint Optimization

Jianqiang Li

South China Agricultural University, China

Keywords: block chain; satellite; hash algorithm; convex optimization.

Abstract: Block chain technology and satellite integration to achieve wide-area security transactions has become a hot topic in the field of information security. It will face two major problems: the real-time transmission of large-span digital currency and the credibility of digital currency transmission under complex interference. In order to solve the above problems, this paper proposes a multi-constrained optimization-based hashing algorithm for long-span digital currency transactions. By analyzing satellite communication means and one-way hashing operation, the relationship between time delays under long-span digital currency transmission is obtained. By optimizing the hashing operation of constraints, the algorithm is improved to a larger extent. The adaptive ability of bit error rate (BER) and the construction of digital token based on multi-constraint enhanced hash algorithm provide a reliable authentication benchmark for digital currency transactions, design a large-span digital currency transaction process, and effectively suppress the information leakage caused by interference in the transmission process. The simulation results show that the performance of the proposed algorithm is greatly improved in security and complexity.

1. Introduction

Digital currency, with block chain as its core, regards irreversible and unique information as the equivalent exchange of human society, which effectively realizes the measurement of "information" value in virtual space, and provides a benchmark for "information exchange" in the information space of the era of artificial intelligence [1].

Focusing on the need of deep Protection and convenient application of private information, the development of block chain technology effectively promotes the common development of technologies including virtual currency, network transaction, privacy protection, redundant backup, information assets, identity authentication and authorization, data encryption and decryption.

Block chain technology, as the "credit" certificate of the intelligent society, has attracted great attention and attention of the world's major powers. In February 2016, the U.S. House of Representatives held a symposium on "Beyond Bitcoin: Emerging Applications of Block Chain Technology", which fully affirmed that Block Chain Technology will bring about changes in American society. "Block Chain Belief" has risen to the national strategy of the United States. The U.S. General Administration and the Homeland Security Administration are taking Block Chain as a kind of National strategy. Examine ways to improve the efficiency of current government business. In February 2018, the EU launched a new mechanism, which will invest 340 million euros to promote the deep development of the new economy in Europe. 22 EU countries signed an agreement to establish the European Block Chain Alliance [2]. In April 2017, Japan implemented the digital monetary system security system led by the Capital Computing Act, incorporating block chains as foreign exchange into Japan's financial supervision system. At present, 2 million physical stores with nodes can use Bitcoin to settle accounts. In December 2016, the State Council issued the National Informatization Plan for the 13th Five-Year Plan, which encourages the advance layout of strategic frontier technologies such as block chains and gives full play to the leading advantages of the first mover [3].

According to a report released by Reportbuyer, the global market size of block chains will increase from 411.5 million US dollars in 2017 to 7683.7 million US dollars in 2022, representing a composite annual growth rate of 79.6% [4].

At present, with the development of globalization and universalization of block chain [5], it will face the following two problems:

1) Real-time problem of long-span transmission of digital currency: Economic globalization drives the globalization of transactions, and the distance of trading places will gradually expand from meter level to kilometer level. The transmission of information is limited by electromagnetic wave velocity, which cannot ensure the real-time security of transactions in long-span [6].

2) Trustworthiness of digital money transmission under complex interference: The increase of transmission distance means that the probability of information being attacked increases exponentially, and the wireless channel cannot ensure information security through relay [7], which will lead to serious information leakage.

In order to solve the above problems, this paper proposes a multi-constrained optimization-based hashing algorithm for long-span digital currency transactions. By analyzing satellite communication means and one-way hashing operation, the relationship between time delays under long-span digital currency transmission is obtained. By optimizing the hashing operation of constraints, the algorithm is improved to a larger extent. The adaptive ability of bit error rate (BER) and the construction of digital token based on multi-constraint enhanced hash algorithm provide a reliable authentication benchmark for digital currency transactions, design a large-span digital currency transaction process, and effectively suppress the information leakage caused by interference in the transmission process. The simulation results show that the performance of the proposed algorithm is greatly improved in security and complexity.

2. Basic Theory of Large-scale Digital Money Transmission

2.1 Long-span Information Transmission Method: Satellite Transmission

According to statistics, the global coverage of the ground network does not exceed 40% of the surface area. Therefore, using satellites with different orbits as relays can effectively expand the trading range of digital currency. Satellite network generally consists of three parts, namely earth station, satellite and terminal. Earth station is an important node supporting terminal access system and internet. Satellite will support remote connection between terminal and earth station, while terminal carries satellite network application function [8]. By associating different types of satellites with block chains, different features of digital money can be extended, including:

1) Expansion of trading scope: Satellite network is used as information transmission channel to transfer digital currency information from seller to buyer through satellite beam.

2) Enhancement of transaction security: Satellites can form independent networks and realize point-to-point transactions of digital currency without access to the Internet.

In order to achieve large-span digital currency transmission, satellite communication functions and block chain system architecture can be further integrated, as shown in Figure 1. The network elements that need to be improved include earth stations bEs fusing block chains and terminals that can receive and send satellite signals tEs.

Earth Station Fusing Block Chain bEs : The satellite is assumed to be a transparent forwarding node, that is, the satellite network is only used as the information transmission channel of digital currency. The security of digital currency will be ensured by the security of satellite network. The open links of satellite networks will lead to the leakage of digital currency transactions, and maintaining the security of the whole network will greatly reduce the benefits of satellite networks. Another scheme is to add block chain security protocols from earth stations and terminals, which will form a trusted security tunnel, so that decentralized digital currency transactions can also ensure the reliability and security of transactions through block chain security protocols.

Terminal for transmitting and receiving satellite signals tEs: different from the traditional digital money storage unit [9]. The terminal tEs will have antenna and radio frequency module directly connected to the satellite. Owners can access the digital currency through encryption into bEs. tEs stores the user's digital currency credentials and the user's key $cKey$ of communication and transmission. At this time, users can access the digital money service center for authentication and transaction. In the absence of access to the Internet, transactions between $cKey$ and $Coin$ can be made.

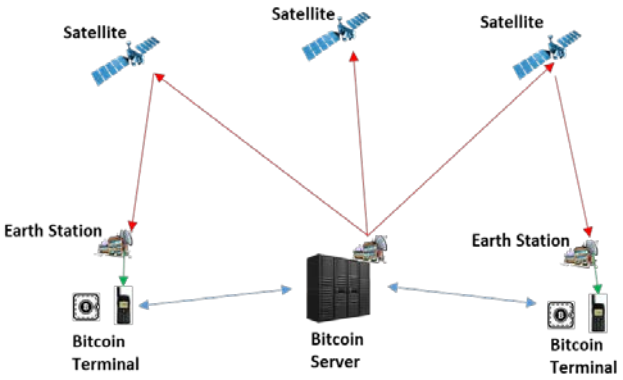

Figure 1. Satellite Network Architecture for Digital Money Transmission

2.2 Block Chain and Digital Money: One-way Hash Operation

The value of digital money lies in the cost of excavation and unforgeability. Therefore, it is necessary to ensure the security of the money source in the process of transmission and transaction, and to verify the value of digital currency quickly. Hash algorithm has the advantages of anti-collision, irreversibility of original image and problem-friendliness, which can ensure the security of digital currency transmission and transaction in the network.

Currently, the security algorithm of Bitcoin adopts SHA-256 algorithm, which produces 256 bits of verification information $Hash$ for the information of digital currency less than 264 bits in length. When a house buyer receives digital money, a pre-check information $Hash'$ can be obtained by using SHA-256 algorithm. At this time, if satisfied $Hash = Hash'$, it indicates that the digital currency has not been tampered with. The SHA-256 algorithm consists of five steps.

Step 1: Redundant bit filling. Since SHA-256 is a fixed-length output, it should be satisfied $n \equiv (448 \bmod 512)$. When the bit length is less than 264, it should be supplemented. If the bit length is more than 264, it should be segmented.

Step 2: Segmentation and merging of data bits. The currency data is grouped into 64 bits and merged into the redundant bit input matrix. From this we can get $X = [R_{(448)}, \mathrm{Coin}_{(64)}(i)]$.

Step 3: Initialize the cache. Multiple iterations can ensure the irreversibility of the check values. Therefore, a 256-bit cache is used to store the median and results of the hash function.

Step 4: Iterative operation. Six simple logic functions of AND, XOR and de-reciprocity are used and 64 steps of iteration are performed. The input of the iteration operation is the cache input in step 3, and the cache content is updated each time.

Step 5: Output results. The output of the last iteration is the output.

2.3 Problems in Long-span Digital Money Transmission: Packet Loss Rate

The security of Hash function lies in that the irreversible inference is ensured by the high and small entropy values with uniform distribution of variables. If the output of each bit is selected from a highly unpredictable (high and small entropy) distribution, it is impossible to find one in less than 2n time. From this, we can see that in the scheme of the earth station fused with block chains bEs, to make $Hash(k||x) = y$ the trusted safe tunnel will not be destroyed by the security of Hash function due to the length of time and the number of leaks [10].

From the above, if the quality of transmission channel of satellite network decreases, the error of check value will result in the failure of check value of digital currency, that is, there is no validity $Coin$, so that the mapping, within the valid statistical range, can be guaranteed.

$$Hash(k||x) = h' \tag{1}$$

3. Encryption and Strategy of Digital Money Transaction based on Multi-objective Constraint Control

3.1 Optimization of Hash Algorithms with Multi-objective Constraints

Formula (1) shows that the quality of transmission link decreases, resulting in a mismatch between the test value and the output value. It will be difficult for the recipient of digital currency to judge whether the information is forged or transmission error. Therefore, the optimization of this algorithm aims at overcoming transmission error to the greatest extent on the premise of ensuring secure transactions. Convex optimization is used to measure the safety and efficiency of multi-objective constrained optimization.

Assuming that the transmission of original data x and validation information h , and impulse response through satellite channel $h(t,f)$, the received information is as follows

$$y = x * h(t,f) + n \tag{2}$$

$$h' = h * h(t,f) + n \tag{3}$$

Among them, f is the main frequency of the transmission channel and n is the channel noise and t are time-varying. According to the hash algorithm SHA-256, the expected verification information can be further obtained as follows:

$$h = Hash(x) \tag{4}$$

By substituting the transmitted data into the SHA-256 algorithm, the information to be checked can be obtained as follows:

$$h'' = Hash(y) = Hash(x * h(t,f) + n) \tag{5}$$

The matrix of check error and transmission error is set up, which marks the Hamming distance $H(h',h'')$ between receiving check information h'' and the information to be checked h'' and the position of different digits $L(h',h'')$, and the sum of the Hamming distance $H(h,h'')L(h,h'')$ between expected check information h and the information to be checked h''.

In this case, the constraint function relationship can be obtained by taking security and efficiency as the input characteristics of convex optimization.

$$O = \alpha H(h',h'') + \beta H(h,h'') \tag{6}$$

The α and β is the optimal control coefficient. In this case, to ensure the minimum value of O, the time partial differential can be applied to Formula (6).

$$\frac{\sigma O}{\sigma t} = \alpha \frac{\sigma H(h',h'')}{\sigma t} + \beta \frac{\sigma H(h,h'')}{\sigma t} \tag{7}$$

In formula (6), when h' and h'' passes through the satellite channel, its statistical distribution obeys the rule of Gauss white noise, while the other parameters are stable, it also obeys the Gauss distribution. In this case, the probability density function should be satisfied.

$$p_O(f) = \alpha \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{(x-\mu_1)^2}{2{\sigma_1}^2}} + \beta \frac{1}{\sigma_2\sqrt{2\pi}} e^{-\frac{(x-\mu_2)^2}{2{\sigma_2}^2}} \tag{8}$$

Thus, the optimal O and value α and β can be obtained.

3.2 Unified Digital Token based on Enhanced Hash Algorithms

From the generation and transmission process of digital currency, we can know that the security of digital currency information needs to be ensured by the identity of the holder and the transmission key. Therefore, when dealing with digital currency based on satellite network, it is necessary to take into account the above two kinds of information at the same time to form a unified digital token for transaction and transmission security.

Assuming that the holder's identity is authenticated by the digital currency issuing center, it will hold the digital currency Coin , the holder's identity ID and the terminal MID . Trusted transmission secret keys $ekey$ exist in communication networks.

Combining the above hash algorithm, the transaction verification information can be obtained.

$$H_1 = Hash(f(\text{Coin}, \text{ID}, \text{MID}) \tag{9}$$

Similarly, trusted verification information for the transmission secret key can be obtained.

$$H_2 = Hash(f(ekey, \text{ID}, \text{MID}) \tag{10}$$

The final digital token H_1 and H_2 is obtained by substituting it into formula (6) and using the hash function again.

$$H = Hash(H_1, H_2, O) \tag{11}$$

Considering the characteristics of transaction and transmission H, the valid transaction of digital currency can be obtained accurately under $h' = h''$ the confidence range of channel mean and variance in the decoding process.

3.3 The Digital Money Transaction Process under Large Span

After designing hash algorithm and digital token, we can use satellite network to deal with digital currency. Its transaction process needs to interact according to the protocol exchange of each element in the transaction process. Its flow chart is shown in Figure 2, which is described as follows:

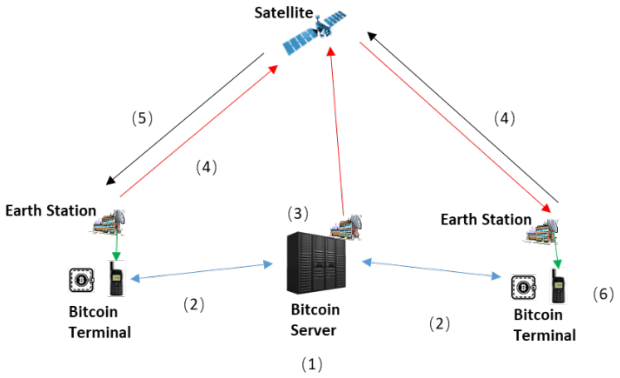

Figure 2. Large-span digital currency trading process

Step 1: The digital token and key of the digital currency are generated by the digital currency trading center, and transmitted to both sides of the transaction by means of networking or solidified chip.

Step 2: The terminal of both sides of the transaction receives the digital token and the transmission secret key, and stores them in the encryption unit of the terminal.

Step 3: The data transmission satellite network selected by the Digital Money Trading Center will send the verification information of the transmission key to the trading terminal through the satellite network.

Step 4: The transaction parties verify the scheduled transmission key and compare it with the key verification information from the satellite network to determine the security and reliability of the network.

Step 5: If the test is correct, the transaction seller encrypts the digital currency with the transmission key, and forms a verification information, which is transmitted to the purchase terminal through the satellite network.

Step 6: After the house buyer receives the information, the encrypted digital currency information is decoded by using the transmission key verification information, and the consistency of the digital currency information is further verified.

This completes the process of digital currency security transaction based on satellite network.

4. Simulation and Analysis

4.1 Construction of Simulation Environment

In order to verify the security and efficiency of the new algorithm, this paper will use the platform of MATLAB to simulate the system and environment, as shown in Figure 3.

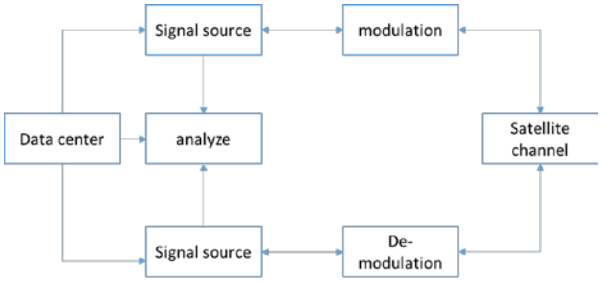

Figure 3. Composition of simulation system

It mainly includes four modules: source, channel, information center and verification analysis. The simulation configuration is set up in the experiment as shown in Table 1. The selected Hash algorithm is SHA-256 and the optimized SHA-256 algorithm in this paper.

Table 1. Configuration of simulation parameters

Simulation parameters	numerical values	simulation parameters	numerical values
Orbital altitude	35800km	error code range	0~256 bit
Information Bit Length	4096bit	Number of Satellite	1
Number of users	2	transactions	100

4.2 Effectiveness Analysis

This experimental group mainly verifies the validity of the validity of the validity of the validation algorithm. In the experiment, test data containing several sets of error information are set up, and different validation conditions are obtained after passing through different channels (with different bit error rates), and whether the results meet the expectations. The simulation results are shown in Figure 4.

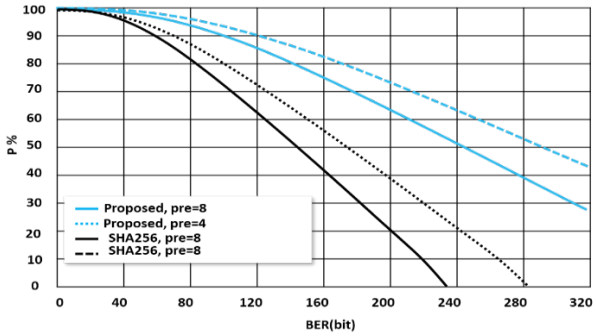

Figure 4. Transaction validity under different algorithms

It can be concluded from the graph that when the number of error test data is the same, the effectiveness of SHA-256 algorithm and the algorithm presented in this paper decreases gradually with the increase of the number of error codes. It shows that when satellite network is used for transmission, channel quality has great effect on transaction efficiency. However, when the bit error rate is 64 bits, the transaction efficiency decreases significantly, while the SHA-256 algorithm without improvement decreases significantly when the bit error rate is 32 bits. This is because the algorithm in this paper sets constraints on security and efficiency optimization, to ensure the security of the transaction while ensuring the security of transmission.

4.3 Complexity Analysis

This experimental group mainly analyses the length of control information data when the same validity is achieved, to verify the complexity of different algorithms. The simulation results are shown in Fig. 5.

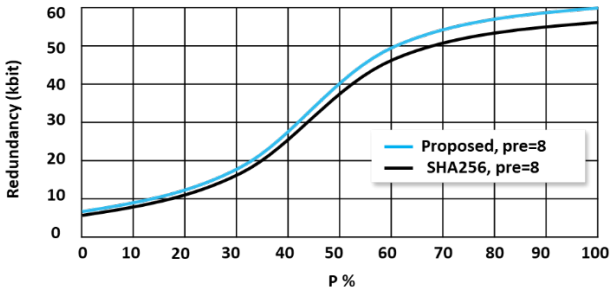

Figure 5. Complexity under different algorithms

It can be concluded from the graph that the complexity of SHA-256 algorithm and the algorithm in this paper increases gradually with the increase of validity. When the efficiency is less than 85%, the complexity of the proposed algorithm is comparable to that of the SHA-256 algorithm. When the efficiency increases to 85%, the complexity of this algorithm is only 2%~5% higher than that of SHA-256 algorithm. Combined with the validity analysis, the proposed algorithm can ensure that the security is unchanged in the case of high error rate, and the complexity of the algorithm is not significantly increased. Therefore, for large-scale digital money transmission, this algorithm can be used to improve security and efficiency.

5. Summary

This paper presents an optimization of hash algorithm for long-span digital currency transactions based on multi-constraint optimization. By optimizing the hash operation of constraints, the adaptability of the algorithm to larger bit error rate is improved, and a digital token based on multi-constraint enhanced hash algorithm is constructed to provide a reliable authentication benchmark for digital currency transactions. Considering the long-span digital currency trading process, it can effectively suppress the information leakage caused by interference in the transmission process. The simulation results show that the proposed algorithm can keep the security unchanged at high bit error rate, and the complexity of the algorithm is not significantly increased. Therefore, for large-scale digital money transmission, this algorithm can be used to improve security and efficiency.

References

[1] Garay, Juan, A. Kiayias, and N. Leonardos. "The Bitcoin Backbone Protocol: Analysis and Applications." (2015).

[2] Miers, Ian, et al. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin." IEEE Symposium on Security & Privacy (2013): 397-411.

[3] Narayanan, Arvind, and J. Clark. "Bitcoin's Academic Pedigree." Communications of the Acm 60.12 (2017):36-45.

[4] Faisal, Tooba, N. Courtois, and A. Serguieva. "The Evolution of Embedding Metadata in Blockchain Transactions." (2018).

[5] Listed, Nos. "A three-step plan for antibiotics. " Nature509.7502(2014):533-533.

[6] Lin, Wenliang, et al. "A new satellite communication bandwidth allocation combined services model and network performance optimization." International Journal of Satellite Communications & Networking 35.3(2017): 263-277.

[7] Sells, Ray, and M. Fennell. "Application of a robust control algorithm for satellite cyber-security and system resilience." (2017).

[8] Abdelsalam, Ahmed, et al. "Robust security framework for DVB-RCS satellite networks (RSSN)." International Journal of Satellite Communications & Networking 35.1 (2017):17-43.

[9] Liu, Jun, et al. "A Novel Cooperative Physical Layer Security Scheme for Satellite Downlinks." Chinese Journal of Electronics v.27.4 (2018):198-203.

[10] Vazquez-Castro, Maria Angeles, and M. Hayashi. "Information-theoretic Physical Layer Security for Satellite Channels." (2017).