**Internet of Things and Cloud Computing**
2020; 8(4): 52-59
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20200804.13
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

# Research on Block Chain Product Evaluation System

**Shao Yong, Yan Changshun***

Faculty of Information Technology, Beijing University of Technology, Beijing, China

**Email address:**
shaoyong@bjut.edu.cn (Shao Yong), yuewuxing@bjut.edu.cn (Yan Changshun)
*Corresponding author

**To cite this article:**
Shao Yong, Yan Changshun. Research on Block Chain Product Evaluation System. *Internet of Things and Cloud Computing*. Vol. 8, No. 4, 2020, pp. 52-59. doi: 10.11648/j.iotcc.20200804.13

**Received**: November 11, 2020; **Accepted**: December 16, 2020; **Published**: January 12, 2021

**Abstract:** Block chain technology has occupied a very important position in today's society. This emerging technology has been successfully explored and developed in many fields and scenarios. However, due to the fact that block chain technology is still in the exploratory stage, there is no rigid specification and index for block chain products, Integrating the research results of block chain technology architecture and security risk assessment, this paper designs a set of evaluation indicators for block chain products. The indicators are divided into six aspects, including P2P network technology evaluation index, distributed ledger technology evaluation index, asymmetric encryption technology evaluation index, smart contract evaluation index, consensus mechanism evaluation index and other security technologies Evaluation indicators, each big evaluation index is subdivided into several more in-depth evaluation indicators, and each of the specific analysis and explanation. Finally, based on the previous analysis and design work, a block chain product evaluation software is developed, which provides users with the function of comprehensive evaluation of block chain products. The design and software implementation of the block chain product evaluation system can effectively improve the efficiency in the development of block chain products and the quality of the products themselves, which is conducive to the further development of the block chain field.

**Keywords:** Block Chain, Architecture Analysis, Evaluation Indicators, Evaluation Software

## 1. Introduction

Block chain technology has attracted the attention of countries all over the world. The Australian stock exchange took the lead in introducing Block chain technology for stock trading, the Bank of Northern Ireland actively promoted the issuance of digital currency, and the White House of the United States spent a lot of money to obtain Block chain technology. In addition, the first Block chain technology stock was actively issued and made public by Nasdaq, which also served as a push Power, so that the Block chain technology in the attention, but also in the rapid development.

In the 13th five year national information plan released in 2016, the attention to Block chain technology is also clear at a glance. According to the statistics of the Ministry of industry and information technology of China in 2018, as of the end of March, there have been 456 enterprises related to Block chain technology in our country. It can be seen that the momentum of the Block chain industry is also booming in China, attracting the participation of numerous industry giants. For example, Alibaba, Jingdong, Baidu and so on, which we are familiar with, have begun to explore in the field of Block chain. Not only that, China's four major banks have also begun to dabble in the field of Block chain. The industry report of the Ministry of industry and information technology of China also shows that in the past three years, the investment in Block chain has increased significantly, which fully shows that the development of this emerging technology in China is progressing step by step.

With the passage of time, in the past few years, the application of Block chain technology has been more closely linked with the real economy. However, as an emerging technology that is still maturing, Block chain technology still belongs to the exploration stage. The Block chain products developed with it as the core may not have a thorough or skilled understanding of Block chain technology in many aspects There are a series of problems. The key to solve these problems is to develop a set of systematic evaluation indicators for the characteristics of Block chain products, and use these evaluation indicators to carry out a series of evaluation of Block chain products and detect whether their

characteristics meet the requirements.

In this paper, starting from the key to solve these problems, firstly, the research results of block chain technology architecture and security risk assessment are deeply studied. Block chain architecture mainly studies the design and practice of block chain product evaluation index [1]. Security analysis focuses on network security, password security and consensus mechanism security. Network security focuses on the common network attacks against blockchain products. The first is DDoS attack [2]. The second is witch attack [3]. The third is solar eclipse attack [4]. Password security studies common attack methods against block chain password security. The first is exhaustive attack [5]. The second is collision attack [6]. The third is quantum computing attack [7]. The fourth is digital certificate management [8]. The fifth is CA authentication [9]. Consensus mechanism security studies consensus algorithm. The use of consensus algorithm varies according to the type of chain, so the security involved is also different. POW consensus algorithm has the largest energy consumption, and its block time is very long, which is difficult to meet the demand. In terms of security, POW faces 51% computing power attack. POW also has the disadvantage of easy bifurcation and no finality [10]. POS consensus algorithm has low resource consumption and short block time, but it is easy to generate security vulnerabilities, bifurcation and no finality [11]. Dpos resource consumption is low and can reach consensus verification of second level, but it is still easy to generate vulnerabilities and has no finality [12]. Pert has the advantages of low energy consumption, high speed, low security, but no bifurcation [13]. In the consensus algorithm security problems, the following several attacks are studied. The first is 51% attack [14]. The second is selfish mining [15]. The third is the block chain bribery attack [16]. To deal with these attacks, we can reasonably define the security scope of formula algorithm, and the choice of consensus algorithm is closer to the business scenario of application, which makes the consensus algorithm multiple or switchable.

Based on these achievements, a set of systematic evaluation indicators for the characteristics of block chain products is designed, and an evaluation software is developed to support a series of automatic evaluation of block chain products.

# 2. Security Analysis based on Block Chain Technology Architecture

Block chain has such technical advantages as distributed storage, tamper-proof and anonymity, which provide a broad possibility for its development and application etc. However, block chain technology still needs further in-depth research, and there are more or less problems in its application in various fields. In terms of block chain technology, the most concern is its security risk. in addition, the decentralized and self-organized disruptive nature may also cause some technical security issues which cannot be ignored. The common security risks include:

### *2.1. Internet Security*

There are three kinds of common network attacks on block chain products, namely DDoS attack, witch attack and eclipse attack. Network attacks generally have the following characteristics: first, the method is simple and low-cost; second, the attack method is not easy to be detected; third, network attacks usually identify the defect that block nodes do not have enough verification when they join and exit. In view of the network attack, we generally adopt to strengthen the defense capability of DDoS, because DDoS is one of the most common network attack means. Besides, strengthening the access mechanism and verification mechanism of the node are also needed.

### *2.2. Password Security*

Common attacks on block chain password security are as follows: exhaustive attack, collision attack, quantum computing attack etc. To cope with these common password security problems, different storage methods are required to ensure the security of private keys, among which software storage is the most widely used. In addition, hardware storage and split storage are also used for solving this issue. PKI digital certificate management and the use of CA authentication can also help us encrypt data to a certain extent to ensure the confidentiality of transmission.

### *2.3. Ledger Data Security*

The data storage structure provides a favorable feature for block chain not to be tampered with, but also provides an opportunity for junk information to be linked up to a certain extent, that means some problems may occur in the protection of sensitive data. Due to the unhampered nature of block chain, it is difficult to modify and delete data on the block chain, which makes it extremely difficult to supervise harmful information. For some private data, as block chain is a kind of distributed ledger, several nodes are often required to participate in the process of storage and verification, so people's concerns about ledger privacy are inevitable. To deal with the problem of harmful information on the chain, we can add information review mechanism, whose function is to confirm the service subject of block chain and seek a balance with privacy protection. For privacy protection, we can store the private data in the outer chain and isolate the private data in the ledger. In addition, the encryption protection, desensitization processing and anonymous transaction of the data also provide favorable protection for privacy protection.

### *2.4. Consensus Mechanism Security*

As a distributed system, block chain has the characteristics of decentralization. In other words, in order to ensure the consistency of ledger data, it is necessary to establish a consensus protocol between nodes. The use of consensus algorithms varies depending on the type of chain and therefore the security involved. In terms of energy consumption, PoW consensus algorithm is the most time-consuming algorithm,

and its block time is very long, which is difficult to meet the demand. In terms of security, PoW is faced with 51% power attack. Besides, PoW also has the disadvantage of easy bifurcation and no finality. PoS consensus algorithm has low resource consumption and short block time, but it is easy to generate security holes and fork, even has no finality. DPoS has low resource consumption and can reach the second level of consensus verification, but it is still easy to generate holes and has no finality. PBFT has low energy consumption, slower speed, lower safety, but no bifurcation.

The security problems in the consensus algorithm generally come from the following attack methods: Double Spend attack, Majority attack, Selfish Mining and Bribery attack. In response to these attacks, we can reasonably define the security scope of the formula algorithm, and choose the consensus algorithm which is closer to the applied business scenario, so that the consensus algorithm can be switched.

### *2.5. Smart Contract Security*

The task of smart contract is to translate business logic into code, complete compilation and deployment, so that it can execute automatically under agreed conditions. Because digital assets are often the main operating object, smart contracts have high value as well as high risk. Usually, there are lots of problems on intelligent design and implementation of the contract. The main reason is that in the process of business logic code, the programmer has no definite standard and templates, so to write a perfect code almost impossible and there will be many places not rigorous in logic. In that case, many security issues in the business logic of smart contracts will be found. There are many types of smart contract security vulnerabilities, among which the most common is access control. In addition, although there are not many security holes found on virtual machines, they have a large impact and therefore need to be paid attention to.

To address these issues, the first step is to have the code for the smart contract fully verified by the auditor. In addition, the encryption of smart contracts should be done strictly and a set of standard templates for smart contracts should be developed to improve the efficiency of programmers in coding business logic. Finally, the iteration and formal verification of intelligent contracts need to be carried out continuously.

## 3. Design of Measurement Indicator for Block Chain Products

According to the above security risk analysis of block chain technical architecture, the measurement indicators of block chain products are designed as follows: Peer-to-Peer network technology measurement indicator, distributed ledger measurement indicator, Asymmetric Crystallographic technology measurement indicator, consensus mechanism measurement indicator, smart contract measurement indicator and other security technology measurement indicator. As shown in the table 1.

### *3.1. P2P Network Technology Measurement Indicator*

The measurement indicator of P2P network technology mainly includes P2P networking, transmission mechanism, nodes addition and deletion. The block chain products adopt P2P networking. In this process, packets of communication data between nodes should be intercepted and verified to confirm whether they conform to the point-to-point networking mode between the block chain nodes. Block chain products that adopt broadcast or multicast transmission mechanism for information and data transmission also need confirmation. The method is the same as above that communication packets between nodes are required to be intercepted. At the same time, the new nodes and the exiting nodes also need to verify according to the intercepted data packets, so as to confirm that their network can automatically recognize the joining and exiting of service nodes. In terms of implementation, some tools such as Wire shark can be used to intercept and parse communication packets.

***Table 1.*** *Measurement indicator of block chain products.*

| | | |
|---|---|---|
| the measurement indicators of block chain products | P2P network technology measurement indicator | Peer to Peer Networking<br>Transmission Mechanism<br>Node Additions and Deletions |
| | Distributed ledger measurement indicator | Header Hash<br>Hash Used<br>Times tamp<br>Merkel Root<br>distributed storage |
| | Asymmetric Cryptography technology measurement indicator | hash method<br>digital signature<br>Private Key Protection<br>Cryptography Algorithm |
| | consensus mechanism measurement indicator | Term inability<br>Consensus<br>Legality |
| | smart contract measurement indicator | Contract Language<br>Trigger Mode<br>Term-inability |
| | other security technology measurement indicator | Cross-chain Asset Trading<br>Cross-chain Smart Contracts |

### *3.2. Distributed Ledger Measurement Indicator*

Five indicators are proposed in the distributed ledger technical evaluation, which are header hash, hash used, time-stamp, Merkel root and distributed storage. These indicators require to ensure that they contain correct hash data, time-stamp data, and Merkel root data by detecting block chain structures. Main test content is to verify that whether the block structure stored on the node contains a header hash computed by a hash function, whether the block structure contains the header hash of the previous block, whether the block structure contains the correct time-stamp information and a hash computed Merkel root. For distributed storage, block data is required to be distributed stored on all nodes. The specific content of the test is to verify whether block data is distributed and stored on all nodes.

### *3.3. Asymmetric Cryptography Technology Measurement Indicator*

Asymmetric encryption means that different keys are used during encryption and decryption. In asymmetric encryption, each user is assigned a pair of keys, which we call public key and private key. The public key is used during encryption, while the private key is used during decryption. For openness, user needs to expose the public key to the entire network while keeping the private key private. Because the sharing of encryption keys in symmetric encryption leads to a series of security risks, public key encryption is a good solution to this problem.

The public key is open to the entire network, so that all users can access the public key of the individual user. After a series of operations (such as encrypting the data), the information is returned to the original user. When receiving the message, the user begins to decrypt the content, and during this retrieval, the private key is needed. This mechanism ensures that cipher-text is not accessible to any user other than the owner, thus providing a secure environment for the transmission of encrypted information and data over the network to the satisfaction of the receiver and sender.

Asymmetric cryptography provides a secure environment, mainly because it is vary difficult to derive or calculate the private key. But to get a user's private key is still not impossible.

A series of measurement indicators for asymmetric encryption technology are proposed as follows. The first is hash method which requires supporting hash algorithm to calculate block hash. The main content of this indicator is to verify whether hash algorithm can accomplish the calculation of data hash. The second is digital signature/verification, which requires the support of digital signature algorithm to complete the transaction data signature/verification operation. The third is the protection of private key, which is a very important indicator. It requires the block chain product to support the protection of private key of service node and client side. This indicator is to verify whether the private key is only allowed to be used by owners, and whether the storage and transmission have protection measures. The fourth is secret algorithm, which requires the product support for SM2 and SM3 secret algorithms and CA authentication with secret certificates. The evaluation content is to verify whether hash calculation can be performed with SM2 and whether digital signature/verification is performed with SM3. In addition, whether CA authentication is performed with secret certificates is also needed to be verified. While the last verification is an optional evaluation item.

### *3.4. Consensus Mechanism Measurement Indicator*

The evaluation of the consensus mechanism starts from three aspects. The first is to evaluate its term inability by verifying whether the consistent results of the consensus process at different nodes can be completed in a limited time and whether the block chain products support the term-inability in the consensus process. The second is the ability of consensus. That means the product should be verified whether the consensus process can output the same results when correct information is entered at different nodes. Finally, legitimacy is determined by verifying whether the decision result of consensus process at different nodes is the proposal put forward by other nodes.

### *3.5. Smart Contract Measurement Indicator*

The evaluation of smart contract starts from three aspects. The contract language needs to be evaluated by verifying the type of programming language supported by smart contract, check whether can the contract correctly operate and meet the needs of users to confirm and whether it can correctly support one or more contract languages. The second is the trigger mode. By verifying the penalty mode supported by the smart contract to measure whether the transaction or condition can run correctly after triggering and meet the needs of users, then it can confirm whether the transaction or condition can run. Finally, it is term inability, which is indicated to support the termination of the contract within limited time, limited steps and limited cost. This evaluation indicator is to verify that the intelligent contract supports the termination mode, and whether the contract can be terminated within limited time, limited steps and limited cost after the contract runs.

Truffle can be used for evaluating smart contracts. Truffle is easy to use. The test automation framework it provides is a typical framework. The framework provides two approaches: one is a JavaScript authoring mode that allows the contract to be manipulated and executed from the outside, and the other one uses solidity programming language which is not very common in use, so there will be no details here. Simply put, it is an advanced external execution contract, which is suitable for the BTTM scenario. Using Truffle means use the clean room environment which is provided for users to run a script that needed to test. When Truffle works, it uses the advanced snapshot feature which can ensure the scripts are independent of each other, that is, non-shared. When running with other Reuther clients, Truffle will redeploy when the script starts to be tested, thus it ensures that the user has a contract to test.

### *3.6. Other Security Technology Measurement Indicator*

This indicator covers two parts. One is cross-chain asset transaction. It can confirm whether the product supports the cross-chain roll-in and roll-out operation of digital assets by verifying whether it supports the cross-chain roll-in and roll-out operation of digital assets and completing the cross-chain asset transfer correctly. The second is the cross-chain smart contract. It verify whether a product support publishing, triggering, running and destroying operation of cross-chain contract, and whether can it correctly completing the relevant operation of cross-chain contract.

## 4. Development of Block Chain Product Evaluation Software

### *4.1. Requirement Analysis*

This software provide the function of evaluating block chain products. It conduct comprehensive analysis and calculation according to the results of each evaluation indicator provided by users, then give the corresponding final evaluation results. The following requirement analysis will be divided into two parts, functional requirements and non-functional requirements.

(1) Functional Requirement

The block chain product evaluation software has three main functional modules, and the functional requirements are as follows:

Interactive module: the task of this module is to complete the submission of user information. The user inputs the data according to the interface, including the name of the block chain product to be evaluated and the information of each evaluation indicator. In addition, after the data processing module stores and analyzes the collected data, the evaluation result will be output and displayed to the user which means a complete evaluation is completed.

Data processing module: the information input by users is stored in the database, and the evaluation results provided for each measurement indicator are calculated according to the established algorithm. The software evaluates the evaluation results by means of score accumulation and finally gets a specific value to judge whether the evaluation results are qualified.

Management module: the administrator can delete the data by logging in the background of the evaluation software.

(2) Nonfunctional Requirements

Non-functional requirements are mainly described from the aspects of performance and reliability

Performance Requirements: in terms of data processing, the collected data should be analyzed and calculated by certain algorithms. Therefore, the best algorithm as far as possible will be selected in the code design, so as to get the correct evaluation results and feedback to users in the shortest time.

Reliability Requirements: in terms of reliability, the software requires timely feedback after receiving user messages, and ensures that the platform can operate effectively on the hardware with high compression resistance.

### *4.2. System Design*

System design includes function module design and database design.

(1) Function Module Design

According to the demand analysis, the module function diagram can be summarized as shown in figure 1.

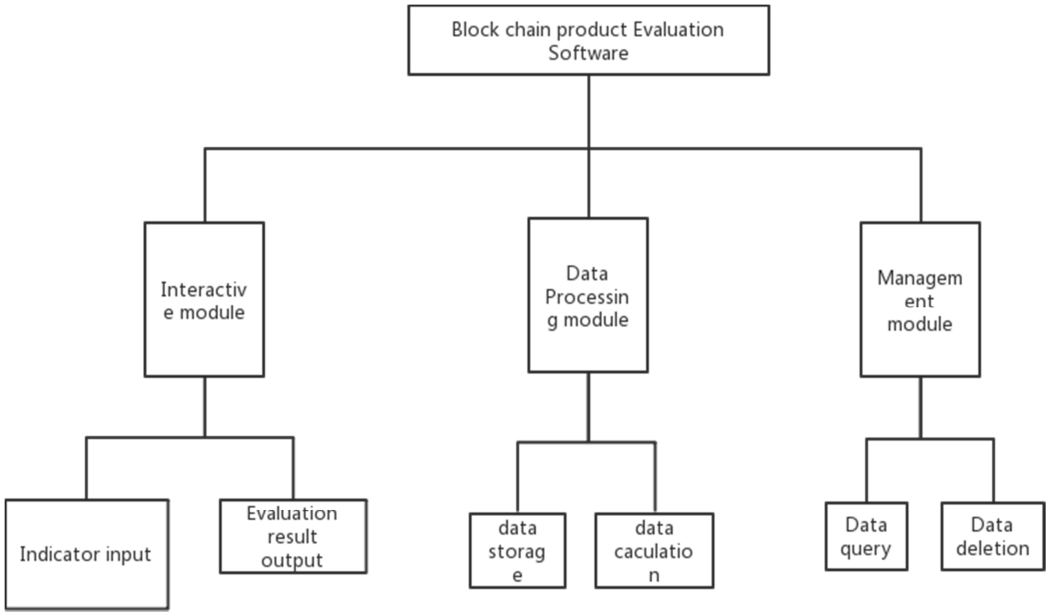


***Figure 1.*** *Function module diagram.*

Interaction module's task is to enable users to input the measurement data and enables the background to output the result to the user. First, the user enters the name of the block chain product and the result of each evaluation index

according to the content prompted on the interface. Secondly, the system collects these information into the background and feeds back the test results to the user after a series of operations, that is, displays them on the interface. Interactive module is the main module of the whole software, which will conduct a comprehensive evaluation on the quality of block chain products according to the results of a series of evaluation indicators input by users and the evaluation model that has been designed.

Data processing module includes data collection and calculation. The software will collect and store the data submitted by users into the database. Meanwhile, the test results of these measurement indicators will be calculated in the background according to the specified algorithm to get the final test results. Data processing module will collect and store the data submitted by users in the database.

Management module is mainly used for the administrator of the system background data management. The administrator needs to log in to enter the administrator management interface, where the stored data can be browsed and deleted. To ensure the security of the data, the user is not entitled to enter the management interface.

(2) Database Design

Conceptual model design: The e-r diagram of the block chain product evaluation software is shown in figure 2.

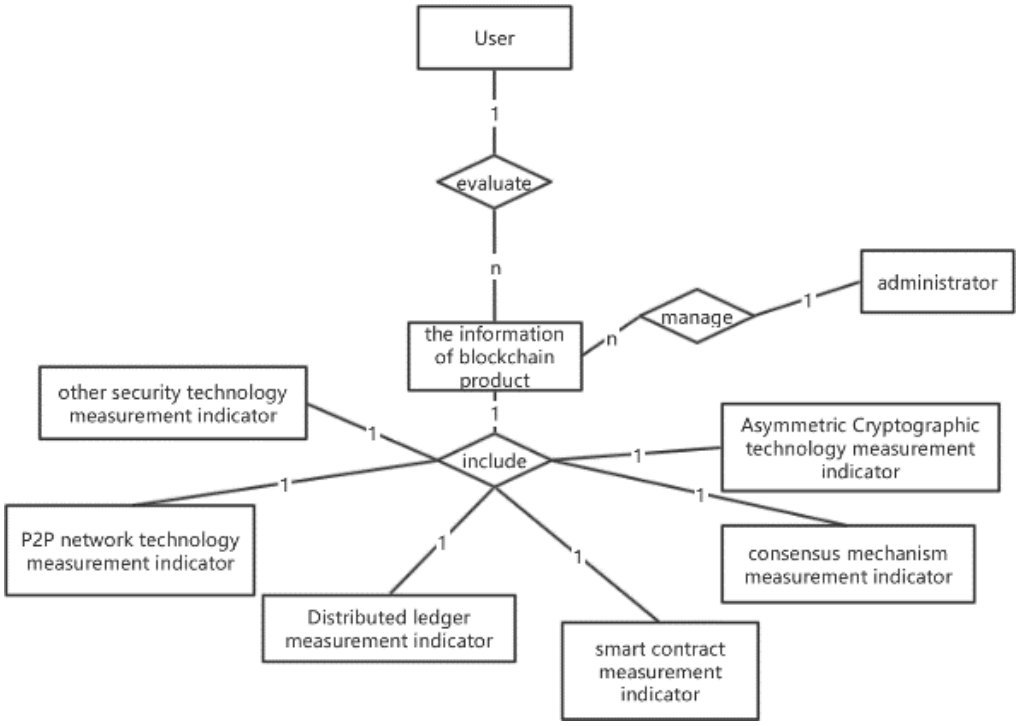


***Figure 2.*** *E-R diagram design.*

Logic design:

User information table design:(user_id, user_pw, test_id);

Block chain product information table design:(test_id, name, result, result_1, result_2, result_3, result_4, result_5, result_6);

Administrator information table design:(admin_id, admin_pw);

The design of P2P network technology measurement table:(test_id, result_1, indicator_1, indicator_2, indicator_3);

The design of distributed ledger measurement table:(test_id, result_2, indicator_4, indicator_5, indicator_6, indicator_7, indicator_8);

The design of asymmetric encryption technology measurement table:(test_id, result_3, indicator_9, indicator_10, indicator_11, indicator_12);

The design of consensus mechanism measurement table:(test_id, result_4, indicator_13, indicator_14, indicator_15);

The design of smart contract measurement table:(test_id, result_5, indicator_16, indicator_17, indicator_18);

The design of other security technologies measurement table: test_id, result_6, indicator_19, indicator_20

### *4.3. Display of Software Core Module*

The main function of the block chain software evaluation software is to conduct a comprehensive evaluation of a block chain product according to various evaluation indexes provided by users, and to give a reasonable evaluation result according to the designed evaluation model. On this basis, you can also provide users with some considerations and risk analysis. The administrator is responsible for browsing and modifying background data. The core software modules are shown below.

The measurement interface: Users input relevant block chain product information according to the prompts, collect each piece of information of the block chain product in turn, and give a comprehensive evaluation of the product according to the evaluation results. The demonstration is shown in figure 3 and figure 4.

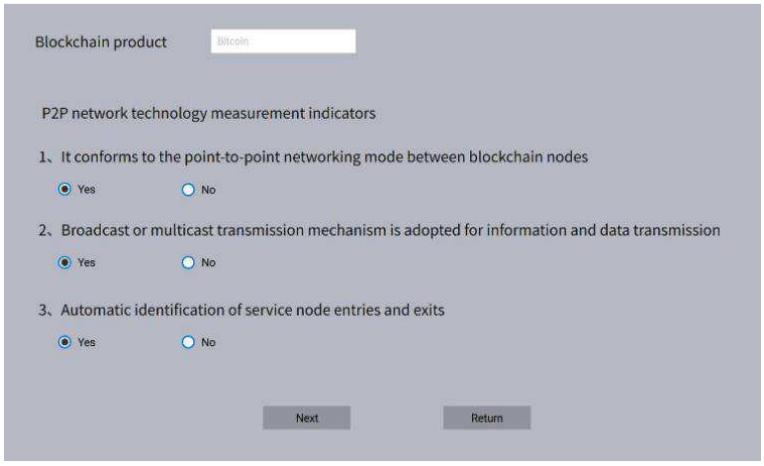


***Figure 3.*** *P2P network technology evaluation index.*


***Figure 4.*** *Other security technology evaluation indicators.*

The background implementation: The administrator enters the system background through the authentication, may view the data, and carries on the deletion to these data. As shown in figure 5.


***Figure 5.*** *The background implementation.*

# 5. Conclusion

Based on the results of block chain technical architecture analysis and security risk assessment, a set of evaluation indicators for block chain products was designed. Finally, based on the previous analysis and design, a block chain product evaluation software was developed, which provided users with the function of comprehensive evaluation of block chain products.

The user inputs the information of the software to be evaluated through the main interface, including its name and the evaluation results of various evaluation indicators, such as whether the software conforms to the point-to-point networking mode between block chain nodes, and gives two options: Yes or no. after collecting all the data input by the user, it is stored in the database, and then, according to the test designed in the background, the software can be used to evaluate the software The evaluation model evaluates the six modules of the block chain product respectively, and then gives the final evaluation score and suggestions based on the evaluation results of sub items, and finally feeds back these information to users. The administrator can enter the background of the software system after the identity authentication, access the database, and can maintain and delete the data in the database under certain circumstances.

The evaluation model given by this software is not an absolute evaluation model, but a specific evaluation model designed for individuals' understanding of block chain technology.

Finally, it needs to be pointed out that the research on the evaluation indicators of block chain products is a long-term, profound and lasting work. Through this attempt, the purpose is to have a deep understanding of blockchain technology and its products, and hope that a series of block chain product evaluation indicators can be put forward when others or other institutions study this aspect help.

# Acknowledgements

My thesis would like to thank the Beijing software product quality inspection center and Beijing Key Laboratory of testing technology for their help. They have given us a lot of financial support through the new generation of information testing technology and research projects (40025001201838). They also provide an experimental and testing environment for our research process. At the same time, I would like to thank the authors of the references and relevant researchers, whose research has provided me with important reference and help, and provided me with a good reference completing my paper.

# References

[1] Lei-peng Xiang, Design and Practice of Blockchain System Testing. Modern computer, Vol 5, 2018, pp. 24-26.

[2] Ying-xuan Zheng, Construction of campus network security model for NS2 network to resist DDoS attack. Network Security Technology & Application, Vol 10, 2019, pp. 98-99.

[3] Xiang-hua Wang, Xin Song, Witch attack detection method based on node location message verification in WSN. Computer Applications and Software, Vol 35, 2018, pp. 321-326.

[4] Liang Zhang, Bai-xiang Liu, Ru-Yi Zhang, Bin-xin Jiang, Yi-Jiang Liu, Overview of Blockchain Technology. Computer Engineering, Vol 45, 2019, pp. 1-12.

[5] Zhe LI, Yi-liang Han, Yu LI, A Key Exchange Cryptosystem Based on Polar Codes. Netinfo Security, Vol 19, 2019, pp. 84-90.

[6] Dan-qing Duan, Hong-ru Wei, Collision Attack on MIBS Algorithm. Computer science, Vol 45, 2018, pp. 222-225.

[7] Wei-qing You, Xiao-ming Chen, Jian Qi, Research on a Kind of Anti quantum Computing Public Key Cryptosystem. Netinfo Security, Vol 17, 2017, pp. 53-60.

[8] Yu Wang, Ming Zhu, Xia Yan, Application Research of Asymmetric Encryption Algorithm in Identity Authentication. Computer Technology and Development, Vol 30, 2020, pp. 94-98.

[9] Ke-wei Hou, Design of electronic secret key identity remote automatic verification system in heterogeneous environment. Automation & Instrumentation, Vol 2, 2020, pp. 85-88.

[10] Chun-mei Guo, Bao-ping Zhu, An Improved Blockchain Consensus Algorithm. Computer and Digital Engineering, Vol 48, 2020, pp. 1290-1293.

[11] Meng-yu Wu, Guo-sheng Zhu, Shan-chao Wu, Improved consensus mechanism of blockchain based on proof-of-work and proof-of-stake. Journal of Computer Applications, Vol 40, 2020, pp. 2274-2278.

[12] Ying Gao, Xue-cheng Tan, Improvement of DPOS consensus mechanism. Application Research of Computers, Vol 37, 2018, pp. 3086-3090.

[13] Ying-xu Lai, Zun-xu Bo, Research on sybil attack in defense blockchain based on improved PBFT algorithm. Journal on Communications, Vol 41, 2020, pp. 104-117.

[14] Lei Wang, Nan Ren, Baozhen Li, Research on evolutionary game and prevention and control strategy of block-chain 51%double spendattack. Computer Engineering and Applications, Vol 10, 2019, pp. 1-9.

[15] Jian Han, Jing Zou, Han Jiang, Qiu-liang Xu, Research on Mining Attacks in Bitcoin. Journal of Cryptologic Research, Vol 5, 2018, pp. 470-483.

[16] Wei-dong Fang, Wu-xiong Zhang, Tao Pan, Wei chen, Yang Yang, Cyber Security in Blockchain. Threats and Countermeasures, Vol 3, 2018, pp. 87-104.