International Journal of Intelligent Information Systems
2021; 10(5): 98-103
http://www.sciencepublishinggroup.com/j/ijiis
doi: 10.11648/j.ijiis.20211005.12
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Construction of Blockchain Product Technology Evaluation Index System

Yan Changshun, Shao Yong*

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

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

To cite this article:
Yan Changshun, Shao Yong. Construction of Blockchain Product Technology Evaluation Index System. *International Journal of Intelligent Information Systems*. Vol. 10, No. 5, 2021, pp. 98-103. doi: 10.11648/j.ijiis.20211005.12

Received: October 18, 2021; **Accepted**: November 9, 2021; **Published**: November 12, 2021

Abstract: Blockchain products are more and more widely used. How to reasonably evaluate blockchain products has become a hot issue. The main work of this paper is to establish a set of general evaluation indicators for blockchain products, and analyze the needs of future software systems. Firstly, the paper analyzes the common five-tier architecture adopted by the current blockchain system, namely data layer, network layer, consensus layer, smart contract layer and application layer, and expounds the hierarchical characteristics and technical contents of each layer in detail; Then on this basis, a set of general evaluation indicators is proposed for the current common blockchain products, in which the evaluation indicators can be divided into six items: distributed ledger evaluation indicators, public key password evaluation indicators, point-to-point network technology evaluation indicators, consensus mechanism evaluation indicators, intelligent contract mechanism evaluation indicators and upper layer application evaluation indicators. The establishment of indicators can comprehensively evaluate the availability, security and system performance of blockchain products. Finally, based on the evaluation index, the functional and non functional analysis of the blockchain product evaluation system is carried out, which lays a good foundation for the realization of software in the future. The design of evaluation indicators and the functional analysis of the evaluation system will promote the standardization of blockchain products.

Keywords: Blockchain, Evaluation Index, Requirement Analysis

1. Introduction

After Nakamoto put forward the concept of bitcoin system in 2008, the upsurge of virtual currency lasted for a long time. This currency is different from the previous paper currency or electronic currency. It has no currency issuer, and the transaction does not need to go through any third party. The transaction between payer and payee can even be carried out safely under complete anonymity, These characteristics make virtual currency popular. Bitcoin and other virtual currencies are also regarded as the 1.0 era of blockchain technology [1]. But at the same time, some people have also found the underlying technology of virtual currency blockchain, whose value and application scenarios are far more than virtual currency [2]. As a decentralized and distrusted distributed electronic accounting system, blockchain can be applied to more fields. Finally, at the end of 2013, Ethereum with Turing complete attribute was born. On the basis of traditional blockchain, he added programmable scripts, that is, smart contracts [3]. These smart contracts can be run under Ethereum virtual machine, which makes it possible to run programs under blockchain technology, which is also regarded as the arrival of blockchain 2.0 era [4]. The emergence of Ethereum has greatly expanded the usable scope of blockchain, so that its use is not only limited to the field of virtual currency and finance, but also can be used in education, medical product supply and other aspects. In the following period of time, blockchain technology has developed rapidly [5, 6]. Various countries, regions and enterprises have invested a lot of manpower and funds to carry out relevant research on blockchain, and various related products based on blockchain have been born one after another. However, due to the large number of relevant technical elements contained in the blockchain, such as distributed storage, consensus mechanism, encryption algorithm, etc., various blockchain systems adopt different consensus mechanisms, encryption algorithms,

networking communication methods, etc [7].

At present, the research on blockchain mainly focuses on two aspects [8]. The first is the further improvement of virtual currencies such as bitcoin. Although bitcoin system was already a very perfect virtual currency system at the time it was proposed, with the passage of time, people have found that bitcoin system also has many defects [9]. For example, it adopts POW and workload proof algorithm, Therefore, there is a waste of resources and computing power [10]. The algorithm also reduces the writing speed of bitcoin blockchain, so that a block can be written to the blockchain every 10 minutes [11]. Even if a transaction needs to wait 10 minutes to be verified. Moreover, due to the need to ensure security and decentralization, the transaction throughput of bitcoin system has decreased, and the average number of transactions can only reach 7 per second, which also limits the development of bitcoin system [12]. Therefore, some changed tokens have been proposed one after another, such as Wright coin, whose block generation speed is four times that of bitcoin, and Monroe coin, which adopts the way of returning signature, so as to hide the sender of transaction and improve the security of the system. These are all improvements made for the shortcomings of bitcoin. On the other hand, the research mainly focuses on the infrastructure of the blockchain. So far, the greatest achievement is the birth of Ethereum [13]. Its emergence makes it possible to run complex programs on the blockchain system and greatly expands the usable scope of the blockchain. The change of Ethereum mainly puts forward the concept of smart contract. In other aspects, such as corporate mechanism, people have noticed the shortcomings of pow algorithm, and put forward improved algorithm, proof of equity, POS algorithm, and dpos algorithm. Both algorithms reduce the consumption and waste of resources and improve the operation efficiency of the system. In addition, the blockchain system has been more clearly divided in terms of permissions [14]. Any node such as bitcoin Ethereum can join. In addition, the systems that disclose all data to all nodes are included in the common chain. In addition to the public chain, there are also alliance chains and private chains. Compared with the common chain, they improve the permission level [15]. Alliance stores usually need permission to join, while private chains are only used in a small range. These basic studies expand the availability of blockchains, At the same time, it improves the operation efficiency of the blockchain system.

In the face of such a large number of blockchain products and complex technical elements, there is no set of mature evaluation standards to evaluate blockchain products on the market. This paper discusses and studies based on this background, hoping to put forward a set of general standards for the evaluation of blockchain products.

2. Design of Evaluation Index for Blockchain Products

Here, a set of evaluation indicators for blockchain products is proposed, including six evaluation directions: distributed ledger evaluation indicators, public key cryptography evaluation indicators, point-to-point network technology evaluation indicators, consensus mechanism evaluation indicators, smart contract mechanism evaluation indicators and upper layer application evaluation indicators. For each evaluation direction, several specific evaluation indexes are proposed to evaluate the direction.

2.1. Distributed Ledger Evaluation Index

Distributed ledger can be said to be a blockchain in a narrow sense or the underlying structure part of the whole blockchain system. Therefore, the evaluation index design of distributed ledger is mainly considered from the perspective of structure. A complete block includes block header and block body, in which the block header contains all important information of the block, including, The hash value and hash that can connect the previous block with the block can be used to calculate and generate the header hash of the Merkel number, the timestamp used to determine the generation sequence of the block, and the Merkel root of the header node that records the Merkel number in the block body. The existence of these four parts enables the blockchain to form and complete its most basic functions, The integrity of these four parts is tested to check whether the blockchain product has the most basic functions. In addition, different distributed ledgers have different openness. For example, public chains such as bitcoin Ethereum have a high degree of openness, while some private chains have a low degree of openness, Therefore, the openness test of the distributed ledger is also included as an indicator, so that the characteristics of the blockchain product can be better reflected. Therefore, there are five main evaluation indicators of the distributed ledger, namely header hash, husband hash, Merkel root, timestamp and openness. The evaluation indicators of distributed ledger are shown in Table 1.

Table 1. *Distributed ledger evaluation index.*

Evaluation index	Indicator description
Header hash	The structure in the block header is detected to verify whether it contains an accurate header hash.
Parent hash	The structure in the block header is detected to verify whether it contains an accurate parent hash.
Merkel root	Detect the structure in the block head to verify whether it contains accurate Merkel root.
time stamp	The structure in the block header is detected to verify whether it contains an accurate time stamp.
Openness	Test the openness of the blockchain system

2.2. Public Key Cryptography Evaluation Index

Public key cryptography is also called asymmetric cryptography, which is relative to symmetric cryptography. Symmetric cryptography uses the same key in the process of encryption and decryption, while public key cryptography uses the private key in the process of encryption and the public key in the process of decryption. In the block chain, the solution principle of elliptic and discrete logarithm problems is often used to generate a pair of public keys and private keys,

The public key is generally published, while the private key is in the user's own hands. Taking bitcoin system as an example, if you want to complete a bitcoin transfer operation, you need to apply the private key to encrypt and sign the content and specify the address of the transaction input. Generally, the address is generated by the public key through hash operation, Then the receiver decrypts the transaction through its public key, that is, the process of verifying the signature, so that the transaction is completed. Since the application of cryptography directly involves the transaction problem, its security problem is particularly important. Based on the security perspective, the following evaluation indexes are proposed, namely Hassi anti-collision, privacy protection and private key protection, And the state secret algorithm. Hassi's anti-collision performance is mainly aimed at common collision attacks. By mastering the characteristics of the hash function and deliberately using some data, they will produce the same value through hash operation. A large number of the same hash values will cause loopholes in the system. A good hash function should have very low collision performance, Privacy protection is mainly aimed at the possible disclosure of user privacy in the transaction process. For example, in bitcoin system, the transaction is visible in the whole network. Therefore, through the analysis of data, we can infer the specific trader and its related information. Using privacy protection protocol can effectively avoid this problem, improve user anonymity and private key protection, It is mainly aimed at the possible leakage and improper storage of the private key. Because the private key is only held by the user, and its length and complexity are high, it is generally difficult for the user to remember it directly. If the system provides a corresponding private key protection mechanism, the risk of loss or leakage of the private key can be reduced. The state secret algorithm refers to whether the system adopts sm2sm3 state secret algorithm, That is, using the state secret certificate for CA verification, these methods can effectively improve the security of the system. The evaluation indicators of public key cryptography are shown in Table 2.

Table 2. *Public key cryptography evaluation index.*

Evaluation index	Indicator description
Hash anti-collision	Test whether the hash algorithm adopted by the blockchain system has good anti-collision attack ability.
Privacy protection	Check whether the blockchain system provides protection for the user's transaction information
Private key protection	Verify whether the blockchain system can guarantee the security of the user's private key
State secret algorithm	Check whether the blockchain system uses sm2sm3 national secret algorithm and CA certificate verification

2.3. Evaluation Index of Peer-to-Peer Network Technology

Peer to peer network communication technology, also known as P2P network communication technology, aims to enable all nodes in the system to have the same status and exchange data. The use of P2P technology is also an important basis for the decentralization of the blockchain system. It makes each node in the blockchain system have the same status without any higher weight or special nodes, The evaluation indexes of point-to-point network technology are as follows, including reliability, fault tolerance to node faults, and verification of node additions and deletions. Reliability means that the data transmission of a P2P network protocol must be reliable, such as TCP protocol, that is, in the process of data transmission, try to reduce the error or loss of data, so that in the blockchain system, other nodes can carry out effective verification only after receiving the information from the node. The fault tolerance of faulty nodes means that the protocol allows one or more nodes in the system to have faults, and the faults should not affect the normal operation of the system. The addition and deletion of nodes refers to the P2P network protocol of the blockchain system, which should be able to verify the newly added and exited nodes in the system in time to ensure that the system is in operation, There will be no errors due to node omission or redundant detention. The evaluation indexes of point-to-point network technology are shown in Table 3.

Table 3. *Evaluation index of peer-to-peer network technology.*

Evaluation index	Indicator description
reliability	Check whether the P2P protocol adopted by the blockchain system is reliable
Fault tolerance of node failure	Check whether the P2P protocol used in the system allows a certain number of nodes to fail
Verification of node addition and deletion	Check whether the blockchain system can automatically identify nodes for addition and deletion

2.4. Consensus Mechanism Evaluation Index

Consensus mechanism accounts for a large proportion in the blockchain system. By adopting different consensus mechanisms, various indicators of the system, such as performance and security, will also change greatly. Therefore, the research on consensus algorithm also accounts for a large proportion in the blockchain research system. The consensus mechanism adopted by the blockchain system, Compared with the consensus mechanism in the traditional distributed system, it has improved to a certain extent, but there are still many problems. The first is the problem of security. There are many attack methods against consensus, such as 51% attack, double flower attack, selfish mining attack, deterministic algorithm replay attack, all-out oppression attack, blockchain bribery attack, etc, These attacks will undoubtedly have a great impact on the security of the blockchain system. The second is the scalability of the consensus mechanism. Although some consensus algorithms have excellent performance in some aspects, they also have great defects in others. The scalability of these consensus algorithms is very low. The third is the degree of decentralization, Decentralization is one of the most important characteristics of the blockchain system. At the level of consensus mechanism, the degree of decentralization is specifically reflected in the number of nodes. The more nodes, the higher the degree of decentralization, and the more advantages of the blockchain system can be reflected. For these problems, the proposed evaluation indicators are as follows, including the degree of decentralization and resource consumption, The percentage of fault-tolerant nodes, as well

as certainty. As mentioned above, the degree of decentralization is an important indicator to measure the characteristics of a blockchain system. The fewer nodes, the lower the degree of decentralization. It can not reflect the advantages of the blockchain system. Resource consumption is an integral part of scalability. Algorithms with high resource consumption, such as POW algorithm, need to consume a lot of resources, As well as the long block write interval, its application scope has certain limitations. The percentage of fault-tolerant nodes is also a part of scalability. With only a higher percentage of blockchain systems, the robustness of the new system is better, and the consensus mechanism used has a wider range of applications. Finally, certainty is an important aspect of security. It refers to the possibility that relevant information can be tampered with once it is entered into the block. In some algorithms, such as pow, tampering with information is not impossible, but the probability is relatively low, while in other algorithms, tampering is absolutely impossible in theory. The evaluation indicators of consensus mechanism are shown in Table 4.

Table 4. *Consensus mechanism evaluation index.*

Evaluation index	Indicator description
Degree of decentralization	The degree of decentralization is determined by detecting the number of nodes in the system.
resource consumption	Test the consensus mechanism of the system and the degree of resource use.
Percentage of fault tolerant nodes	The consensus mechanism adopted by the system is tested to allow the percentage of failed nodes in the total nodes.
certainty	Check whether the information of the blockchain system can be changed once written into the block.

2.5. Evaluation Index of Smart Contract Mechanism

The smart contract mechanism does not have to be used in the blockchain system, but the decentralized and high security characteristics of the blockchain system can make the smart contract mechanism play its role better. The smart contract in the blockchain was first inspired by the script in the bitcoin system. It can also be said that the script command in the bitcoin system is the prototype of the smart contract, Compared with unchangeable script code, smart contract is more flexible and has a wide range of applications. It is more like a transaction. These characteristics also improve the complexity of smart contract design and practice, and produce a series of security problems. Based on the above problems, the proposed evaluation indicators of smart contract mechanism include trigger mechanism, terminatability and fallback, And isolation. The trigger mechanism is mainly used to evaluate whether the smart contract can select the correct contract and act on the correct contract object when specific conditions are met. It is an evaluation index for its functional attributes. Termination is used to judge whether the contract can be terminated immediately in case of unexpected circumstances requiring temporary termination of the contract. Fallback means that since the smart contract is more similar to a transaction, it should have a fallback mechanism similar to a transaction, that is, when the contract is temporarily terminated, it can correctly fallback to the state before the start of the contract without any impact on the data. Isolation is proposed from the perspective of security. The condition is to verify whether the smart contract runs in a sandbox environment, That is, in the virtual machine or container, if the data in the blockchain is directly operated by the smart contract, the data in the block may be damaged, resulting in security problems. The evaluation indicators of smart contract mechanism are shown in Table 5.

Table 5. *Evaluation index of smart contract mechanism.*

Evaluation index	Indicator description
Trigger mechanism	Check whether the trigger conditions and objects of the smart contract used in the system are correct
Termination	Check whether the smart contract can be temporarily terminated during the process
Fallback	Check whether the smart contract can return to the unexecuted state after temporary termination
Isolation	Check whether the smart contract adopted by the system has an independent operating environment

2.6. Upper Application Evaluation Index

For the top-level application system, it should be directly oriented to the user, and enable the user to complete the functional logic that the system can achieve under a series of operations. The evaluation indexes for the application system are as follows, including functional integrity, interface aesthetics and operation simplicity. Functional integrity means that calling the product through the interface can realize all the functions that the product should realize. Interface aesthetics means that the UI interface provided to users for operation should be beautiful enough, including the placement of navigation bars of various menus and the shape design of icons and various function buttons. It should make users feel comfortable after seeing it. The simplicity of operation means that users facing the application may not understand blockchain technology, Therefore, the underlying content of the blockchain should be encapsulated as much as possible, and only the most concise operation logic should be provided to the user, so that the user can quickly become familiar with the application and be able to use it skillfully. The upper application evaluation indicators are shown in Table 6.

Table 6. *Upper application evaluation index.*

Evaluation index	Indicator description
Functional integrity	Check whether the upper application of the system can realize various functions provided by the blockchain system
Interface aesthetics	Check whether the interface design of the upper application is reasonable and beautiful
Ease of operation	Check whether the operation logic of the upper application is concise enough

3. Demand Analysis of Evaluation System

Requirements analysis is an important process of software design and development. Good requirements analysis can

guide the subsequent software design and make the goal of design and development more clear.

3.1. Functional Requirements Analysis

From the perspective of function, the requirements to be realized by the system include the following aspects. Firstly, the user can choose to evaluate the blockchain product in the interface. At the beginning of the evaluation, the user can enter the basic information of the blockchain product, including the name of the blockchain product, and then the user should be able to evaluate the blockchain product in the evaluation system according to the actual situation of the blockchain product, Select or enter the options of corresponding indicators. After entering all indicators in turn, the user can submit the results. Before submitting, the user can modify the filled indicators. After submitting, the system should be able to evaluate and score the characteristics of the blockchain product according to the information submitted by the user, The evaluation results are presented to the user, and then the user can return to the main interface to evaluate other products again or exit the system.

Secondly, the system should have one or more administrator users. The role of administrator users is to maintain various existing blockchain product evaluation information, including modifying and deleting information. In order to ensure the security of data, users without administrator authority cannot view all blockchain product evaluation information.

3.2. Non Functional Requirements Analysis

The non functional requirements of the system mainly include the following aspects:

First, the operation interface is simple and beautiful. Since the logical functions of the system are not complex and relatively simple from the perspective of function, the interface design should also strive to be simple, so that users can immediately master the use method of the system after contacting the system. At the same time, the simple and beautiful interface will also give users a good use experience.

Second, because the volume of the system is relatively small, we should improve the operation efficiency and response speed of the system as much as possible, so as to enable users to complete their business needs as soon as possible and achieve the purpose of using the system.

Third, because the information involved in the system is relatively sensitive and involves some private information of user products, the system should improve the security of stored data and prevent data loss and leakage. At the same time, it should ensure the security of administrator account and prevent the problem of data modification or deletion caused by account theft.

4. Conclusion

Various application products based on blockchain technology emerge in endlessly, but at present, there is no product on the market that can evaluate many blockchain products and all aspects in the market. The purpose of this paper is to propose a set of evaluation system for general blockchain products based on such a current situation. It should be pointed out that the blockchain evaluation system involved in this paper is only for general blockchain products with broad significance. For blockchain products in some fields, the evaluation indicators of the evaluation system may not be fully consistent. The author believes that this is a major difficulty in designing blockchain product evaluation system and a direction worthy of further consideration in the future, Finally, the author believes that it is difficult to design a set of blockchain product evaluation system which is very universal and can improve the usable value under the current situation of diversified blockchain products and the design of many blockchain products has not been standardized, However, in this case, the application research on the development of evaluation indicators and related systems of blockchain products still has high value. The continuous design of evaluation indicators and the development of evaluation system will also promote the standardization of blockchain products, which needs to be carried out for a long time.

Acknowledgements

I would like to thank the authors of references and relevant researchers. Their research has given me important reference and help and provided a good reference for the completion of my thesis.

References

[1] Zhang Chengdong, Li Minjie, Analysis and Prospect of virtual currency. Vol 8, 2021, pp. 65-68.

[2] Tan Zuocai, On the Legal Relationship and Private Law Protection of Virtual Currency Circulation. China Business and Market, Vol 3, 2021, pp. 102-110.

[3] Gou Chenchen, Research on the current situation and development of blockchain and bitcoin. China broadband, Vol 5, 2021, pp. 129.

[4] Huo Zhenye, Su Bo, Research on layered blockchain architecture based on Ethereum. Computer Applications and Software, Vol 9, 2020, pp. 16-19, 26.

[5] Li Xinyu, Jia Weiyang,. Application of Blockchain Technology in Medical Insurance, Vol 18, 2021, pp. 44-46.

[6] Liu Hanqing, Yuan Na, Lei-peng Xiang, A Survey on Attacking Strategies in Blockchain. Chinese Journal of Computers, Vol 4, 2021, pp. 786-805.

[7] Li Linwei, Blockchain based proxy re encryption information sharing and secure multi-party computing model. Changjiang Information &Communications, Vol 2, 2021, pp. 107-110.

[8] Du Ruizhong, Tan Ailun, Tian Junfeng, Public key searchable encryption scheme based on blockchain. Journal on Communications, Vol 4, 2020, pp. 114-122.

[9] Shi Pengzhan, Blockchain data authority management scheme based on symmetric encryption. Computer Knowledge and Technology, Vol 17, 2021, pp. 24-25, 35.

[10] Zhong Zengsheng, An Improvement on Blockchain-Based PoS Consensus Algorithm. Journal of Chongqing Technology and Business (Natural Sciences Edition), Vol 4, 2021, pp. 36-41.

[11] Zhang Sixian, Wen Jie, A block chain consensus algorithm based on grouping. Computer Applications and Software, Vol 3, 2020, pp. 261-265, 309.

[12] Wu Yue, Li Junxiang, Evolution process of blockchain consensus algorithm. Application Research of Computers, Vol 7, 2020, pp. 2097-2103.

[13] Guo Chunmei, Zhu Baoping, An Improved Blockchain Consensus Algorithm Computer and Digital. Computer and Digital Engineering, Vol 6, 2020, pp. 1290-1293, 1349.

[14] Chen Binger, Wang Banghai, Lao Nanxin, A Quantum-encrypted Blockchain Based on Delegated Proof of Stake (DPoS) Extension. ournal of Guangdong University of Technology, Vol 2, 2021, pp. 34-38.

[15] Zhuang Haiyan, Performance Analysis of Consensus Algorithm in Private Blockchain. Journal of Binzhou University, Vol 2, 2020, pp. 63-68.