2022 7th IEEE International Conference on Data Science in Cyberspace (DSC) | 978-1-6654-7480-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/DSC55868.2022.00067

Security Evaluation Model of Blockchain System Based on Combination Weighting and Grey Clustering

Jiahao Qi
School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, China
qijiahao@bupt.edu.cn

Ziyu Guo
School of Information and Communication Engineering
Beijing University of Posts and Telecommunications
Beijing, China
zyguo@bupt.edu.cn

Yueming Lu
School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, China
ymlu@bupt.edu.cn

Jiaqi Gao
School of Information and Communication Engineering
Beijing University of Posts and Telecommunications
Beijing, China
gaojiaqi@bupt.edu.cn

Yihong Guo
School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, China
guoyihong@bupt.edu.cn

Fanyao Meng
School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, China
mengfy@bupt.edu.cn

***Abstract*—With the widespread application of blockchain technology in social and economic fields, various security challenges have become increasingly prominent and attracted many researchers to work in this domain. To address this issue, we propose a blockchain system security evaluation model based on game theory combination weighting and grey clustering. Considering the correlation between indexes, the security evaluation index system is constructed hierarchically from the technical system framework of blockchain. Then we use the combination weighting algorithm based on game theory to optimize the ratio of subjective and objective weights, and balance the evaluation error caused by the difference between subjective and objective weights to make the weight quantification more scientific and accurate. Finally, the security evaluation level of the blockchain system is determined by grey clustering evaluation method. The effectiveness of this method is verified by our experiments, which provides a useful reference for the security evaluation of blockchain systems.**

Keywords—blockchain, combination weighting, grey clustering, security evaluation

I. INTRODUCTION

Blockchain is a distributed ledger with the characteristics of decentralization, tamper-proof, traceability, openness and transparency. Common blockchain systems include Bitcoin[1], Ethereum [2], and Hyperledger [3], which is essentially a decentralized database [4]. Blockchain can provide secure electronic transaction services and trusted peer-to-peer value transmission without relying on third-party trusted institutions. As a brand-new data storage, management and transmission technology, blockchain becomes a national strategic technology. However, with the rapid development of blockchain technology, the security risks faced by the blockchain are becoming increasingly serious. Therefore, the security evaluation of blockchain systems has become the study focus at home and abroad.

Blockchain-based information systems face similar security risks to other information systems at the user layer, interface layer, and core infrastructure layer. Zhu Yan et al. [5] summarized and analyzed the core technologies of the blockchain system from the control point of the third-level security level 2.0, but did not give the overall security evaluation results of the blockchain system. Ye Congcong et al. [6] proposed a model for security detection based on the structure of the blockchain to solve the problem of incomplete analysis of a single attack using mathematical methods. Qin Chaoxia et al. [7] proposed a new security risk assessment model from two aspects of technical architecture and computing power, but the analytical hierarchy process(AHP) method chosen by them relies too much on the opinions of experts, and the assignment of the weight of security risk factors is not accurate enough. Song Yingchun et al. [8] proposed a method to dynamically measure and evaluate blockchain security risks based on the blockchain maturity model.

According to the literatures, most of the existing blockchain security evaluation methods have simple evaluation processes and lack a complete and comprehensive evaluation model framework. In addition, there are many existing security standards, but when implemented into the index system of actual security assessment, there are many indexes such as blockchain function and performance, and less attention is paid to the security of data information. Moreover, the selected evaluation method is relatively subjective in the determination of index weights, and is mostly completed by expert evaluation,

DOI 10.1109/DSC55868.2022.00067

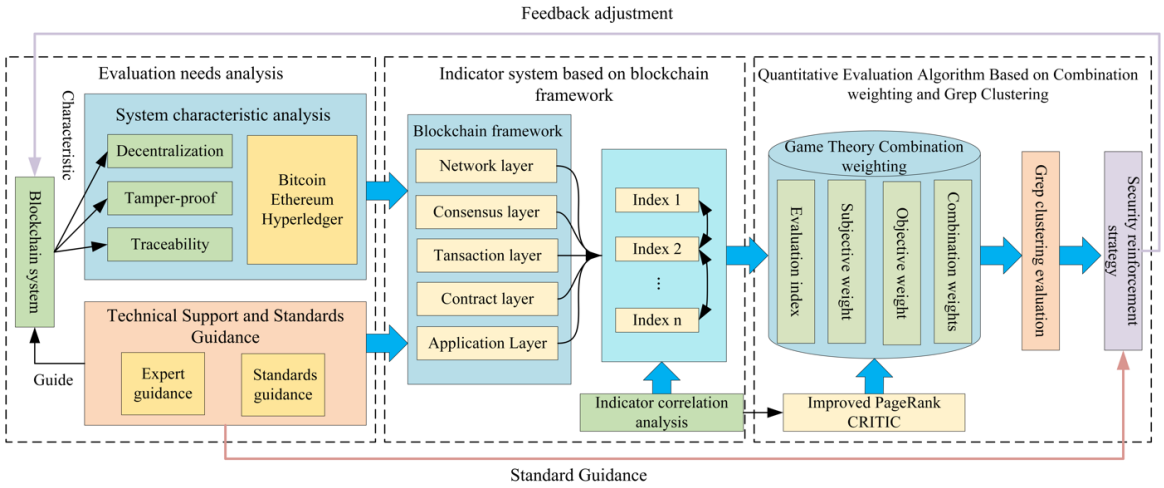

Fig. 1. Security evaluation model of blockchain system based on combination weighting and grey clustering

which lacks index correlation analysis. Therefore, this paper further improves the security evaluation index system of the blockchain system from the perspective of the core technical framework of the blockchain system and the correlation analysis of indexes. By improving the traditional weighting method, the combination weighting algorithm based on game theory is introduced, and then a security evaluation model based on combination weighting and grey clustering is proposed.

II. Security Evaluation Model of Blockchain System Based on Combination Weighting and Grey Clustering

In view of the lack of a unified security evaluation model for the blockchain system, this paper proposes a security evaluation model for the blockchain system based on the combination weighting and grey clustering, as shown in Fig. 1, according to the national standard(GB) information security evaluation criteria and classified protection of information security level 3 [9] (referred to as level 3 equal protection) standard, and on the basis of considering the mutual influence between the evaluations. The evaluation model combines the technical system framework of the blockchain to construct the security evaluation index system of the blockchain system. The combination weighting method based on game theory is used to optimize the ratio of subjective and objective weights, and the security level of the blockchain system is obtained through grey clustering evaluation. The evaluation model expounds the evaluation process and key considerations of the blockchain system, and provides support for the construction of the security enhancement strategy of the blockchain system.

A. Indicator system based on blockchain framework

In this paper, referring to the GB information security assessment criteria and the control points of the three-level standard for equal protection, on the basis of considering the blockchain framework, the security assessment index system is constructed hierarchically. The indexes obtained based on the blockchain framework have different impacts on the security evaluation of the entire system, and there is a certain correlation between the evaluation indexes. Therefore, by constructing the index system for correlation analysis between them, the security of the system can be more comprehensively and accurately reflected to ensure the scientific validity of system security evaluations.

Currently, mainstream blockchain systems include Bitcoin, Ethereum, and Hyperledger. The different characteristics of these blockchain systems bring new challenges to the security evaluation of blockchain systems. However, no matter what kind of blockchain system, according to the system framework of the blockchain, it can be divided into network layer, consensus layer, transaction layer, contract layer and application layer, as shown in Fig. 2.

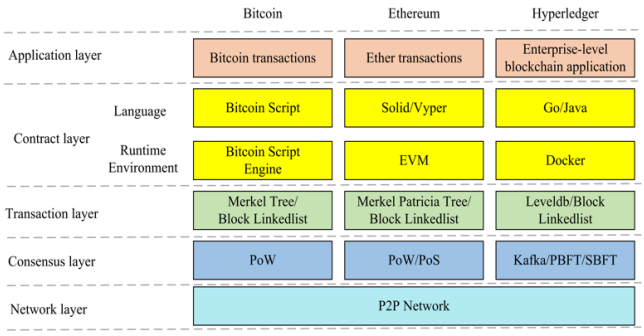

Fig. 2. Blockchain framework

On the basis of the analysis of the blockchain system framework, combined with the GB information security evaluation criteria and level 3 equal protection standard, the blockchain information security evaluation index is divided into five first-level indexes, namely, peer-to-peer network security, consensus mechanism security, distributed ledger security, smart contract security, application expansions and environments security. After expansion, integration, screening and elimination of redundancy, a total of 22 second-level indexes are obtained, as shown in Table 1. The following is an

explanation of the indicators at each level, and provides the basis for the subsequent index scores.

TABLE I. BLOCKCHAIN INFORMATION SECURITY EVALUATION INDEX SYSTEM

Security assessment objectives	First-level indicator（u_j）	Secondary indicators（u_{jp}）
Blockchain system	Peer-to-Peer network security（u_1）	Self-protection and adaptation（u_{11}）
		Node access control（u_{12}）
		Get updates on network status（u_{13}）
		Dynamic monitoring of network nodes（u_{14}）
	Consensus mechanism security（u_2）	Consensus resource control（u_{21}）
		Data backup（u_{22}）
		System hot redundancy（u_{23}）
		Consensus fault tolerance（u_{24}）
		Choice of consensus mechanism（u_{25}）
		Number and location of nodes（u_{26}）
	Distributed ledger security（u_3）	Ledger access control（u_{31}）
		Key management（u_{32}）
		Data confidentiality（u_{33}）
		Data integrity（u_{34}）
		Data availability（u_{35}）
		Identity and transaction privacy protection（u_{36}）
	Smart contract security（u_4）	Perform authentication（u_{41}）
		Protection from malicious code（u_{42}）
		Behavioral event audit（u_{43}）
		Audit records（u_{44}）
	Application extensions and environments security（u_5）	Storage capacity（u_{51}）
		Physical environment security（u_{52}）

1) Peer-to-Peer network security: A distributed peer-to-peer network is a computer network that contains only nodes with equivalent control and operational capabilities. In order to evaluate the access, transmission and network security status of consensus nodes and network nodes in the blockchain, distributed peer-to-peer network security mainly evaluates the blockchain P2P network from control points such as software fault tolerance, identity authentication, and security audit. Specific secondary indexes include self-protection and adaptive capabilities, node access control, network status update, and network node dynamic detection.

2) Consensus mechanism security: The consensus mechanism [10] is a way to ensure that the member nodes of the blockchain system reach a consensus on a series of ordered transaction sequences. Since the blockchain is characterized by decentralization, there is no centralized accounting node to ensure that the records of transactions on all nodes are consistent. The role of the consensus mechanism is to achieve data consistency and operational synchronization between nodes in the blockchain. The security of the consensus mechanism mainly evaluates the security of the consensus layer of the blockchain from control points such as resource control, data backup and recovery, and consensus effect. Specific secondary indexes include consensus resource control, data backup, system hot redundancy, consensus fault tolerance, consensus mechanism choice, number and location of nodes.

3) Distributed ledger security: Distributed ledger [11] is a distributed data storage structure that is serialized, synchronously shared, and tamper-proof among each node member. It can provide storage and query services for various data generated during the operation of the blockchain system. This paper selects six secondary indexes from the aspects of access control, data confidentiality, data integrity and other control points, key management, and privacy protection. Specific secondary indexes include ledger access control, key management, data confidentiality, data integrity, data availability, identity and transaction privacy protection.

4) Smart contract security: A smart contract is a computer program or script that runs on the blockchain and is a carrier for implementing business logic. As the carrier of data, the blockchain stores the key information of a series of transactions, and smart contracts are the rules of operating these data in the blockchain. The security assessment for the smart contract layer should start from the control points such as identity authentication, malicious code prevention, and security audit, and analyze it item by item. Specific secondary indexes include execution of identity verification, malicious code attack, behavior event audit, and audit records.

5) Application expansions and environmentals security: The distributed ledger will continue to expand with the changes of the nodes of the blockchain, so it is necessary to continuously expand the storage capacity, and the environment in which the blockchain application is located is also an evaluation index that needs to be paid attention to. For the scalability and environmental security of the application, two secondary indexes, such as storage capacity and physical environmental security, are selected.

III. QUANTITATIVE EVALUATION ALGORITHM BASED ON COMBINATION WEIGHTING AND GREY CLUSTERING

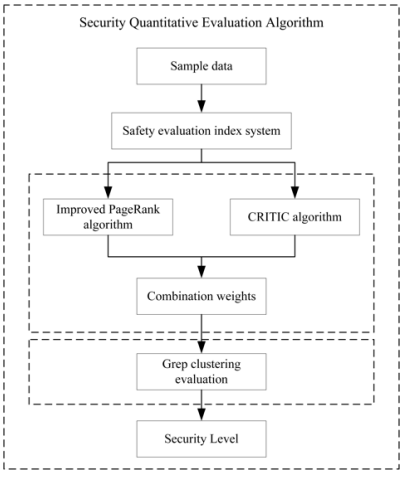

Fig. 3. Flowchart of quantitative evaluation algorithm

The quantitative evaluation algorithm is mainly composed of game theory combination weighting and grey clustering evaluation, as shown in Fig. 3. Considering that a single subjective and objective weight confirmation method is not accurate enough, this paper uses the method of game theory to combine the subjective and objective weights obtained by the two weight determination algorithms, and then obtains the security evaluation results of the blockchain system through the grey clustering evaluation. Finally, it analyzes the results combined with the opinions of experts, and provides good information security improvement feedback to the target system to improve the information security level of the system.

A. Calculation of subjective weights based on sorting-based weighting algorithm

The ranking-based weight confirmation algorithm uses the idea of PageRank [12] to combine the basic principle of Markov chain and the correlation between indexes, and determines the weight of indexes according to the collective evaluation results of experts. Using this algorithm to determine the weight of indexes not only considers the correlation between indexes, but also integrates the evaluation results of experts [13].

The improved ranking-based weight determination algorithm based on the idea of PageRank is based on the following assumption: if a node receives a larger weight from other pointing chains, then this node is more important. At the same time, the quality of the inbound nodes pointing to the node is different, and the node with high quality will transfer more weights to other nodes through the link, so the node with higher quality points to node *A*, the more important node *A* is.

The formula for calculating the *PR* value of each node is:

$$PR_{(p_i)} = \alpha \sum_{p_j \in M_{p_i}} \frac{PR_{(p_i)}}{L_{(p_j)}} \quad \frac{(1-\alpha)}{N} \tag{1}$$

Where, M_{p_i} is the set of all nodes that have out-chains for p_i node, $L_{(p_j)}$ is the number of out-chains of nodes, and N is the total number of nodes, α is the probability the user randomly reaches a node, generally taken as 0.85. The *PR* value can be calculated according to equation (1). When the iteration tends to be stable, the result can be obtained.

B. Calculation of objective weight based on CRITIC method

The objective weight of each index of the CRITIC method is calculated by the amount of information contained in the index data. The amount of information is represented by the contrast strength and correlation between indexes [14]. The contrast strength usually takes the standard deviation of the data. Considering the influence of the mean on the contrast strength, this paper takes the coefficient of variation as the contrast strength. The CRITIC method is suitable for data that has a certain correlation between the analyzed index factors. As an improvement of the entropy weight method, it fully shows the difference and conflict between the indexes, and has strong practicability. The algorithm steps are as follows:

Suppose there are *m* evaluation objects, and *n* evaluation indexes form the original evaluation matrix $X = \left(x_{ij}\right)_{mxn}$, where x_{ij} represents the value of the j-th indexes of the i-th object.

Standardize the indicators in the evaluation matrix *X*:

$$\overline{x}_J = \frac{1}{m}\sum_{i=1}^{m} x_{ij}| \tag{2}$$

$$s_j = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(x_{ij} - \overline{x}_j\right)^2} \tag{3}$$

$$x_{ij}^{*} = \frac{x_{ij} - \overline{x_j}}{s_j} \quad (i = 1,2,\cdots,m; j = 1,2,\cdots,n) \tag{4}$$

Determination of index variation coefficient:

$$v_j = \frac{s_j}{\overline{x_j}} (j = 1,2,\cdots,n) \tag{5}$$

where v_j is the coefficient of variation of the j-th index.

Use the standardized matrix *X* to extract the correlation coefficient, and get the correlation coefficient matrix:

$$R = \left(r_{kj}\right)_{nxn} (k = 1,2,\cdots,n; j = 1,2,\cdots,n) \tag{6}$$

The quantification coefficient of the degree of independence of each indicator:

$$n_j = \sum_{k=1}^{n}\left(1 - r_{kj}\right), j \quad 1,2,\cdots,n \tag{7}$$

The comprehensive coefficient of each evaluation index:

$$C_j = v_j n_j, j = 1,2,\cdots,n \tag{8}$$

Objective weight of each indicator:

$$W_j = \frac{C_j}{\sum_{j=1}^{n} C_j} (j = 1,2,\cdots,n) \tag{8}$$

C. Combination Weights Based on Game Theory

The combination weighting method based on game theory takes the Nash equilibrium as the coordination goal to find the balance between different weights in the conflict between the weights obtained by the subjective and objective weighting methods, which is an integrated process of mutual comparison and coordination. This method can take into account the subjective and objective weights, comprehensively consider the inherent information between each index, reduce the randomness of weight determination, and improve the scientific rationality of index weighting. The combination weighting steps are as follows [15]:

The weight of each index is determined by the ranking-based confirmation weight method and the CRITIC method respectively. The basic weight vector set is

$\{w_{k1}, w_{k2}, \cdots, w_{kn}\}$, $k = 1, 2, \ldots, L$, where L is the number of methods to determine the weight, this paper takes $L = 2$, n is the number of evaluation index. The linear combination weight coefficient is $\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_L\}$. Then the combined weight w is:

$$w = \sum_{k=1}^{L} \alpha_k w_k^T, \alpha_k > 0, k = 1, 2, \ldots, L \tag{10}$$

In (10): when α is the optimal combination coefficient, w is the optimal combination weight.

Therefore, the above analysis transforms the problem of finding the optimal combination weight into the problem of finding the optimal linear combination weight coefficient. In order to obtain the optimal weight w^*, according to the idea of game theory, with the minimum deviation between w and w_k as the goal, the above linear combination weight coefficient is optimized, and the obtained objective function is:

$$\min \left\| \sum_{k=1}^{L} \boldsymbol{\alpha}_k \boldsymbol{w}_k^T - \boldsymbol{w}_k \right\|_2, k = 1, 2, \cdots, L \tag{11}$$

According to the properties of matrix differentiation, the optimal first-order derivative condition of (11) is:

$$\sum_{k=1}^{L} \alpha_k \boldsymbol{w}_k w_k^T = \boldsymbol{w}_k w_k^T, k = 1, 2, \ldots, L \tag{12}$$

The α_k obtained by the above formula is normalized to obtain a_k^*, and the calculation formula is as follows:

$$a_k^* = \frac{\alpha_k}{\sum_{k=1}^{L} \alpha_k} \tag{13}$$

The combination weights based on game theory are:

$$w^* = \sum_{k=1}^{L} a_k^* w_k^T, k = 1, 2, \ldots, L \tag{14}$$

D. Grey Clustering Evaluation Based on Game Theory Combination Weighting

The security situation of the blockchain system is caused by the interaction of various related factors, which makes the security evaluation of the blockchain system have multi-factor and incomplete characteristics. In order to solve these problems with "grey" (partial information is clear, and some information is not clear), this paper introduces the grey clustering evaluation method.

Grey clustering evaluation is a method of dividing the evaluation objects into several predefined categories according to the whitening weight function in the grey system [16]. The steps of grey clustering evaluation based on the combination weighting method are as follows:

1) Determine grey: The security status of the blockchain system can be quantitatively represented by the grey-level classification method. According to the type and requirements of the evaluation results, five grey classifications are set: "lower", "low", "medium", "high", "higher", and represented by k values of 1, 2, 3, 4, and 5.

2) Building a whitening weight function: The whitening weight function is usually determined according to the turning point of the index, and the specific value of the turning point is generally given by domain experts. See Table 2 for the determination of the grey turning point of the blockchain system evaluation index.

TABLE II. GREY CLASSIFICATION BOUNDARY VALUES OF SYSTEM SECURITY EVALUATION INDEXES

The grey classification of the index	k=1	k=2	k=3	k=4	k=5
Index grey turning point	5.5	6.5	7.5	8.5	9.5

From the above table, we can obtain the whitening weight function expressions of the five grey classifications of "lower", "low", "medium", "high" and "higher" for the safety security evaluation indexes, which are:

$$f_j^1(x) = \begin{cases} 0, x \notin [0, 6.5] \\ 1, x \in [4.0, 5.5] \\ \dfrac{6.5 - x}{6.5 - 5.5}, x \in [5.5, 6.5] \end{cases} \tag{15}$$

$$f_j^2(x) = \begin{cases} 0, x \notin [5.5, 7.5] \\ \dfrac{x - 5.5}{6.5 - 5.5}, x \in [5.5, 6.5] \\ \dfrac{6.5 - x}{7.5 - 6.5}, x \in [6.5, 7.5] \end{cases} \tag{16}$$

$$f_j^3(x) = \begin{cases} 0, x \notin [6.5, 8.5] \\ \dfrac{x - 6.5}{7.5 - 6.5}, x \in [6.5, 7.5] \\ \dfrac{6.5 - x}{8.5 - 7.5}, x \in [7.5, 8.5] \end{cases} \tag{17}$$

$$f_j^4(x) = \begin{cases} 0, x \notin [7.5, 9.5] \\ \dfrac{x - 7.5}{8.5 - 7.5}, x \in [7.5, 8.5] \\ \dfrac{9.5 - x}{9.5 - 8.5}, x \in [8.5, 9.5] \end{cases} \tag{18}$$

$$f_j^5(x) = \begin{cases} 0, x \notin [8.5, 10] \\ \dfrac{x - 8.5}{9.5 - 8.5}, x \in [8.5, 9.5] \\ 1, x \in [9.5, 10] \end{cases} \tag{19}$$

3) Calculate the clustering coefficient:

$$\sigma_j^k = \sum_{j=1}^{m} f_j^k \left(x_{ij} \right) w_j \tag{20}$$

In (20): x_{ij} is the j-th index value of the i-th evaluation object, and w_j is the combination weight of the j-th index value.

4) Determine the safety evaluation level:

$$\max_{0 \le k \le 1} \left\{ \sigma_j^k \right\} = \sigma_j^{k^*} \tag{21}$$

In (21): $\sigma_j^{k^*}$ is the largest grey clustering coefficient, and k^* is the gray classification corresponding to the i-th object. In order

to more conveniently evaluate the security status of the blockchain system, the evaluation results are divided into 5 levels, namely "higher security", "high security", "medium security", "low security" and "lower security". The grey classes corresponding to each security level and their corresponding descriptions are shown in Table 3:

TABLE III. SAFETY EVALUATION LEVEL

System status level	Grey classification	Describe
higher security	k=5	The indexes of the blockchain system reache the top standard
high security	k=4	The indexes of the blockchain system have reached a good standard
medium security	k=3	The indexes of the blockchain system are higher than the basic level
low security	k=2	The indexes of the blockchain system have reached the basic level
lower security	k=1	The indexes of the blockchain system have not reached the basic level

IV. EXPERIMENTAL ANALYSIS

In this section, a total of 6 groups of target system samples are investigated, and the items involved in the index system were scored by experts in the survey, and the data are obtained through statistical calculation. Among them, systems 1-4 are conventional samples selected in combination with expert evaluation, and systems 5 and 6 are excellent simulation samples. Considering the number of indexes in Table 1, we take the quantitative evaluation of peer-to-peer network security u_1 and consensus mechanism security u_2 in the primary indexes as the demonstration of the overall security evaluation of the blockchain system. When the subjective weight is determined, 10 experts are selected to score the mutual influence between indicators. The scoring of experts on the relationship between indexes is shown in Table 4:

TABLE IV. EXPERTS' SCORING OF THE RELATIONSHIP BETWEEN INDEXES

	u_{11}	u_{12}	u_{13}	u_{14}	u_{21}	u_{22}	u_{23}	u_{24}	u_{25}	u_{26}
u_{11}	0	3	5	5	4	5	1	2	3	10
u_{12}	1	0	3	3	5	1	1	1	1	3
u_{13}	3	1	0	7	5	5	1	1	3	8
u_{14}	3	3	8	0	5	3	4	1	3	10
u_{21}	3	1	1	1	0	3	3	3	10	8
u_{22}	3	1	2	1	3	0	7	5	3	5
u_{23}	7	5	6	6	3	5	0	5	7	6
u_{24}	6	1	1	1	3	2	7	0	8	8
u_{25}	5	7	8	8	10	10	9	10	0	10
u_{26}	8	7	9	9	6	10	8	5	10	0

Firstly, the adjacency matrix Q is constructed according to the scoring of experts in Table 4. The value of row i-th and column j-th in the adjacency matrix represents the number of experts who believe that the i-th index will affect the j-th index. If Q_{32} is 1, it means that one expert thinks that index u_{13} has an impact on u_{12}. The adjacency matrix Q is shown below.

$$Q=\begin{bmatrix}0&3&5&5&4&5&1&2&3&10\\1&0&3&3&5&1&1&1&1&3\\3&1&0&7&5&5&1&1&3&8\\3&3&8&0&5&3&4&1&3&10\\3&1&1&1&0&3&3&3&10&8\\3&1&2&1&3&0&7&5&3&5\\7&5&6&6&3&5&0&5&7&6\\6&1&1&1&3&2&7&0&8&8\\5&7&8&8&10&10&9&10&0&10\\8&7&9&9&6&10&8&5&10&0\end{bmatrix}$$

The column vectors of the adjacency matrix Q are normalized, and the probability transition matrix S is obtained as follows.

$$S=\begin{bmatrix}0&0.10&0.12&0.12&0.09&0.11&0.02&0.06&0.06&0.15\\0.03&0&0.07&0.07&0.11&0.02&0.02&0.03&0.02&0.04\\0.08&0.03&0&0.17&0.11&0.11&0.02&0.03&0.06&0.12\\0.08&0.10&0.19&0&0.11&0.07&0.10&0.03&0.06&0.15\\0.08&0.03&0.02&0.02&0&0.07&0.07&0.09&0.21&0.12\\0.08&0.03&0.05&0.02&0.07&0&0.17&0.15&0.06&0.07\\0.18&0.17&0.14&0.15&0.07&0.11&0&0.15&0.15&0.09\\0.15&0.03&0.02&0.02&0.07&0.05&0.17&0&0.17&0.12\\0.13&0.24&0.19&0.20&0.23&0.23&0.22&0.30&0&0.15\\0.21&0.24&0.21&0.22&0.14&0.23&0.20&0.15&0.21&0\end{bmatrix}$$

Bringing the probability transfer matrix S obtained above into (22), we can get the final transfer matrix G.

$$G=aS+\frac{1-a}{N}U \tag{22}$$

Where, a is a random probability, which is generally 0.85. N is the number of index nodes, which is 10. U is a matrix with all values of 1.

$$P_{n+1}=GP_n \tag{23}$$

Bring the final transfer matrix into (23), after continuous iteration, we can calculate the vector W' composed of P_n as shown below.

$$W'=\{w_{11},w_{12},\cdots,w_{26}\}=\{0.0912,0.0670,\cdots,0.1564\}$$

The objective weight is determined by using the standardized data. The final summary of the standardized sample data is shown in Table 5.

TABLE V. SAMPLE DATA

indexes	sample					
	system1	*system2*	*system3*	*system4*	*system 5*	*system 6*
u_{11}	7.50	7.70	7.60	8.30	8.50	8.80
u_{12}	7.20	7.40	7.50	7.70	9.0	9.20
u_{13}	7.60	7.70	7.80	7.40	9.10	9.30
u_{14}	7.10	7.60	8.00	7.10	8.60	8.50
u_{21}	7.30	7.80	8.20	8.10	8.80	8.60
u_{22}	7.20	7.10	7.50	6.90	7.80	7.60
u_{23}	7.40	7.80	7.60	7.20	8.20	8.40
u_{24}	7.00	7.50	7.60	7.10	8.10	8.20
u_{25}	7.20	7.30	7.50	7.20	7.90	8.40
u_{26}	7.50	7.60	7.40	6.90	8.00	8.20

The objective weight is calculated by the Critic method as

$$w_1'' = \{w_{11}, w_{12}, \cdots, w_{26}\} = \{0.1730, 0.1213, \cdots, 0.1111\}$$

The basic weight vector set is brought into the formula of the combination weighting method based on game theory, and the obtained combination weight is shown in Table 6.

TABLE VI. WEIGHTS OF VARIOUS INDICATORS

index	Subjective weight	Objective weight	Combination weights
u_{11}	0.0912	0.1730	0.1456
u_{12}	0.0670	0.1213	0.1032
u_{13}	0.0972	0.0879	0.0918
u_{14}	0.0952	0.0942	0.0953
u_{21}	0.1031	0.1246	0.1180
u_{22}	0.0976	0.0878	0.0919
u_{23}	0.0969	0.0701	0.0800
u_{24}	0.0787	0.0621	0.0684
u_{25}	0.1168	0.0678	0.0855
u_{26}	0.1564	0.1111	0.1278

The whitening weight function value is calculated according to the sample data in Table 5, and the grey clustering coefficients of each index with respect to different grey classifications was obtained by using the combination weights in Table 6. The grey clustering coefficients reflect the membership degrees of each system at different security levels, which is shown in Table 7.

TABLE VII. GREY CLUSTERING COEFFICIENTS OF DIFFERENT SYSTEMS FOR DIFFERENT GREY CLASSES

System	k=1	k=2	k=3	k=4	k=5
system 1	0.00	0.12	0.52	0.01	0.00
system 2	0.00	0.05	0.51	0.09	0.00
system 3	0.00	0.00	0.47	0.17	0.00
system 4	0.00	0.10	0.34	0.21	0.00
system 5	0.00	0.00	0.06	0.43	0.15
system 6	0.00	0.00	0.08	0.36	0.20

The comprehensive scores and rankings of the six system samples are calculated by using the sample data and combination weights, which is shown in Table 8.

TABLE VIII. EVALUATION RESULTS OF SAFETY LEVEL OF EACH SYSTEM

System	Overall rating	Security Level	Ranking
system 1	7.3773	medium	6
system 2	7.6213	medium	4
system 3	7.7307	medium	3
system 4	7.5080	medium	5
system 5	8.4845	high	2
system 6	8.6068	high	1

Finally, the comprehensive scores of six system samples are calculated = {7.3773, 7.6213, 7.7307, 7.5080, 8.4845, 8.6068}. As shown in Figure 4, the corresponding security levels of the six systems are: {medium, medium, medium, medium, high, high}, the performance of systems 5 and 6 is good, the security level is high, and the security level of systems 1 to 4 is medium, which is in line with the expected results of the experiment.

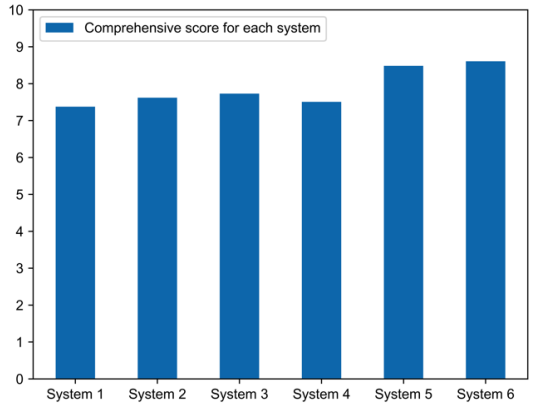

Fig. 4. Comprehensive score of each system

In order to analyze the impact of different weighting methods on the evaluation results, the index weights obtained by each weighting method are compared in Figure 5. From the weight results of the combination weighting method based on game theory, the combination weight is generally close to the average value of the two weight results. Considering the characteristics of the combination weighting method, it is believed that the combination weighting method based on game theory takes both subjectivity and objectivity into account. The results are more reasonable than the results of the PageRank method and the Critic method. At the same time, it can also be observed that self-protection and self-adaptation and the number and location indicators of nodes account for a large proportion of the total weight, which is one of the important factors affecting the evaluation score of peer-to-peer network security and consensus mechanism security. The security level of each index will quickly and effectively improve the overall security level of the system.

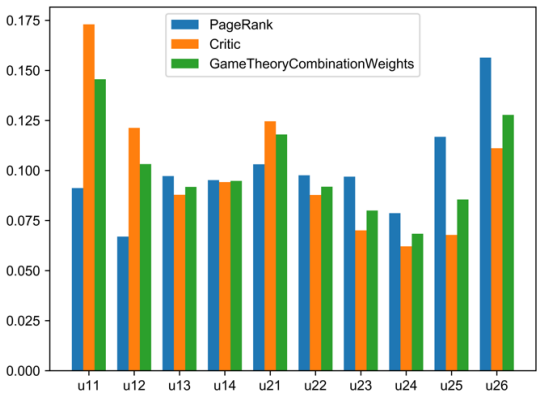

Fig. 5. Index weights of each weighting method

V. Conclusion

Aiming at the lack of a unified security evaluation model for the existing blockchain evaluation methods, we propose a blockchain system security evaluation model based on the combination weighting and grep clustering. The model uses a combination weighting method combining subjective and objective, which balances the evaluation error caused by a single weighting method. Considering the correlation between indexes, we put forward the security evaluation index system for blockchain system based on the core framework of blockchain. Finally, the grey clustering evaluation is used to determine the security evaluation level of the blockchain system. Through example verification, it is proved that the model has good usability, which provides useful model support for the security evaluation of the blockchain system.

Acknowledgment

This research is supported by the National Key R&D Program of China under Grant (No. 2019YFB2102400)

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System[J]. Social Science Electronic Publishing, 2008.

[2] Wood G . Ethereum: a secure decentralised generalised transaction ledger. 2014.

[3] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the thirteenth EuroSys conference. 2018: 1-15.

[4] Engelhardt M A . Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector[J]. Technology Innovation Management Review, 2017, 7(10):22-34.

[5] ZHU Yan, ZHANG Yi, WANG Di, QIN Bo-han, GUO Qian, FENG Rong-quan, ZHAO Zhang-jie. Research on blockchain evaluation methods under the classified protection of cybersecurity[J]. Chinese Journal of Engineering, 2020, 42(10): 1267-1285.

[6] Ye CC, Li GQ, Cai HM, Gu YG. Security detection model of blockchain. Ruan Jian Xue Bao/Journal of Software,2018,29(5):1348−1359 (in Chinese).

[7] QIN Chaoxia, GUO Bing, SHEN Yan, et al. Security Risk Assessment Model of Blockchain[J]. Acta Electronica Sinica, 2021, 49(1): 117-124.

[8] SONG YinChun,NING Xiaoya. Blockchain technology risk assessment and control [J]. Finance and accounting monthly,2021(14):124-130.

[9] Zhihong Tian,Bailing Wang,Zhiwei Ye,Hongli Zhang. The Survey of Information System Security Classified Protection[A]. Intelligent Information Technology Application Association.Electronics and Signal Processing （EEIC 2011 LNEE V2） [C].Intelligent Information Technology Application Association, 2011:6.

[10] Mingxiao D , Xiaofeng M , Zhe Z , et al. A review on consensus algorithm of blockchain[C]// 2017:2567-2572.

[11] Sekiguchi K , Chiba M , Kashima M . The Securities Settlement System and Distributed Ledger Technology[J]. Bank of Japan Research Laboratory Series, 2018.

[12] Li C, Liu W, Cao Y, et al. Method for evaluating the importance of power grid nodes based on PageRank algorithm[J]. IET Generation, Transmission & Distribution, 2014, 8(11): 1843-1847.

[13] ZUO J X, GUO Z Y, ZHANG J, et al. Security evaluation method for confidential and stable complex systems[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 58-65.

[14] LUO Ning,HE Molin,GAO Hua,et al.Comprehensive evaluation method for a distribution network based on improved AHP-CRITIC combination weighting and an extension evaluation model[J].Power System Protection and Control,2021,49(16):86-96

[15] Lai C, Chen X, Chen X, et al. A fuzzy comprehensive evaluation model for flood risk based on the combination weight of game theory[J]. Natural Hazards, 2015, 77(2): 1243-1259.

[16] Guo Z, Lu Y, Tian H, et al. A security evaluation model for multi-source heterogeneous systems based on IOT and edge computing[J]. Cluster Computing, 2021: 1-15.