Computers, Materials & Continua CMC, vol.61, no.2, pp.677-686, 2019

Research on Architecture of Risk Assessment System Based on Block Chain

Yang Zhao[1] , Shibin Zhang[1, *], Min Yang[1], Peilin He[1] and Qirun Wang[2]

Abstract: The risk assessment system has been applied to the information security, energy, medical and other industries. Through the risk assessment system, it is possible to quantify the possibility of the impact or loss caused by an event before or after an event, thereby avoiding the risk or reducing the loss. However, the existing risk assessment system architecture is mostly a centralized architecture, which could lead to problems such as data leakage, tampering, and central cheating. Combined with the technology of block chain, which has the characteristics of decentralization, security and credibility, collective maintenance, and untamperability. This paper proposes a new block chain-based risk assessment system architecture and a consensus mechanism algorithm based on DPOS improvement. This architecture uses an improved consensus mechanism to achieve a safe and efficient risk assessment solving the problem of data tampering in the risk assessment process, avoiding data leakage caused by improper data storage. A convenient, safe and fast risk assessment is achieved in conjunction with the improved consensus mechanism. In addition, by comparing existing risk assessment architecture, the advantages and impacts of the new block chain-based risk assessment system architecture are analyzed.

Keywords: Risk assessment system architecture, block chain, decentralization.

1 Introduction

At present, there are few studies on the structure of risk assessment models, and the existing risk assessment structures are mostly based on a centralized structure. In the centralized structure, a risk assessment center receives the risk assessment data and calculate the result. Once the risk assessment center is attacked, it is easy to cause data leakage, tampering, and service stoppage. Moreover, it is difficult to forensics and review, if the risk assessment center cheats.

The emergence of block chain has changed this situation. In terms of data storage, the block chain architecture has decentralized, high security and privacy protection that makes it suitable for storing and protecting important private data, in data authentication, the block chain is jointly verified and recorded by the consensus nodes, so that the data cannot be falsified and forged [Yuan and Wang (2016)]. This paper proposes a new block

[1] Chengdu University of Information Technology, Chengdu, 610225, China.

[2] University of Hertfordshire, Hertford AL10 9AB, UK.

[*] Corresponding Author: Shibin Zhang. Email: cuitzsb@cuit.edu.cn.

chain-based risk assessment system architecture. The main features of the architecture are as follows:

1. Assessment and check node: The risk assessment agencies are ranked according to the credit value. The top 101 risk assessment agencies acts as a risk assessment node, and the 20th place after 101 as the check node. They conduct risk assessments under the coordination of the DPOS consensus mechanism.
2. Risk assessment data storage structure: this paper proposed a storage structure that use the block chain, and stores the Hash value of the data into the block chain. The Hash value of the data can be used to verify the authenticity of the original value in the database, and the Merkle root can quickly locate the data location.
3. Distributed database: The original value of the data is encrypted and stored in the database, reducing the block chain storage pressure.

The content of this paper is arranged as follows: Section 1 gives an overview of the of the risk assessment system architecture. Section 2 introduces the research status of the risk assessment system architecture. Section 3 presents the entire block chain based risk assessment system architecture. Section 4 compares the architecture. Section 5 presents a summary and outlook on the work of this paper.

2 Related works

The risk assessment system architecture is wildly used in computer science [Kun (2016); Wangen, Hallstensen and Snekkenes (2017)], economics [Yang, Li, Ji et al. (2001); Zhong, Peng and Kou (2010); Saha, Bose and Mahanti (2001)], energy environment [Zhang, Duan and Liu (2014); Gao, Xu, Liu (2014); Chuvieco, Aguado, Yebra et al. (2010)], medical health [Ding, Zhao and Wang (2018); Imperiale, Yu, Monahan et al.(2017); Ma, Liu and Chen (2014)] and other disciplines. Take the information security industry as an example, information security risk assessment has a history of more than 30 years. As early as the 1970s and 1980s, a risk assessment system and a series of standard systems and technical systems were established to ensure the authority and notarization of the evaluation result [Feng, Zhang and Zhang (2004)]. However, most of the research are based on the innovation and improvement of risk assessment algorithms and few scholars have improved based on the risk assessment architecture. Therefore, the current risk assessment system architecture is mostly based on a centralized structure (see Fig. 1).

Figure 1: Centralized risk assessment framework

2.1 Blockchain definition and structure

The definition of block chain is roughly divided into two types. The narrow sense block chain refers to decentralized node shared data book. The generalized block chain refers to the use of chain-encrypted structures to store and verify data, the distribution nodes to generate and update data under the consensus mechanism, and a decentralized structure for operating data using programmable scripts (smart contracts).

A block chain is a chained block structure composed of different blocks. The block includes the block header and the block body (see Fig. 2).

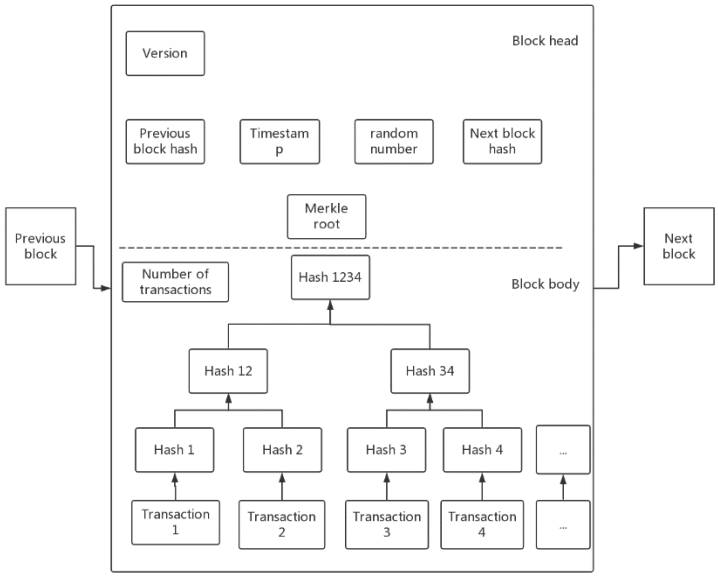

Figure 2: Block structure of Block chain

The block header includes the current block version number, the previous block address, the target hash value of the current block, the timestamp, the random number for the POW consensus mechanism and the Merkle root. Each block stores information about the previous block, therefore modifying the value of one block affects all subsequent blocks, so the data of each block cannot be falsified.

The block body consists of the number of transactions, the merkle tree, and the transaction data. The Merkle tree is a data structure based on a hash function. Its characteristic is that the value of each non-leaf node is the hash value of its leaf node. A hash function is an algorithm that through input of arbitrary length produces a fixed-length output and different inputs will have different outputs. The hash function is also a tone-way function, that is, it is easy to calculate the hash of the data, but it is difficult to calculate the original data by the hash value. Such a data structure can be used in the block chain to verify that the data has been tampered with, or that the transmission is incorrect. All data in the block body is generated by the hash process of the merkle tree. A Merkle root is stored in the head of the block chain.

2.2 Blockchain share authorization certificate (DPOS) consensus mechanism

The DPOS consensus mechanism is an improved POS consensus mechanism. Its idea is similar to "board decision making". It is considered to be a more effective, more decentralized, and more flexible consensus mechanism. All nodes in the block chain will vote for 101 stock representatives and stock representatives record block in turn. Each node can vote freely according to the performance of the representative node to select the equity representative [Yuan and Wang (2016); Yuan, Ni, Zeng et al. (2018)]. This reduces the number of recording nodes in the block and increases the recording efficiency of the block. Its consensus mechanism is as follows:

1. The node is selected by all nodes to vote, and the node with the highest number of votes and willing to be the representative node is elected as the representative node. Representing the node to record the block in turn, after receiving the book, it will get a certain reward.
2. If the representative node is erroneously recorded, or if the signing of the block is missed, then the next block is used for accounting. The representative node that missed the billing will be marked, and the next round of voting will likely be thrown by the remaining nodes.
3. The weight of voting for all shareholder nodes is determined by the number of digital currencies in the current block chain owned. That is to say, the shareholder node with more digital currency has a larger proportion of votes.
4. Each shareholder node uses its public key as an identifier in the block chain.

3 Decentralized risk assessment system architecture

The risk assessment system architecture consists of many components (see Fig. 3).

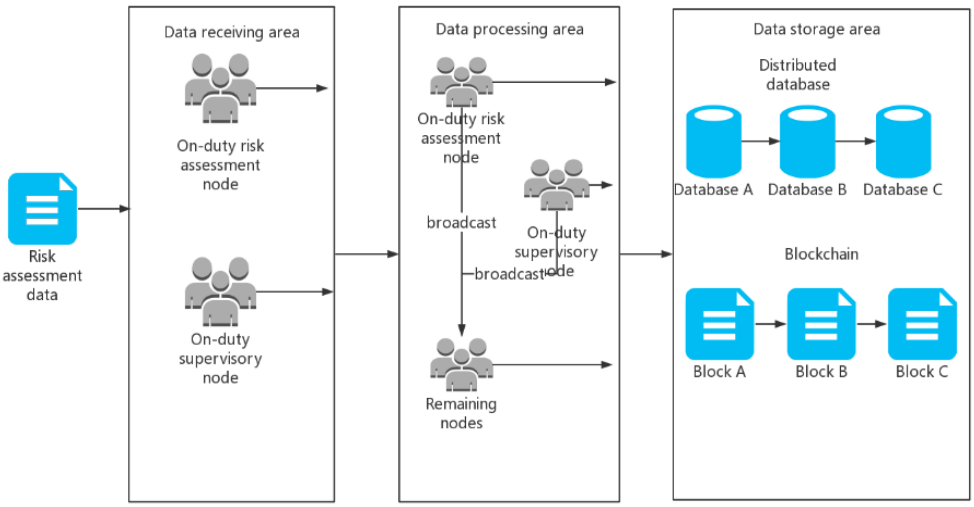

Figure 3: Risk assessment system architecture

The new risk assessment system architecture is divided into three parts, data receiving area, data processing area and data storage area according to different functions:

1. Data receiving area: On-duty risk assessment node and supervisory node receive risk assessment data.
2. Data processing area: Some nodes conduct risk assessment, some nodes supervise the risk assessment results, and the remaining nodes record the risk assessment results.
3. Data storage area: The data storage area is composed of a distributed database and a block chain, and the distributed database stores specific dat.
4. A and risk assessment results. The block chain stores a Hash value of data.

The traditional centralized risk assessment system architecture has problem that risk assessment results and risk assessment data have been tampered, and inefficiencies are assessed. Therefore, a block chain-based risk assessment structure is designed, which can effectively use the risk assessment node to achieve decentralized, safe and fast risk assessment. Due to the large amount of data, the risk assessment data is encrypted and stored by the distributed database, and the Hash value of the risk assessment data is stored in the Blockchain. This architecture Ensure the authenticity of the data while saving storage space (see Fig. 4).

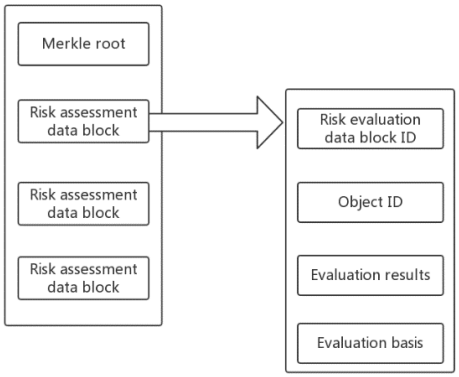

Figure 4: Block structure

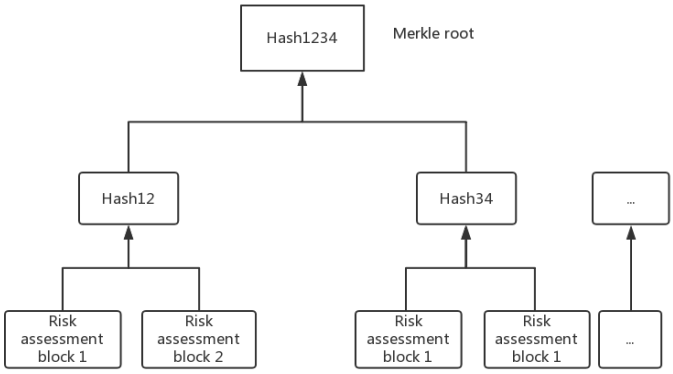

Figure 5: Merkle tree structure

3.1 Risk assessment data block

The risk assessment data block includes the data block ID, the object ID, the evaluation result, and the evaluation basis. The object ID is the identity of the evaluation object, and the evaluation result is the object risk value obtained after the risk assessment, and the evaluation basis includes the object risk assessment data and the algorithm identifier used. Due to the large amount of data in the object risk assessment, the hash value of the object risk assessment data is stored in the risk assessment data block. This can save both storage space and ensure the authenticity of object risk assessment data in a distributed database.

3.2 Risk assessment node, result check node and improved DPOS algorithm

The risk assessment process is based on an improved DPOS consensus algorithm. First, the top 101 risk assessment agencies are selected as risk assessment nodes. The risk assessment data is received in turn and the risk assessment algorithm is used to evaluate the risk of the object. The 20th place after 101 is responsible for using the risk assessment algorithm to verify the results of the assessment nodes. After the verification is successful, the data will be anchored into the block chain. After successfully anchoring the block chain, the assessment nodes and the check node will receive a certain credit score. If the risk assessment node does not complete the risk assessment or the evaluation result error within the specified time, it will be deducted a certain credit score and evaluated by the next risk assessment node. The verification node does not complete the verification of the result provided by the risk assessment node within the specified time or performs the error verification. The cheating will deduct credit points and re-verified by the next verification node. The risk assessment agency will be re-ranked according to credit scores every 30 days. Nodes ranked after 101 will be kicked out of the risk assessment node group, and those ranked after 131 will be kicked out of the check group. By introducing credit scores, the enthusiasm of each node can be fully mobilized, and the number of credit scores will affect the social assessment of the risk assessment agency. The specific process of risk assessment node and result check node is as follows:

1. Risk assessment data received by the shift risk assessment and results check nodes
2. The shift risk assessment node calculates the risk data utilization risk assessment algorithm, and obtains the results and broadcasts them.
3. After the verification node receives the broadcast, the risk assessment algorithm is used to derive the risk assessment result. The result is compared with that received by the broadcast. If the comparison result is the same, the correct broadcast is verified, otherwise, the broadcast is checked incorrectly.
4. The remaining nodes will record only after receiving the correct broadcast. Otherwise the record fails.
5. If successful, return to Step 1. If the record fails, search for the broadcast record, if there is no broadcast, deduct the credit value of the broadcast node that should broadcast. If the broadcast is complete, the credit value of the risk assessment node is deducted. The risk assessment is repeated by the next round of shift nodes.

Since all the evaluation data and results are stored in the block chain, if the check node cheats, the risk assessment node can appeal the result.

3.3 Risk assessment data query and verification

In order to protect the privacy of the user, all the raw data of the risk assessment is encrypted and stored in a distributed database. The fields stored include number, Merkle root, object ID, evaluation result, evaluation data, algorithm identification, risk evaluation data block ID.

The distributed database provides the user with a query interface, and the user can query the result of the risk assessment through the ID. The specific process is as follows:

1. The user initiates a query request to the query interface.
2. Interface to authenticate user identity.
3. Return Merkle root to legitimate users, evaluation results, behavior data, algorithm ID
4. The user finds a certain block in the block chain through the Merkle root and risk evaluation data block ID, and extracts the data Hash value in the block.
5. Compare the data Hash value in the database with the data Hash value in the block.
6. Under the premise that the behavior data is correct, the algorithm ID is used to find the corresponding algorithm, and the data and algorithm are used to calculate the risk assessment result, and then compared with the results in the database.

4 Analysis and comparison with traditional risk assessment

Blockchain structure with decentralization, timing sequence data, collective maintenance, programmable and secure. There is a risk assessment center in the traditional risk assessment system, and all risk assessment data is processed by a center, which is a typical centralized structure. The risk assessment system of the centralized structure has a series of problems that can be solved by the risk assessment system of the block chain structure. Specific problems and solutions are shown in Tab. 1.

Table 1: Problems and solutions

Type	Problems	Solutions
Data identification	The evaluation of data by a center does not guarantee the authenticity of the evaluation results. There may be a center to tamper with the data	Multiple nodes simultaneously assess risk and stored in a block chain that cannot be tampered with.
	The review is difficult because of the data is processed by a center f-rom the receipt of the results. It is difficult to find evidence by the center to cheat.	All nodes have the same data for easy review.
Data storage	Once the evaluation center is attacked, a large amount of data will	All nodes have the same data, and even if one node

be invalidated.	receives an attack, the remaining node data will not be affected.
The entire evaluation system will stop working when the center is down.	Multiple nodes have the ability to evaluate at the same time

Tab. 2. Compares the architecture of the risk assessment system in the literature of various industries with the structure of the risk assessment system.

Table 2: Compare several risk assessment frameworks

Type	**Architecture of the risk assessment**	**Blockchain**
Energy environment	fire risk assessment [Chuvieco, Aguado, Yebra et al. (2010)]	No
	Power System Static Security Online Risk Assessment [Zhu, Luo and Duan (2013)]	No
Medical health	CRC [Ding, Zhao and Wang (2018)]	No
	Venous thromboembolic risk assessment system architecture [Hong and Yang (2014)]	No
Economics	Loan risk assessment [Saha, Bose and Mahanti (2016)]	No
	ISRA [Wangen, Hallstensen and Snekkenes (2017)]	No
Computer science	Blockchain-based risk assessment system architecture	No
		Yes

5 Conclusion

Nowadays, block chain is widely applied to information security, education, medical, financial and other industries. The block chain-based risk assessment system architecture proposed in this paper can optimize the structure of the existing risk assessment system architecture, and incorporate the idea of decentralization to make risk assessment more efficient, safe, and fair. However, the decentralized architecture of risk assessment system may encounter problems in the implementation, and it needs to be continuously

Acknowledgement: This work is supported by the National Key Research and Development Project of China (No. 2017YFB0802302), the National Natural Science Foundation of China (No. 61572086, No. 61402058), the Innovation Team of Quantum Security Communication of Sichuan Province (No. 17TD0009), the Academic and

Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), the Application Foundation Project of Sichuan Province(No.2017JY0168), the Key Research and Development Project of Sichuan Province (No. 2018TJPT0012), the Science and Technology Support Project of Sichuan Province (No. 2016FZ0112, No. 2018GZ0204).

References

Chuvieco, E.; Aguado, I.; Yebra, M.; Nietoa, H.; Salasa, J. et al. (2010): Development of a framework for fire risk assessment using remote sensing and geographic information system technologies. *Ecological Modelling*, vol. 221, no. 1, pp. 46-58.

Ding, L. J.; Zhao, L. Z.; Wang, Y. (2018): Studying the health risk assessment model of Chinese colorectal cancer. Chinese *Journal of Prevention & Control of Chronic Diseases*, vol. 26, no. 5, pp. 325-338.

Duan, Y.; Zhang, B. H.; Liu, Y. F. (2014): Security risk assessment using fast probabilistic power flow considering static power-frequency characteristics of power systems. *International Journal of Electrical Power & Energy Systems*, vol. 60, no. 60, pp. 53-58.

Feng, D. G.; Zhang, Y.; Zhang, Y. Q. (2004): Summary of information security risk assessment. *Journal of Communications*, vol. 25, no. 7, pp. 10-18.

Gao, J. P.; Xu, Z. S.; Liu, D. L. (2014): Application of the model based on fuzzy consistent matrix and AHP in the assessment of fire risk of subway tunnel. *Procedia Engineering*, vol. 71, no. 16, pp. 591-596.

Gaute, W.; Christoffer, H.; Einar, S. (2017): A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, vol. 17, no. 6, pp. 681-699.

Hong, Y. L.; Yang, X. M. (2014): Progress in clinical application of venous thromboembolic risk assessment system architecture. *Chongqing Medical*, vol. 35, no. 1, pp. 4829-4841.

Imperiale, T. F.; Yu, M.; Monahan, P. O.; Stump, T. E.; Tabbey R. et al. (2017): Risk of advanced neoplasia using the national cancer institute's colorectal cancer risk assessment tool. *Journal of the National Cancer Institute*, vol. 109, no. 1, pp. 171-181.

Ma, H. M.; Liu, X. Q.; Chen, H. Y. (2014): Urban mosquito disease risk research based on risk assessment matrix method. *Chinese Journal of Disease Control*, vol. 18, no. 9, pp. 887-890.

Saha, P.; Bose, I.; Mahanti, A. (2016): A knowledge based scheme for risk assessment in loan processing by banks. *Decision Support Systems*, vol. 84, no. 1, pp. 78-88.

Yang, B.; Li, X. L.; Ji, H.; Jing, X. (2001): An early warning system for loan risk assessment using artificial neural networks. *Knowledge-Based Systems*, vol. 14, no. 5, pp. 303-306.

Yuan, Y.; Ni, X. C.; Zeng, S.; Wang, F. Y. (2018): Development status and prospects of block chain consensus algorithm. *Journal of Automation*, vol. 44, no. 11, pp. 86-100.

Yuan, Y.; Wang, F. Y. (2016): Development status and prospect of block chain technology. *Journal of Automation*, vol. 42, no. 4, pp. 481-494.

Zhang, K. (2016): *Research on Information Security Risk Assessment Based on AHP and BP*. Hebei University of Engineering.

Zhong, X.; Peng, Y.; Kou, G. (2010): A dynamic self-adoptive genetic algorithm for personal credit risk assessment. *International Conference on Information Sciences and Interaction Sciences*, pp. 711-716.

Zhu, Y. H.; Luo, Y.; Duan, T. (2001): Static security online risk assessment of power system based on real-time evaluation model of transmission line. *Power automation equipment*, vol. 34, no. 7, pp. 150-156.