Threat Intelligence Sharing Model and Profit Distribution Based on Blockchain and Smart Contracts

Huiyang Shi[1], Wenjie Wang[2], Ling Liu[1,2], Yue Lin[1,2], Peng Liu[1], Weiqiang Xie[1,2], He Wang[2], and Yuqing Zhang[1,2(✉)]

[1] National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 100093, China
{shihuiyang,zhangyq}@ucas.ac.cn, {liul,lil,luip, xiewq}@nipc.org.cn

[2] School of Cyber Engineering, Xidian University, Xian 710071, China
wangwj@ucas.ac.cn, hewang@xidian.edu.cn

Abstract. The new generation of cyber threat attacks has gradually shifted to APT attacks. The attack technology is complex and changeable. The sharing of threat intelligence can improve network defense capabilities. However, privacy issues, trust issues, and sharing mechanisms make the sharing process inefficient. The characteristics of decentralization, anonymity, and non-tamperability are suitable for solving problems in threat intelligence sharing. In this paper, we propose a new threat intelligence sharing model based on the alliance chain in blockchain technology: CITAShare, which includes a distributed architecture database, and the update of data relies on the consensus algorithm. We build the model to implement the process of sharing threat intelligence through smart contracts and solved the privacy issues in the sharing process consequently. Additionally, we find that current intelligence sharing platforms often lack an effective incentive mechanism, so we propose a profit distribution method based on improved Shapley value to motivate the sharers. Our scheme guaranteed rationality in the operational perspective by using the smart contract in the specific distribution process.

Keywords: Threat intelligence sharing · Smart contract · CITA · Shapley value · Profit distribution · Blockchain · Privacy protection

1 Introduction

The main challenges in threat intelligence sharing are justice and security [1]. Fairness lies in how to establish a suitable reward mechanism to improve sharing enthusiasm. Security refers to protecting the organization's private data from malicious use by competitors. There are the following problems in TI I (Threat Intelligence) sharing: The enterprise can not accurately judge what threats are caused by the IOC of generated data; The quality of TI is not high, and the availability is not vital; The data privacy is poor, and the sharing willingness is low lacking of the corresponding incentive mechanism. Table 1 shows the issues and solutions.

Q. Liu et al. (Eds.): *Proceedings of the 11th International Conference on Computer Engineering and Networks*, LNEE 808, pp. 645–654, 2022.
https://doi.org/10.1007/978-981-16-6554-7_70

Table 1. Issues and solutions of cyber threat intelligence sharing

Issues of Cyber Threat Intelligence Sharing	Exisiting solutions
Centralized organization management	Cloud Platform/CYBEX/
Lack of trust mechanisms	Blockchain-Based frame
The data storage	Physical unclonable functions
Data access control	Cloud storage/Off-chain storage ACL rules
Privacy and security	Blind Signature/Multiple channels
The incentive mechanisms of data sharing	Shapley value/game theory

This paper proposes a sharing model based on blockchain technology for the following considerations: decentralization and non-tampering modification in the blockchain solve the performance and mistrust problems in traditional centralized systems [2]. There has been much application of blockchain in business and medical treatment, but there is not much research on the combination of threat intelligence sharing and blockchain. In threat intelligence sharing, there are problems with protecting data privacy and risk control [3]. The decentralization of blockchain technology and account anonymity can solve those problems. Figure 1 shows the application in threat intelligence. To summarize, our contributions are the following:

- The paper proposes a new TI sharing model based on CITA architecture. The intelligence sharing functions are realized through smart contracts: the node registration, data on-chain, data reading, and data query.
- The research proposes using the off-chain storage based on local consensus in the CITA architecture to solve the threat intelligence's privacy security.
- We solve the problem of profit distribution by improved Shapley value and blockchain. It also proposes that when we share TI, the payment fees are based on management departments' assessment of TI. The proposed scheme is reasonable and practical.

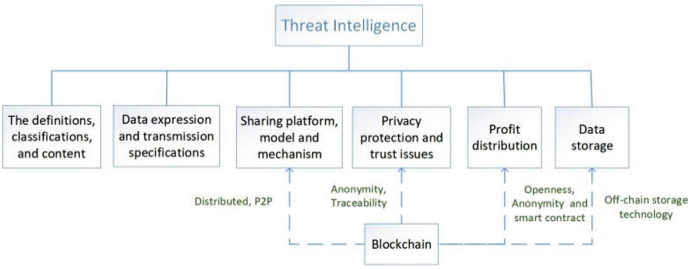

Fig. 1. Application of blockchain in threat intelligence

The rest of the paper is as follows: the second part introduces the related work. The third part proposes a new model based on CITA architecture and solves the privacy security. We resolve the distribution of benefits with improved Shapley and smart contracts in Sect. 4. The last part summarizes the article and discusses future work.

2 Related Works

In recent years, academics have conducted in-depth research on threat intelligence sharing models. In terms of sharing models and sharing mechanisms, they proposed a sharing model based on the g-SIS model, trust classification method, distributed deployment structure. We thoroughly investigated the relevant literature on blockchain technology in threat intelligence sharing in the past five years, found that there are still many unresolved issues.

The paper introduces a new model for threat sharing based on blockchain, which used the Hyperledger Fabric alliance chain to perform a test platform [4]. The node registration, data accounting, analysis transaction, and early warning response function are realized based on the new model of blockchain [5]. [6] has studied the EMRShare framework promoting the sharing and management of electronic medical records and implemented a prototype system. The paper [7] highlights an innovative framework based on blockchain to protect IoT data's privacy and security in a smart city environment.

[8] The paper proposes a DrivMan solution based on PUF and blockchain to achieve trust management and data sharing in a vehicle-mounted self-organizing network. [9] introduced an analysis of network attacks and defenses based on Stackelberg games, and verified through numerical results obtained from a large number of simulations. [10] emphasized the incentive mechanism of medical data sharing, combined blockchain technology and Shapley distribution. [11] introduced the concept of risk coefficient in cyber threat intelligence sharing, and improved Shapley value to make the profit distribution more fair and reasonable. [12] proposed an evolutionary game model for threat intelligence sharing, allowing companies to independently decide whether to participate in CYBEX framework and whether to share threat intelligence.

3 New Sharing Model

3.1 Comparative Discussion

The CITA model solves two major problems in intelligence sharing: trust issues and privacy protection. In this architecture, members have access mechanisms. The user's transaction authority is managed through complex permissions management, including sending transactions, creating contracts, and contract method invocation authority, etc. And it protects privacy as well. Sidechain technology is introduced to solve privacy. Besides, the CITA architecture provides users with free service models and support charging mode, which can better control the user's use of system resources. One of the representatives in the alliance chain is the Hyperledger Fabric project, which was designed by IBM. The comparison framework is shown in Table 2. The consensus mechanism in this architecture uses a Byzantine fault-tolerant tender mint algorithm to

reduce the consensus time and improve the system throughput. It uses CompactBlock technology to compress the size of the consensus block, improve network bandwidth utilization. The contract is easy to deploy, call, and upgrade.

Table 2. Hyperledger fabric VS CITA

Architecture	Consensus mechanism	Smart contract	Economy	Participants
Hyperledger Fabric	Kafka/raft	Go/Javascript	Free mode	Endorsers Orderers non-endorsing peers
CITA	CITA-BFT	Solidity	Free mode/charing mode	Consensus node common node

3.2 System Design Based on CITA Framework

CITA is the first blockchain framework that uses microservices architecture. It provides a functional blockchain architecture for TI sharing between the corporates, and We intensely discuss its contribution to data management. For example, in supply chain finance, the architecture is used to improve security, realize the transparency of the whole process to the world, and decentralized books to complete automatic payment, thus reducing human mistakes and significantly improving efficiency.

The network processing capacity is equivalent to the processing power of a single node. Through microservices, each node is decoupled into six microservices: Consensus, Remote Procedure Call Protocol (RPCP), Executor, Auth, Network and Chain. Various components exchange information through a message bus. Chain and Executor are independent of each other, which improves transaction processing performance. A role-based permission control system is also implemented to assign permissions to participate organizations by providing node and user identity verification to exclude unauthorized nodes or organizations [13]. Besides, to protect user privacy, the architecture offers support for private transactions, as is shown in Fig. 2.

3.3 Privacy Issues

CITA proposes a privacy scheme based on partial consensus off-chain storage technology. It stored private data off the chain after separating it from other intelligence. The data's hash summary is saved in the block, and access to off-chain data is authorized when it is required. The transaction package data only be transmitted and processed between the parties involved in the transaction, and will not broadcast to the entire network. The private transaction data is only saved to the relevant node which has the decrypted private

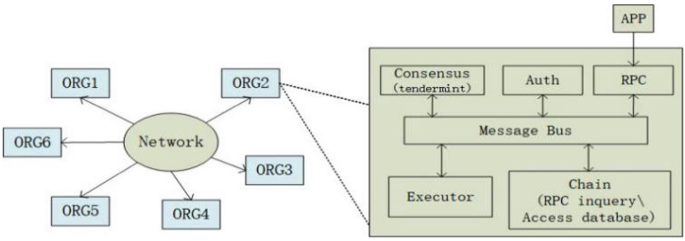

Fig. 2. Network architecture based on CITA

key. The corresponding node decrypts before executing the transaction. The transaction data will not be sent to remote nodes, so the transaction data will never be leaked [14].

We use the nodes to represent the departments in the organization. Node 1 in ORG 1 can only share with node 5 in ORG 2 and node 9 in ORG 4. Other nodes outside the three departments do not have access Authority, we realize threat intelligence sharing among the three departments through partial execution technology. The encrypted data is stored through an off-chain storage mechanism. The intelligence hash summary is packaged in the block. The node with the decrypted private key and peer public key can only access the complete data after decrypting locally. Nodes without access rights can receive the hash value of the intelligence. Nodes cannot obtain off-chain data without decrypting the private key. This method realizes privacy security issues. As is shown in Fig. 3.

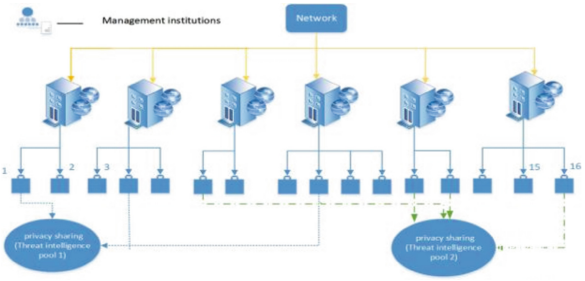

Fig. 3. Blockchain-based mechanism for Privacy protection

We use the following steps to explain how node 1 in ORG 1, node 5 in ORG 3, and node 9 in ORG 4 achieve private data:

- After the threat intelligence of node one is submitted to the blockchain network, the content is encrypted using a symmetric key, and then we hash the encrypted ciphertext;
- The paper uses an off-chain storage mechanism to store threat intelligence and put the hash summary on the chain;
- After packaging the encrypted data and the symmetric key, it is transmitted to the shared node through a point-to-point protocol;
- Node 5 or Node 9 decrypts with the local private key and node one public key. And we obtain threat intelligence through off-chain access technology.

3.4 Implementation of Sharing Platform Function

To illustrate how we can share threat intelligence under the CITA architecture, we divide this process into four main modules: node registration, data on-chain, data reading, data query. And after smart contract deployment, it generates contract addresses and accounts. When we implement the functional module, we interact with the smart contract through the interface, and the smart contract is programmed with Solidity [15].

Node Registration. When the organization tries to join the threat block as a node, it needs to apply for node registration with the administrator in the architecture. First, create and initialize a founding block, then start the blockchain network. The node completes the configuration work. And then, we create an account and define the user registration function in the smart contract. After the registration is completed, the blockchain will store user information.

Data Upload. The organization will upload the data after joining the node. The uploaded message includes the name, content, number of the submitter organization. After the upload is completed, it will be stored in the blockchain and turn the number. We define the upload function to post data to achieve the data upload.

Data Reading. This module realizes that the buyer makes purchases and reads the data from the blockchain. We define the acquisition function in the smart contract. First, use the MakeKey method of the SmartData class to retrieve the key of the current data. Finally, we use the update Data method to update confidential data.

Data Query. Transaction intelligence is stored in the blockchain, and the data will not tamper. If threat intelligence needs to be deleted, it can be removed through an algorithm. However, the deleted intelligence is in the block on the traceability of blockchain. It can still be found through historical records, which guarantees the trust of the data contribution.

4 Profit Distribution

4.1 Benefit Distribution Process

The conventional method does not describe the details of the intelligence-sharing process, such as trust issues and privacy issues between organizations, which severely restricts the organizations' enthusiasm to share intelligence [16]. Decentralization in blockchain technology solves the trust problem in traditional techniques. Cryptography solutions such as zero-knowledge proof and off-chain storage mechanism solve sensitive intelligence privacy and security issues. Therefore, we use blockchain technology to solve the problem of benefit distribution for threat intelligence sharing. Among them, smart contract technology realizes the automatic placement of incentives. The Shapley value method for income distribution among the people solves the fairness of sharing intelligence among organizations. Figure 4 depicts the benefit distribution model.

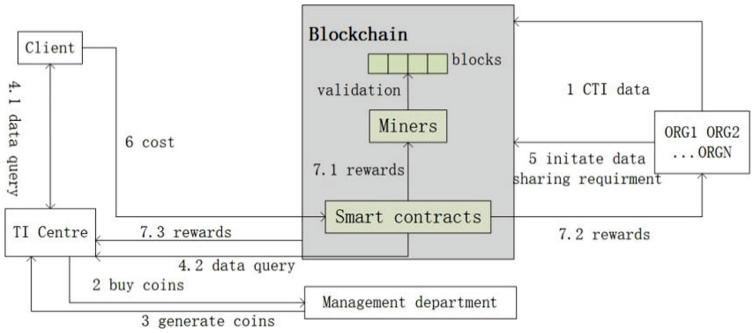

Fig. 4. Reward mechanism based on shapley and smart contracts

In the threat intelligence sharing model based on blockchain technology, we divide the blockchain system participants into three categories: intelligence analysis center, alliance sharing members, and miners. The client is on the demand of threat intelligence. After receiving the information, the intelligence analysis agency analyzes and evaluates the information through technical means, and then provides it to the client. Shared members are providers of data. Miners record the data transmission on the blockchain. Participants are defined as: $\mathrm{N} = \mathrm{C} \cup \mathrm{M} \cup \mathrm{U}$, which represents an intelligence analysis agency. $M = \{M_1, M_2, \cdots, M_k\}$ representing a group of miners, and $O = \{O_1, O_2, \cdots, O_k\}$ represents a set of data providers. ORG 1, ORG 2… ORG N shared information is stored on the blockchain, and sensitive data is stored off-chain through an off-chain storage solution. The client can be an organization member or a non-organization member. Administrators perform permission operations on it, and members of the alliance are authorized to access shared information. If members outside the alliance gain access, the access cost is higher than that of the alliance members. This mechanism also primarily promotes members to join the alliance. To obtain access to information, members must first purchase virtual currency from the management department through legal tender. Alliance revenue comes from the client's access cost. After the client makes the payment, the intelligence-sharing request is responded to, and the smart contract is executed. The distribution of benefits will be distributed among miners and alliance members, and intelligence analysis centers. The analysis center processes the shared intelligence of the alliance. Miners pack the data on the blockchain into blocks, and the more shared intelligence, the more valuable, the more revenue the analysis center and miners get [17].

We define $\varphi(O_i)$ as the Shapley value income allocated to ORG i, $v(O)$ is the total revenue allocated to the shared organization. $\varphi(M_k)$ is defined as the Shapley value income allocated to M_k. P_k is defined as the probability of miner M_k. The probability is related to the consensus algorithm. This article uses the tendermint algorithm. $\varphi(M_k)$ is proportional to P_k and $v(N)$, $\forall M_k \in M$, $v(N)$ is the total revenue. $\varphi(C_j)$ is the revenue of the information center, $\varphi(C_j) = W * F_s * \mathrm{b}_k^s * V_s$.

In addition to using the Shapley value to realize the benefit distribution of threat intelligence sharing, sharing organizations and ordinary users need to pay the fee to a third-party organization when they access shared intelligence. The cost depends on the

assessment of intelligence by the third-party organization. The evaluation includes three aspects: threat intelligence impact, universality, and whether access users are among the sharing organizations. The effect of threat intelligence on the organization is divided into slight, intermediate, and advanced. Threat intelligence can lead to the leakage of crucial sensitive information or lead to DDOS attacks is in advanced scope. Universality considers the frequency of threat intelligence occurs. If the impact on threat intelligence and the frequency of the occurrence are high and the user does not belong to the sharing organization, then the payment fees are higher. We use this strategy to achieve the effect and fairness of TI sharing and promote the enthusiasm of threat intelligence sharing.

4.2 Implementation

To implement our proposed sharing model based on blockchain technology, we use the open-source blockchain specification under the CITA architecture to implement the benefit distribution. We experiment on a computer equipped with an Intel Core i5 1.6 GHz CPU, 8 GB RAM, and Ubuntu 18.04 operating system. The implementation process of the algorithm can be summarized as follows:

Buy the Coins. The client buys the coins, the token is used for trading or getting access to the threat information. It is similar to any other cryptocurrency. After the client pays, a third-party institution pays a specific token to the account. If the client does not have the requisite coins in his account, the transaction will fail.

Initiate TI Sharing Requirements. After receiving the request for intelligence sharing, the client can initiate the intelligence. The data owner will get the incentives after the intelligence sharing is committed.

Check if the Client is on the List. Check that the allowed sharing list of the matched information, and add the requester if the file is empty. If it is not empty, it will traverse whether the requester is already on the list. If it is, it will output. If not, it will be added to the list.

Gain Benefit Distribution

1) The allocation of miners traverses all miners first and traverses other nodes for each miner. If the node is normal, the count tmp_q is increased by 1. After going through a round, calculate $q+ = 1/tmp_q$. The final revenue of miners is $1/n * q$.
2) It traverses the league members in which it is located. Let S be the scale of the alliance and n be the size of the participant set. First, calculate $tmp_x = (\mathrm{s} - 1)! * (\mathrm{n} - \mathrm{s})!/\mathrm{n}!$. The relative contribution of tmp_con is equal to the alliance's contribution minus the contributions excluding the participant. calculate $x+ = tmp_{\mathrm{x}} * tmp\_con$. After traversing the alliance member, let S be the member's risk minus 1/n, that is the difference between the risk taken and the risk shared. Finally, we calculate the revenue of the organization.
3) The intelligence analysis centers first traverse all centers, and each independent center calculates the intelligence benefits of the center's three levels of low, middle, and high. Low-value information includes the presence or absence of network

information or network-based data: Hash, IP, and domain name. Medium-value intelligence consists of the traffic data transmitted by the network. High-value intelligence includes TTPS, malicious program detection and analysis data, incident classification intelligence, honeypot data, and passive traffic analysis data belong to this category.

If C_j reprents the service provided by Intelligence Analysis Center j, $\varphi(C_j) = W * F_s * b_k^s * V_s$ is the number of value intelligence services after the last distribution, V_S represents the intelligence value, and F_S represents the intelligence service cost. The benefits of medium-value intelligence are the same as those of high-value intelligence. Finally, the total revenue of the information center is equal to the sum of the revenue of the three types of value.

This paper realizes sharing and incentive mechanism of threat intelligence based on blockchain and smart contract. It solves the problems about data storagey, profit distribution and privacy. In the sharing architecture we designed, the data structure can be stored in the block and the transactions can be traced back. This platform describes the specific implementation of each functional module and gives the key algorithm. The sharing architecture is practical through simple platform test.

5 Conclusion and Future Work

This paper proposes a new TI sharing mechanism based on the blockchain technology CITA architecture Model, which solves threat intelligence privacy and storage problems. We also introduce the distribution of benefits based on smart contracts and improved Shapley value schemes. This distribution scheme incentivizes the sharing alliance to participate in intelligence sharing. The proposed model and benefit distribution plan are reasonable and practical.

In the future, We'll go deeper into the content of CTI and categorize them to improve the sharing efficiency. And we will also study the evaluation of the Opensource Threat Intelligence.

Acknowledgment. We are grateful to thank our anonymous reviewers for their insightful comments. This work is supported by National Key Research and Development Project (2018YFB0804701), National Natural Science Foundation of China (No. U1836210, No. 61572460).

References

1. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. **72**, 212–233 (2018)
2. Amofa, S., et al.: A blockchain-based architecture framework for secure sharing of personal health data, pp. 1–6 (2018)
3. Liu, X., Wang, Z., Jin, C., Li, F., Li, G.: A blockchain-based medical data sharing and protection scheme. IEEE Access **7**, 118943–118953 (2019)

4. Homan, D., Shiel, I., Thorpe, C.: A new network model for cyber threat intelligence sharing using blockchain technology, pp. 1–6 (2019)
5. Vakilinia, I., Tosh, D.K., Sengupta, S.: Privacy-preserving cybersecurity information exchange mechanism, pp. 1–7 (2017)
6. Xiao, Z., et al.: EMRSHare: a cross-organizational medical data sharing and management framework using permissioned blockchain, pp. 998–1003 (2018)
7. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W.: PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Comput. Secur. **88**, 101653 (2020)
8. Javaid, U., Aman, M.N., Sikdar, B.: DrivMan: driving trust management and data sharing in vanets with blockchain and smart contracts, pp. 1–5 (2019)
9. Rawat, D.B., Njilla, L., Kwiat, K., Kamhoua, C.: iShare: blockchain-based privacy-aware multi-agent information sharing games for cyber-security. In: 2018 International Conference on Computing, Networking and Communications (ICNC) (2018)
10. Zhu, L., Dong, H., Shen, M., Gai, K.: An incentive mechanism using shapley value for blockchain-based medical data sharing (2019)
11. Xu, Z., Peng, Z., Yang, L., Chen, X.: An improved shapley value method for a green supply chain income distribution mechanism. Int. J. Environ. Res. Public Health **15**, 1976 (2018). https://doi.org/10.3390/ijerph15091976
12. Rutkowski, A., et al.: CYBEX: the cybersecurity information exchange framework (x.1500) **40**, 59–64 (2010)
13. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30 (2016)
14. Gai, K., Wu, Y., Zhu, L., Qiu, M., Shen, M.: Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inf. **15**, 3548–3558 (2019)
15. Pham, H., Le, T., Pham, T., Nguyen, H., Le, T.: Enhanced security of IoT data sharing management by smart contracts and blockchain, pp. 398–403 (2019)
16. Kassem, J.A., Sayeed, S., Marcogisbert, H., Pervez, Z., Dahal, K.: DNS-IDM: a blockchain identity management system to secure personal data sharing in a network. Appl. Sci. **9**, 2953 (2019)
17. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. **34**, 355–364 (2017)