DOI: 10.53469/wjimt.2025.08(07).02

Cyber Threat Intelligence Sharing Mechanism and Implementation Based on Blockchain Smart Contracts

Alexander Bilenko

School of Cyberspace Security, Udayana University, Denpasar 80232, Indonesia

Abstract: ***In an extremely open cyber environment, people are often exposed to multiple and complex cyber threats. In order to clean up the cyber environment, we need to study how to realize an efficient, intelligent and secure cyberthreat intelligence sharing mechanism, so as to rationally handle information threatening China's cybersecurity based on high synergy. Given the innovative development of blockchain technology, its peer-to-peer distributed trust management mechanism can form the secure transmission of network intelligence information. In addition, leveraging its traceability, tamper-proofing, self-maintaining and other advantages in this regard, making blockchain smart contracts a vehicle for building and operating cyberthreat intelligence sharing mechanisms a highly viable work plan. This paper focuses on analysis from the perspective of the applicability of blockchain smart contracts in the construction of cyberthreat intelligence sharing mechanisms, conceives the internal process of cyberthreat information sharing mechanisms based on blockchain smart contract, and makes further thoughts on the implementation of relevant mechanisms.***

Keywords: Cyber threat intelligence; Blockchain; A sharing mechanism.

1. INTRODUCTION

In the cyber world, threat intelligence information in the network cannot be ignored. Such information is characterized by randomness and secrecy, and can form negative effects such as terrorist threats to network users and malicious guidance, and also poses a threat to the healthy development of national society. The idea of building a network threat intelligence sharing mechanism based on blockchain smart contracts, This occurs in the context of China's overall awareness of intelligence fusion and sharing, and it must be achieved in the condition that it fully follows the characteristics of blockchain technology and is highly applicable to both the main and the object dimensions. Ding and Wu (2024) systematically reviewed self-supervised learning for ECG and PPG signals [1]. Complementing this, Restrepo et al. (2024) developed multimodal embedding alignment for healthcare in low-resource settings [2]. Natural language processing innovations include Yang et al.'s (2025) GAN-based text summarization combining transductive and reinforcement learning [3]. Industrial applications feature Xie and Chen's (2025) multi-agent system Maestro for manufacturing optimization [4]. System reliability research includes Zhu's (2025) RAID framework for anomaly detection in ad systems [5], Zhang's (2025) CrossPlatformStack for high-availability service deployment [6], and Hu's (2025) AdPercept for visual attention modeling in 3D ads [7]. Computer vision advances include Peng et al.'s (2024) domain-adaptive human pose estimation through representation aggregation-segregation [8]. Anomaly detection is furthered by Zhang et al.'s (2025) ML techniques for biomechanical big data [9], while healthcare AI features Wang's (2025) transformer-GNN hybrid RAGNet for arthritis risk prediction [10]. Enterprise solutions encompass Qi's (2025) generative AI framework AUBIQ for automated business intelligence [11], Fang's (2025) microservice-driven low-code platform for SME digital transformation [12], and Lin's (2025) product management approach to AI governance [13]. Foundational data techniques include Chen's (2023) data mining applications [14]. Computer vision research continues with Wang, Li, and Li's (2024) YOLOv8-based road car detection [15], while causal AI is advanced by Wang's (2025) targeted learning method for MNAR recommendation data [16].

2. APPLICABILITY ANALYSIS OF NETWORK THREAT INTELLIGENCE SHARING MECHANISM BASED ON BLOCKCHAIN SMART CONTRACTS

Cybersecurity threat intelligence is a collection of information that presents potential and immediate threats to organizations and institutions. In the process of intensifying cybersecurity offensive and defensive confrontation, there is a natural asymmetry between the offensive and the defensive sides, and cybersecurity threat intelligence sharing and utilization is a means to effectively improve the response capability and effectiveness of the protection

side. Based on blockchain networks, technologists utilize P2P networking technology to set up a distributed peer-to-peer network, initially build a peer-on-peer contract basis, and then introduce asymmetric cryptographic transmission algorithms that act as "security maintainers" in data transmission and access between nodes. Smart contracts are computer protocols that build contracts through computer code and execute them, which have the advantages of efficiency, detrustability, and automatic fulfillment. In terms of the security and confidentiality of network data storage, technicians set time stamps in the relevant network smart contract architecture and build chain data block structures so that their data can be traced and cannot be tampered with. One of the operational aspects of the network threat intelligence sharing mechanism is to consistently and collaboratively process data. To achieve this goal, technicians need to embed consensus mechanisms in smart contracts, so that they can be automated programming to ensure the portability and standardization of data processing (converged sharing) between nodes. A key issue running through the intelligence sharing process is the ability to form trust relationships and synergies among the blocks nodes. If blockchain smart contracts can solve this problem, then their applicability in the formation of cyber threat intelligence sharing mechanisms can be seen.

2.1 Applicability analysis of shared main body

From a macro perspective, the subjects under the cyberthreat intelligence sharing mechanism should include national, local and other levels cyberthreat agencies, government departments, social organizations, enterprise organizations, and the general public. Therefore, the structure of relevant sharing mechanisms requires a high level of integration of diverse subject relations, and the corresponding integration involves both the integration and sharing of intelligence assets among various departments at all levels of the state, and the vertical integration and sharing between intelligence assets from the state level to the people's level. Among them, the synergy mechanism and the trust mechanism will be the main drivers of the integration and sharing of intelligence assets. However, various types of intelligence sharing agents have different characteristics and different perceptions, and to avoid subjective competition and establish pure trust and synergy mechanisms cannot rely on conventional system establishment, verbal constraints, laws and regulations. This is where blockchain smart contracts come in handy. The technology can meet the high trust, high speed and flattening requirements of relevant mechanisms, and set up network links for the transmission of intelligence assets.

In the application of blockchain smart contracts, the subjective lack of trust of the participating nodes can be broken. It is based on P2P networking and asymmetric encryption transmission mechanism, and is not subject to the interference of subjective will, directly from point to point, so that the information barrier between the sharing subjects is broken, and information integration is realized. In simple terms, the integrated shared intelligence system under this technology simplifies the layer of intelligence transmission, thereby reducing the chance of related intelligence being tampered with and corrupted, thereby ensuring the security and transmission efficiency of intelligence assets. It can be seen that blockchain smart contracts can be applied to complex subjects under the cyber threat intelligence sharing mechanism.

2.2 Shared object applicability analysis

The object under the cyberthreat intelligence sharing mechanism is a variety of intelligence products and information transmitted, pooled and analyzed by different sharing subjects, which together constitute intelligence assets. These objects exist in the form of data during the operation of the sharing mechanism, and are highly prescriptive and highly maintained. Data information that can be used as cyber threat intelligence is generally closely related to national security issues and people's livelihood development issues. Therefore, objects need to be protected with high confidentiality during transmission, for example, subjects sharing information with each other should be set up permissions to retrieve and share information according to the size of the permissions; Intelligence assets should be consolidated into a large, standardized and rigorous database, stored permanently and maintained at a high level, so that information on these assets serves as the basis for interconnectivity among agents based on the intelligence sharing mechanism. In addition, the availability of object resources under cyberthreat intelligence sharing mechanisms comes from multiple sources and has been repeatedly validated in value, and should be explored. Thus, cyberthreat intelligence sharing mechanisms should also be able to dig deep into objects.

In the blockchain smart contract, asymmetric cryptography technology is embedded, which is able to secure intelligence subjects in transit state very well. Among them, the contract public key will serve as the basis for distinguishing the rights of different subjects, and those who hold the public key (nodes) can successfully parse the intelligence raw data. This enables the confidential transmission of the object's resources. At the same time, in smart contract programs, technicians can further set node permissions and functions, so that different nodes obtain and transmit intelligence data in different formats, thereby improving the portability of intelligence assets. In

addition, the application of the chain data block structure in the contract, as well as the application of consensus mechanism and Merkle hash tree verification mechanism, also make the validity and integrity of the intelligence object further guaranteed. It can be seen that the process of data asset management by blockchain smart contracts can be consistent with the maintenance of the characteristics of the intelligence object.

3. INTERNAL PROCESS OF NETWORK THREAT INTELLIGENCE SHARING MECHANISM BASED ON BLOCKCHAIN SMART CONTRACTS

Before the corresponding network threat intelligence sharing mechanism process is formed, each contract node shall unify the requirements analysis of the intelligence sharing business. A standardized and usable cyberthreat intelligence sharing mechanism can then be implemented by developing a process based on requirements and incorporating a strategy for converged sharing of cyberthreat messages into the contract script. The corresponding process design concept is as follows:

First, the smart contract nodes of the block chain set targets for collecting and integrating intelligence assets according to the individual needs of cyberthreat intelligence related businesses, including defining data types, attributes, and space-time conditions.

Second, on the basis of the data indicators collected, the scope of the various participating nodes, that is, the intelligence subjects, is determined. The nodes can also be subdivided into management role nodes and general role nodes. In addition, each participating node needs to be tasked with a clear division of labour, for example, by defining which nodes are responsible for integrating and developing intelligence information, and which ones are responsible to implement operational instructions and maintain coordination. This is also a prerequisite for forming a subsequent intelligence convergence sharing strategy and can guide the scripted deployment of the corresponding strategy in smart contracts.

Third, following the established smart contract rules, form a network threat intelligence fusion relationship among participating nodes, unify instructions and coordinate management. This step is to automate the collection, retrieval, and encryption of the metadata associated with the local database, which is then uploaded to the smart contract.

Fourth, each administrative node follows the contract rules and is responsible for encapsulating in the blockchain the summary information provided by the ordinary nodes such as the list of shared nodes, encrypted metadata, node IDs and so on in the form of data blocks.

Fifth, the various shared nodes use the summary information of the data block as a reference for further acquisition of encrypted metadata, and can conduct data authentication interactions to obtain encrypted public keys. In this way, the node body can smoothly carry out the parsing operation of the associated data, which means that it has completed the sharing of cyber threat intelligence.

Sixth, each body uses the smart contract transaction rules as a reference to encapsulate the data provider node, encrypted metadata summarization, sharing time and other information of cyber threat intelligence information, and store it in the form of transaction blocks in the cyber threat exchange chain.

Seventh, the nodes within the sharing mechanism are based on smart contract rules and intelligence sharing strategies. Further exploit the associated data shared by nodes, including data collection, classification, investigation, etc., to turn the data into usable high-quality cyberthreat intelligence products, and continue the above sharing cycle.

4. FURTHER THINKING ON THE REALIZATION OF NETWORK THREAT INTELLIGENCE SHARING MECHANISMS

First, smart contract nodes should comb through their own business requirements and rationally translate the requirements into a converged sharing strategy, so as to be able to deploy smart contracts by rules under different network threat intelligence sharing mission scenarios. This also facilitates the widespread and full chain flow of cyber threat intelligence assets, highlighting the value of their integrated and shared applications in contemporary society.

Second, all participants should follow the rules of smart contracts, do a good job in data acquisition, including automatically collecting and identifying data, reasonably extracting data from the local database, and then uploading the data to the block chain through data encapsulation. This can greatly reduce the cost of running a cyber threat intelligence sharing mechanism and increase the lubrication of the mechanism.

Third, the various sharing mechanism bodies under smart contracts should simultaneously assume the roles of smart contract initiators and participants, and play a positive role in command coordination, intelligence fusion and intelligence sharing.

Fourth, with the rapid development of computer and network technology, network security incidents are frequent, security vulnerabilities are constantly increasing, and the role and value of threat intelligence are increasing。[4]。Therefore, in order to implement the deep mining of intelligence data on the basis of the healthy operation of the network threat intelligence sharing mechanism based on blockchain smart contracts, pay attention to its diverse application scenarios and the opening up of widespread application value.

5. CONCLUSION

In summary, the establishment of a mechanism for sharing cyber threat intelligence is both necessary and feasible. Today, with the leapfrog development of blockchain technology, the implementation of cyberthreat intelligence sharing mechanisms based on blockchain smart contracts has more technical supporting conditions. People need to fully grasp the main object characteristics in the mechanism design, and then rationally implement the relevant functional requirements based on blockchain technology. In addition, the network threat intelligence sharing mechanism is established to enable relevant network threat information data to be mined and utilized to establish network security barriers, so fully pay attention to the implementation of this level of function in the operation of the relevant sharing mechanism.

FUND PROJECTS

Gansu Province Science and Technology Program Project (Technological Innovation Guidance Program): Network Threat Intelligence Sharing Mechanism and Implementation Based on Blockchain Smart Contract (20CX9ZA072).

Gansu province higher education institution innovation ability promotion project: based on block chain technology network rumor management research (2020A-093).

2018 Gansu University of Political Science and Law Key Research Funding Project: Research on Network Public Opinion Mining Technology Based on Semantic Statistical Analysis (GZF2018XZDLW20).

REFERENCES

[1] Ding, Cheng, and Chenwei Wu. "Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals." medRxiv (2024): 2024-09.
[2] Restrepo, David, et al. "Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications." medRxiv (2024): 2024-06.
[3] Yang, Jing, et al. "A generative adversarial network-based extractive text summarization using transductive and reinforcement learning." IEEE Access (2025).
[4] Xie, Minhui, and Shujian Chen. "Maestro: Multi-Agent Enhanced System for Task Recognition and Optimization in Manufacturing Lines." Authorea Preprints (2025).
[5] Zhu, Bingxin. "RAID: Reliability Automation through Intelligent Detection in Large-Scale Ad Systems." (2025).
[6] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).
[7] Hu, Xiao. "AdPercept: Visual Saliency and Attention Modeling in Ad 3D Design." (2025).
[8] Peng, Qucheng, et al. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." arXiv preprint arXiv:2412.20538 (2024).

[9] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." Molecular & Cellular Biomechanics 22.3 (2025): 669-669.
[10] Wang, Y. (2025). RAGNet: Transformer-GNN-Enhanced Cox–Logistic Hybrid Model for Rheumatoid Arthritis Risk Prediction.
[11] Qi, R. (2025). AUBIQ: A Generative AI-Powered Framework for Automating Business Intelligence Requirements in Resource-Constrained Enterprises. Frontiers in Business and Finance, 2(01), 66-86.
[12] Fang, Z. (2025). Microservice-Driven Modular Low-Code Platform for Accelerating SME Digital Transformation.
[13] Lin, Tingting. "ENTERPRISE AI GOVERNANCE FRAMEWORKS: A PRODUCT MANAGEMENT APPROACH TO BALANCING INNOVATION AND RISK."
[14] Chen, Rensi. "The application of data mining in data analysis." International Conference on Mathematics, Modeling, and Computer Science (MMCS2022). Vol. 12625. SPIE, 2023.
[15] Wang, Hao, Zhengyu Li, and Jianwei Li. "Road car image target detection and recognition based on YOLOv8 deep learning algorithm." unpublished. Available from: http://dx. doi. org/10.54254/2755-2721/69/20241489 (2024).
[16] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.