ISSN 2616-5775 Vol. 8, Issue 8: 15-19, DOI: 10.25236/AJCIS.2025.080803

Implementation of Blockchain Technology in Computer Network Information Security

An Yang

Information & Network Center, Beijing Information Science & Technology University, Beijing, China

Abstract: *In today's highly interconnected digital environment, computer network information security faces multiple threats such as data breaches, identity forgery, and malicious attacks. As a decentralized and tamper-proof distributed ledger system, blockchain technology provides a new technical path for data security through its core features of cryptographic algorithms and consensus mechanisms. This technology can ensure the integrity of information during data transmission and storage, effectively enhance the overall credibility of network systems, and inject new vitality into the information security protection system. Based on this, this paper explores the implementation of blockchain technology in computer network information security.*

Keywords: *Blockchain Technology; Computer; Network Information Security; Implementation*

1. Introduction

Against the backdrop of deep integration of global informatization and digitalization, computer network information security faces multi-source threats such as data theft and malicious code implantation. The protective capabilities of traditional centralized security architectures in aspects such as trusted computing and data encryption have gradually shown deficiencies. The application of blockchain technology can realize data confidentiality. An in-depth exploration of the implementation path of blockchain technology in computer network information security helps build a highly trusted and highly available network security protection system, promotes the development of network security systems toward a distributed direction, and provides forward-looking technical support for coping with an increasingly complex network threat environment.

2. Overview of Blockchain Technology

Blockchain technology uses cryptographic algorithms to achieve full traceability of data records and is composed of parts such as the data layer, network layer, consensus layer, and application layer. The data layer takes the block as the basic unit and uses a chain structure to encrypt and link transaction data in chronological order, ensuring data integrity. The network layer adopts a peer-to-peer transmission mechanism to achieve direct interaction between nodes, avoiding the single-point-of-failure risk of traditional centralized architectures. The consensus layer reaches data consistency among multiple nodes through specific consensus algorithms, with common mechanisms including Proof of Work and Proof of Stake. The application layer carries various business models based on smart contracts, enabling automated execution. By establishing trust in a decentralized manner, blockchain allows participating nodes to verify data without relying on third-party intermediaries, thereby enhancing system security. Compared with traditional databases, blockchain strengthens data protection during information transmission through cryptographic methods such as hash functions and digital signatures, ensuring that data remains tamper-proof during storage and transmission.

3. Application Value of Blockchain Technology in Computer Network Information Security

3.1 Conducive to Enhancing Data Security

The chained data structure of blockchain encrypts and links each data block with the previous one, forming an immutable chain of records. Once information is written, it cannot be modified individually, fundamentally preventing malicious tampering and data forgery risks. The distributed storage model

ISSN 2616-5775 Vol. 8, Issue 8: 15-19, DOI: 10.25236/AJCIS.2025.080803

synchronously stores data copies across multiple nodes, ensuring that even if individual nodes are attacked, the overall data can still maintain integrity, thus improving the system's disaster recovery capability. Blockchain ensures the confidentiality of data during transmission through digital signatures, effectively preventing security threats such as man-in-the-middle attacks and replay attacks. The consensus mechanism performs consistency verification of data among multiple nodes, making it difficult for malicious nodes to unilaterally tamper with records, thereby reducing the likelihood of internal attacks. The traceability feature of blockchain generates timestamps for all data operations, facilitating rapid identification of the source of problems and evidence collection after a security incident occurs.

3.2 Conducive to Building Network System Security

The decentralized nature of blockchain technology eliminates the risk of single-point failures, enabling the network system to maintain stable overall operation without relying on any single central node. Even if some nodes are attacked, the system will not suffer complete paralysis. The distributed consensus mechanism of blockchain ensures data and state consistency among nodes during data exchange and updates, effectively preventing network resource hijacking caused by malicious nodes. At the same time, the immutability of on-chain data makes the operational activities of the network system highly transparent, providing reliable evidence in the event of potential security threats. Cryptographic technologies are widely applied in blockchain networks, using public-private key encryption to achieve node identity authentication and prevent unauthorized access. Blockchain's smart contract functionality can automatically execute security policies within the system, reducing management loopholes caused by human intervention.

4. Implementation Strategies of Blockchain Technology in Computer Network Information Security

4.1 Data Encryption and Privacy Protection

4.1.1 Utilizing Blockchain Encryption Technology

During the process of data generation and storage, a hash function can be used to generate a unique fingerprint for the data, tightly binding the data content with verification information, thereby enabling rapid detection of tampering during subsequent transmission. In data exchanges between nodes, public-key encryption and private-key decryption should be used for information transmission to ensure that data can only be read by authorized recipients, effectively preventing interception during transit. At the same time, digital signature technology can be applied to sign transactions to verify the authenticity of data sources, reducing the risk of forgery and impersonation. Access control can be implemented by deploying encryption-condition-based smart contracts on the chain, setting up multi-level verification mechanisms for accessing sensitive data to ensure that data access complies with preset security policies. Encrypted data can be redundantly stored across distributed nodes so that even if some nodes are compromised, data recovery can still be achieved by relying on copies from other nodes, thereby maintaining data integrity [1].

4.1.2 Establishing a Privacy Protection Mechanism

A permission-tiered access control model should be deployed on the chain, granting different nodes differentiated data reading permissions to ensure that sensitive information is accessible only to authorized entities. Privacy-preserving computation technologies such as zero-knowledge proofs can be introduced to allow nodes to perform verification without exposing the original data content, thereby enabling business collaboration under confidentiality conditions. Ring signature methods can be applied to obfuscate the identity information of both transaction parties, hiding the real identities of specific participants and preventing the exposure of privacy during data tracing. Core privacy data can be stored off-chain in encrypted form, with only summary information retained on-chain, and rapid verification achieved via hash mapping, thereby reducing the probability of direct exposure of private information. Smart contracts can be used to set privacy data lifecycles to ensure that data exceeding its usage period is promptly deleted, avoiding potential risks from long-term storage.

4.1.3 Achieving Distributed Data Storage

In implementing distributed data storage, the multi-node collaboration feature of blockchain should be fully utilized to store data copies across different nodes according to preset strategies, reducing risks

ISSN 2616-5775 Vol. 8, Issue 8: 15-19, DOI: 10.25236/AJCIS.2025.080803

from single-point failures and centralized attacks. Complete data can be fragmented, with each fragment separately encrypted and distributed to nodes located in different geographical locations to achieve physical separation, thereby enhancing data security. Synchronization and verification mechanisms should be established among nodes to ensure that all fragments undergo rapid network-wide consistency verification after updates, preventing data version conflicts. To enhance privacy protection, only data indexes and hash verification values should be recorded on-chain, while the actual content is stored in an off-chain distributed storage network, ensuring retrieval and verification accuracy through hash mapping. Multi-factor authentication can be introduced on distributed nodes to authorize each data call, and node health monitoring and automatic backup mechanisms can be established to automatically activate other copies for data recovery when a node is abnormal, ensuring continuous system availability.

4.2 Identity Authentication and Access Control

4.2.1 Blockchain-Based Identity Authentication

Each node should be assigned a unique public-private key pair, with the public key recorded on the blockchain as an identity identifier and the private key securely kept by the user for identity verification. A distributed identity registration mechanism can be established on the chain so that when a new user joins, a smart contract automatically verifies the validity of their public key and related credentials, avoiding reliance on a single central server. To enhance authentication security, multi-factor authentication can be introduced by combining public-private key verification with dynamic passwords, biometric features, and other methods to achieve multi-layer identity checks. The system can use blockchain to record and compare users' digital signatures to ensure that access activities are consistent with authorized scopes. For cross-system trust, cross-chain protocols can be employed to enable identity verification across different blockchain platforms, allowing users to maintain a unified and trusted identity across multiple network environments. At the same time, all identity authentication processes can be traced using tamper-proof on-chain audit records, ensuring transparency in authentication procedures and comprehensively improving identity security in network environments [2].

4.2.2 Implementing Access Control

An access rights table should be established on the chain, mapping different nodes' role information to their accessible resource ranges, with encrypted storage to prevent unauthorized tampering of permission configurations. Smart contracts can be used to automatically execute access control rules, verifying user identities in real time upon receiving access requests to ensure that only eligible requests are granted resource access. To improve security, a multi-level authorization model can be introduced into the access control mechanism, requiring multi-party approval for access to sensitive data to reduce the risks posed by single-point authorization. All access activities and verification results should be recorded on the blockchain with timestamps to achieve traceable auditing for post-incident analysis. Access logs can also be backed up across distributed nodes to prevent record loss.

4.2.3 Establishing a Trust Mechanism

A system-wide identity registration process based on digital certificates and public-private keys should be set up to ensure that each node's identity information is authentic and unique, with authentication records permanently stored on the blockchain. The consensus mechanism can be used to validate each node's transactions through multi-party verification, preventing a single node from tampering with data. An on-chain reputation scoring system can be introduced to dynamically adjust nodes' trust levels based on their historical behavior and compliance, with higher-trust nodes granted higher permissions. To prevent malicious nodes from repeatedly registering to disrupt the system, smart contracts can be programmed with reputation penalty rules to automatically downgrade offending nodes. All trust-related operations should be timestamped and recorded on the chain, forming a traceable trust evolution path for subsequent review.

4.3 Preventing Malicious Attacks

4.3.1 Resisting DDoS Attacks

In resisting DDoS attacks, network service nodes should be distributed across a multi-node structure in different geographic locations, preventing attack traffic from concentrating on a single target and thus reducing the impact of large-scale traffic surges. In a blockchain system, smart contract–

ISSN 2616-5775 Vol. 8, Issue 8: 15-19, DOI: 10.25236/AJCIS.2025.080803

based traffic monitoring can be deployed to identify abnormally high-frequency requests in real time and automatically trigger throttling or isolation measures. To improve protection accuracy, the on-chain reputation management mechanism can dynamically lower the reputation value of malicious request sources, continuously triggering access restrictions to prevent repeated attacks. At the same time, node verification and multi-signature mechanisms can be introduced to ensure that only legitimate and verified requests are processed by the system, reducing the likelihood of attack traffic consuming system resources. The blockchain's distributed logging capability can also be leveraged to permanently store attack behaviors for future forensic analysis [3].

4.3.2 Preventing Data Tampering

All critical data should undergo a hash computation before being written, generating a unique checksum that is recorded in the block together with a timestamp, ensuring that even the slightest modification can be detected immediately. Through distributed storage, data copies are synchronized across multiple independent nodes, forcing an attacker to control the majority of nodes simultaneously in order to alter records, thereby increasing the attack cost. Smart contracts can be used to automatically execute multi-node verification processes, allowing new data to be written to the chain only after being unanimously confirmed by the majority of nodes, thus avoiding the risk of tampering caused by single-point manipulation. Digital signature technology can be employed to ensure that the source of each piece of data is verifiable and non-forgeable, preventing unauthorized entities from injecting false information. In addition, a periodic verification mechanism can be established among nodes to regularly scan blockchain data integrity; once a hash mismatch is detected, the system should immediately trigger an alert and restore to a secure state.

4.3.3 Detecting and Preventing Malware

Lightweight security agent modules should be deployed at network nodes to collect file signatures, runtime behaviors, and network connection information in real time. These security data should be encrypted and recorded on the blockchain to form a tamper-proof threat intelligence repository. Smart contracts can be configured with malware identification rules so that when a node detects an abnormal behavior pattern, it can automatically trigger isolation and blocking operations to prevent the spread of threats. To improve detection accuracy, a multi-node collaborative verification mechanism can be introduced, allowing different nodes to conduct cross-analysis of suspicious samples, thereby reducing the likelihood of single-point misjudgments. On-chain threat intelligence can also be synchronized in real time with external trusted security databases, enabling the system to quickly update protection strategies and identify new types of malicious programs. Furthermore, access control and digital signature technologies can be combined to strictly verify the installation, update, and execution processes of software, ensuring that only certified applications can run within the system [4].

4.4 Enhancing Data Integrity and Reliability

4.4.1 Data Backup and Recovery

In the data backup and recovery process, blockchain's distributed storage and redundancy mechanisms can be leveraged to ensure high reliability. Critical data should be segmented according to preset strategies, and each segment should be assigned a hash checksum before being encrypted and stored across nodes in different geographic locations, ensuring that single-point failures do not compromise data integrity. A multi-node real-time synchronization mechanism should be established so that backups are completed instantly when data is updated, preventing version inconsistencies caused by delays. Smart contracts can be preconfigured to automate recovery processes, allowing the system to retrieve corresponding segments from other nodes and reassemble them when a node failure is detected, thereby ensuring business continuity. To enhance backup security, layered encryption should be applied to backup data, making it accessible only to authorized entities. Backup data should be regularly subjected to integrity checks, using hash comparisons to quickly identify anomalies and promptly repair them.

4.4.2 Data Verification and Auditing

In the data verification and auditing process, blockchain's immutability can be used to establish a trustworthy end-to-end regulatory system. When data is updated, a unique checksum can be generated through hash computation and recorded on the chain together with a timestamp, ensuring that subsequent verification can quickly detect whether the data has been altered. Smart contracts can be deployed on the chain to automate the verification of critical data; when data is accessed, the system

ISSN 2616-5775 Vol. 8, Issue 8: 15-19, DOI: 10.25236/AJCIS.2025.080803

can instantly compare hash values and return verification results, reducing the burden of manual inspection. All data operation records should be written into the blockchain as transactions and linked to the identity of the operator, making the entire process fully traceable. To improve efficiency, a multi-node collaborative auditing mechanism can be introduced, allowing multiple independent nodes to cross-check records to prevent single-point auditing errors. Regular batch verification and analysis of on-chain data should be conducted, with visual tools used to generate audit reports, enabling security administrators to detect potential risks in a timely manner. In a blockchain environment, this approach builds a transparent, efficient, and trustworthy data verification system, fundamentally enhancing data integrity and reliability [5].

5. Conclusion

In summary, by virtue of its decentralized nature, blockchain technology provides an innovative approach to addressing issues such as data leakage and identity forgery in computer network information security. It can enhance system protection capabilities while improving data integrity and reliability. Efforts should be strengthened in data encryption and privacy protection, the implementation of identity authentication and access control, prevention of malicious attacks, and the enhancement of data integrity and reliability, so as to effectively reduce network threat risks and ensure the stable operation of information systems.

References

[1] Fang Xiang. Protection of Computer Network Information Security in Power Systems [J]. Network Security and Informatization, 2024, (11): 137-139.
[2] Wei Min. Research on Computer Network Information Security Protection Models Based on Artificial Intelligence [J]. Information Recording Materials, 2024, 25(11): 130-132.
[3] Gan Jianfang. Research on Computer Network Information Security Protection Based on Big Data Technology [J]. Information & Computer (Theoretical Edition), 2024, 36(20): 200-202.
[4] Shen Wenxu, Cui Mingliang, Xu Qingshu. Analysis of Network Information Security Protection Measures Based on Virtual Network Technology [J]. Computer Knowledge and Technology, 2024, 20(30): 82-84.
[5] Dong Hongmeng. Application and Protection Strategies of Data Encryption Technology in Computer Network Information Security [J]. Papermaking Equipment and Materials, 2024, 53(10): 130-132.