Blockchain Technology for Security Applications in the Broadcasting Industry (Postprint)

Authors: Xue Jianxia

Date: 2025-07-09T15:43:22+00:00

Abstract

【Objective】 This paper aims to analyze the characteristics of blockchain technology and its application in the broadcasting and television industry to ensure information security. 【Method】Based on factor analysis and theoretical analysis methods, we examine the blockchain technology architecture, key elements, potential risk points, and compliance requirements, and analyze the characteristics of the broadcasting and television industry along with strategies for selecting and utilizing blockchain technology. 【Result】 Through exploration and practice of blockchain technology application in digital copyright management and protection within the broadcasting and television industry, favorable outcomes are demonstrated. 【Conclusion】The research proves that blockchain technology holds practical significance for facilitating smart broadcasting and television and safeguarding information security, and should be vigorously promoted.

Full Text

Preamble

Research on Secure Application of Blockchain Technology in the Broadcasting and Television Industry

(Production Center of Guangxi Radio and Television Station, Nanning, Guangxi 530022)

Abstract

[**Purpose**] This paper aims to analyze the characteristics of blockchain technology and how it can be applied in the broadcasting and television industry to ensure the security of audio-visual information.

[**Methods**] Based on factor analysis and theoretical analysis, this study examines the blockchain technology architecture, key elements, potential risk points,

and compliance requirements. It also analyzes the characteristics of the broadcasting industry and how to select and utilize blockchain technology appropriately.

[**Results**] Through exploration and practice of blockchain technology application in digital copyright management and protection within the broadcasting industry, the 推演 (deductive 推演) effects are promising.

[**Conclusion**] The research demonstrates that blockchain technology has practical significance in supporting smart broadcasting and safeguarding audio-visual information security, and should be vigorously promoted.

Keywords: blockchain technology; smart broadcasting; digital copyright; information security; provenance tracing

1. Research Background

In recent years, "blockchain technology" has been deeply integrated with new-generation information technologies such as big data, artificial intelligence, Internet of Things, and the metaverse, profoundly influencing security transformations across various industries. Regarding what blockchain actually is, different experts and scholars have offered different definitions from different perspectives, but all core definitions include: 1) time-stamped "blocks"; 2) "chain" data structures; 3) distributed node consensus algorithms; 4) cryptographic techniques ensuring tamper-proof and non-forgeable properties; and 5) smart contracts to process and operate data [1].

Blockchain exhibits characteristics of single-node initiation, network-wide broadcasting, cross-verification, and collaborative accounting, enabling multi-node data storage consistency, tamper-resistance, and non-repudiation. Consequently, it is widely applied in: cryptocurrencies, with Bitcoin being the most classic blockchain application; supply chain management (traceability), such as digital collectibles and intellectual property; identity management, providing a secure and decentralized way to verify identity; and voting systems, for creating secure and transparent voting systems with verifiable and tamper-proof voting records. As applications in the broadcasting industry increase and security requirements strengthen, there is an urgent need to introduce blockchain technology.

Broadcasting media need to introduce blockchain technology to enhance their dissemination capacity, guidance, influence, and credibility. Value dissemination is the primary task of broadcasting media. The data consistency, tamper-proofing, and traceability features of blockchain can ensure the authenticity of information dissemination. Only authentic information can achieve value connection with audiences, and only authentic information can promote mainstream socialist values. In this regard, blockchain technology can help broadcasting media transition from information dissemination to value dissemination, improving both information and value dissemination capabilities.

Adhering to the principle of "seeking truth from facts" is fundamental for media to play their public opinion guidance role. By utilizing blockchain's distributed consensus algorithms and information immutability characteristics, broadcasting media can guarantee the authenticity of published information, ensuring they guide public opinion through facts and truth.

Based on blockchain platforms, the distributed characteristics of blockchain further expand the information dissemination space of broadcasting media. Meanwhile, blockchain's traceability features enable "full-process recording" and permanent information preservation, extending the temporal dimension of broadcasting media.

In the era of deep user participation in media content production, broadcasting media can only enhance credibility by reaching consensus through extensive interaction with users. Blockchain's distributed consensus structure allows deep participation from multiple users and members, jointly maintaining and ensuring the authority and credibility of produced content while also enhancing public trust.

2. Research Significance

The "13th Five-Year National Informatization Plan" issued by the State Council first included "blockchain technology" as a strategic frontier technology, making it a key national layout technology. The broadcasting media industry should keep pace with technological development trends, actively conduct in-depth research and application of blockchain technology, and fully utilize blockchain technology in smart broadcasting construction to innovate digital transformation in broadcasting.

3. Blockchain Technology Principles

The system architecture of blockchain technology generally includes a data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [2].

Data Layer. The data layer consists of data blocks and chain structures, including functional modules such as data blocks, timestamps, Merkle trees, and cryptographic technology. For the broadcasting industry, the data layer encapsulates audio-visual program information, account password information, "block" nodes, and transaction information. The timestamp mechanism marks data, while the blockchain structure enables traceability and positioning functions for blockchain data, allowing for 溯源 (traceability), storage, and verification. Each "block" consists of a "block header" and "block body"—the block body contains a certain number of transaction sets, while the block header contains the previous block's hash value, version number, difficulty target, nonce, etc. A block forms a strong association with the previous block through its parent block's hash value, creating a "chain" structure. Additionally, blocks store

the Merkle root value (Merkle Root), which is the hash value of the Merkle tree root node used to quickly verify the integrity of transaction sets within the block. Due to the chain structure defining the binding relationship of block data, if a malicious node attempts to tamper with certain data, this binding relationship would be destroyed, achieving blockchain's tamper-proof characteristics. Because of this chain structure and consensus mechanism, the cost for malicious nodes to forge this binding relationship is extremely high, while verifying malicious behavior is relatively easy.

The basic data unit of the chain structure is the "block," whose internal structure is shown in Figure 2 [Figure 2: see original paper].

The Merkel tree in the structure is a binary tree structure consisting of a root node, several intermediate nodes, and a set of leaf nodes. Leaf nodes store original transaction data, while non-leaf nodes store hash values of their two child nodes. Any change in node data propagates to its parent node, creating a chain reaction. Therefore, this Merkle tree structure can determine whether an element belongs to or exists in a set, enabling efficient comparison in large data volume scenarios and rapid location of modified positions.

Network Layer. Mainly composed of P2P networks, propagation mechanisms, and verification mechanisms, the network layer implements blockchain communication, synchronization, and verification of information and data between nodes [4]. Due to the adoption of peer-to-peer transmission technology, resource sharing does not rely on central servers, and the more participating nodes, the faster data transmission.

Consensus Layer. Primarily the consensus mechanism. Main consensus protocols include: PoX, BFT, and CFT. PoX protocols include PoW, PoS, etc.; BFT protocols mainly solve Byzantine fault tolerance problems, with PBFT being the representative protocol; CFT protocols are commonly used to prevent node misbehavior, with representative protocols including Raft, Paxos, and Kafka. The choice of appropriate consensus protocol depends on whether it is a public chain, consortium chain, or private chain to meet different fault tolerance requirements and adapt to different openness scenarios. Broadcasting industry copyright management systems generally adopt the PoW consensus mechanism.

Incentive Layer. Composed of issuance and distribution mechanisms, its purpose is to reward more nodes for "accounting." For example, Bitcoin adopts a "mining" mechanism where participants continuously provide computing power to obtain rewards.

Contract Layer. This layer enables users to flexibly create smart contracts according to their needs through program code. Through smart contracts, blockchain can be applied to various industries in modern work and life [5].

Application Layer. Encapsulates various script codes, algorithms, and the resulting smart contracts. Generally includes functional blocks such as algorithm mechanisms, program codes, smart contracts, access management, data manage-

ment, security management, and provenance tracing. It implements access control management, external data interface management, security management, and copyright and transaction management functions.

The blockchain technology system architecture is shown in Figure 1 [Figure 1: see original paper].

4. How the Broadcasting Industry Should Choose Blockchain Technology

Blockchain technology in the broadcasting industry can be approached from the following aspects: First, actively learn and comprehend blockchain technology principles and applications to enable blockchain technology to play a greater role in cost reduction, efficiency improvement, and secure broadcasting in the broadcasting industry. Second, deeply explore integration and innovation scenarios where blockchain technology can merge with radio, television, and online audio-visual industries, and formulate an overall plan for blockchain technology application innovation in radio, television, and online audio-visual fields to support digital transformation and upgrading of the broadcasting industry. Third, promptly research and analyze ideological security risks under new technologies and models, and explore security assurance and monitoring systems based on blockchain technology to ensure ideological security.

According to the degree of blockchain decentralization, blockchains can generally be divided into public chains, private chains, and consortium chains. Which type is most suitable for broadcasting industry applications? [6]

Public chains have no central nodes—all nodes access autonomously according to rules, work based on consensus mechanisms, and have no unified management institution. The broadcasting industry should preferably choose public chains when facing mass media and other commercial platforms. Bitcoin and Ethereum are typical public chains. This completely decentralized model can attract more technical personnel from inside and outside the industry to participate, prospering news gathering, program production, and other project crowdsourcing models, sharing economy, thereby supporting digital construction of the broadcasting industry [7].

Private chains operate within an organization where operational rules are formulated by the organization, with modification permissions limited to a few nodes and reading permissions also limited to a few nodes. Members entering private chains require authorization from central nodes. Broadcasting industry internal management, auditing, and other affairs can adopt private chains—for example, regulatory and administrative departments can use private chains for centralized management. Key core data that only needs internal circulation can be stored on private chains to achieve secure, reliable, traceable, and 溯源 (traceable) management [8].

Consortium chains are jointly initiated by several organizations, featuring par-

tial decentralization, and fall between public and private chains, such as Hyperledger. Consortium chains preset some nodes as accountants, with participating members requiring specific characteristics and advance settings. All preset nodes jointly determine the generation of each data block. For the broadcasting media industry exploring blockchain applications, consortium chains are most suitable. Because consortium chains have access mechanisms ensuring the real identity of node members and controllable consensus scope to guarantee consensus security, they enable data sharing cooperation between departments and vertical management departments, and collaboration between government departments and media platforms [9]. Content providers, content reviewers, content broadcasters, and regulatory agencies can form a broadcasting television content consortium chain. These participants can access as independent nodes and jointly maintain the consortium chain, thereby ensuring the credibility of multiple alliance chains.

5. Blockchain Security Risks

(1) Node Security Risk. Although blockchain is jointly maintained by multiple nodes and it is almost impossible to attack large numbers of nodes simultaneously, attackers can target nodes with weaker protection capabilities, thereby threatening the stability of the blockchain network. In public chain mode, node joining lacks effective verification and monitoring—attackers can destroy the authenticity of distributed ledgers by adding large numbers of malicious nodes, exploiting this decentralized anonymity to evade accountability [10].

(2) Consensus and Contract Risk. Although consensus mechanisms ensure "ledger" data consistency and smart contracts avoid manual operations through automatic execution, consensus mechanisms and smart contracts lack unified secure coding paradigms. Security vulnerabilities may exist when interfacing with upper-layer applications, potentially leading to illegal transactions.

(3) Key Management Risk. Node identities rely on private keys as unique identifiers to initiate transactions, verify, and prove. Once private keys are lost or leaked, attackers may impersonate legitimate user identities to operate data, causing privacy leakage issues. Backdoors and vulnerabilities in non-state cryptographic algorithms may also provide opportunities for attackers.

(4) Harmful Information On-Chain Risk. In public chain mode, harmful information such as "pornography, gambling, and drugs" and "violence and terrorism" is difficult to remove once on-chain. Blockchain databases generally only have three basic operations: create, write, and read. While data is difficult to maliciously tamper with, harmful information is also difficult to delete. Although operations like "hard forks" and "rollbacks" can modify harmful information, implementation is difficult and costly. Moreover, once on-chain, it quickly spreads through peer-to-peer data distribution, with uncontrollable impact scope [11].

6. Blockchain Security Compliance Requirements

To ensure better application of blockchain technology in the broadcasting industry, security compliance must first be guaranteed, taking the third-level requirements of the cybersecurity classification protection extension requirements as an example.

Secure Physical Environment. Blockchain platforms and operation and maintenance locations should be guaranteed to be within China's territory.

Secure Communication Network—Network Architecture Requirements: Should not carry blockchain applications higher than its security protection level; offline blockchain nodes should be able to synchronize data after rejoining the blockchain platform; after normal restart of blockchain nodes or recovery from abnormal scenarios, blockchain nodes should normally participate in consensus and synchronization to ensure data consistency; should support dynamic addition and deletion of blockchain nodes without affecting blockchain applications; should ensure two-way authentication in blockchain node communication processes; blockchain nodes should have backward version compatibility, supporting old version data after node upgrades.

Secure Regional Boundary—Boundary Protection. Should guarantee that blockchain platforms provide identity verification mechanisms such as PKI certification (including single CA certification or cross-certification among multiple CAs) to restrict node access and prevent malicious nodes from joining the blockchain platform [12].

Secure Computing Environment—Access Control Requirements. Should support strict restrictions on reading, writing, and other access permissions to blockchain platform resources by different types of users through access control strategies, multi-channel isolation, and smart contracts; should have effective request failure identification and processing capabilities, such as ending sessions, limiting illegal access attempts, and automatic timeout logout; should have user identity authentication and access authorization for blockchain platform smart contracts; should follow the principle of minimum necessity when opening sensitive data access authorization to blockchain platform and application users, requiring data owner authorization; should adopt authentication and authorization access control technologies to restrict queries and operations on ledger data and state data in blockchain applications to prevent unauthorized reading and tampering.

Secure Computing Environment—Security Audit Requirements. Should conduct security audit records on smart contract deployment and operation of blockchain platforms; should have arbitration response mechanisms for blockchain platform smart contracts, capable of executing smart contract freezing and recovery after arbitration, with corresponding records retained; should conduct audit records on updates, deletions, ownership changes, and other operations of on-chain data in blockchain applications to provide trace-

ability capabilities; should ensure that blockchain platforms' data operations on blockchain applications can be audited by blockchain application users; audit record retention time should meet legal and regulatory requirements.

Requirements for Smart Contracts. Should provide smart contract security development specifications, clarifying development security requirements for smart contracts in interface security, security configuration, and operational security, and establish smart contract security detection mechanisms; blockchain virtual machines should ensure secure precompiled contract calling and execution, safely handling abnormal calls without virtual machine escape, arbitrary code execution, and other vulnerabilities; should conduct baseline security detection, framework security detection, source code security detection, etc., on smart contracts, and inform users of detection results and risk conditions; calls between smart contracts should perform call permission verification and restriction [13].

Requirements for Consensus Security. Should disclose blockchain platforms' consensus mechanisms, synchronization network models, fault tolerance conditions, and applicable scenarios; blockchain platforms' consensus mechanisms should support dynamic scaling down and scaling up of blockchain nodes; blockchain platforms' consensus mechanisms should have fault tolerance and consistency, with anti-replay attack capabilities.

Requirements for Data Traceability. Should adopt technical means such as watermarking to achieve traceability of sensitive data in data display links, and adopt verification technology or cryptographic technology to protect the integrity of traceability data; should adopt technical measures such as data marking and data lineage analysis to achieve data source traceability for introduced or collected data; should adopt technical measures such as watermarking to achieve traceability of data in data export and sharing links, with watermarks having concealment and anti-tampering capabilities.

Requirements for Data Integrity. Transactions and ledgers should have complete data records on multiple blockchain nodes, ensuring data consistency among blockchain nodes; should ensure that transaction data and ledger data adopt cryptographic technology to guarantee data integrity across blockchain nodes.

Requirements for Data Confidentiality. Should ensure the use of cryptographic technology to achieve secure storage of personal privacy information in transaction data and ledger data; should ensure that generated application data and user personal information are stored domestically, with cross-border transfer following national regulations; should ensure that only with data owner authorization do blockchain platform operators or third parties have data management permissions for blockchain applications.

Requirements for Centralized Management of Security Management Centers. Should have monitoring functions for business resources of blockchain platforms, including the number of on-chain transactions, pending transactions,

and contract quantities; should have monitoring functions for business resources of blockchain nodes, including blockchain nodes initiating transactions or contracts, verifying transactions or contracts, etc.; should provide alarms when monitored business resources exceed set ranges.

Requirements for Cryptographic Management in Security Operation and Maintenance Management. Blockchain systems using cryptographic technology, cryptographic products, and cryptographic services should comply with laws, regulations, and relevant national and industry standards for cryptography; adopted cryptographic products should meet the second-level and above security requirements of "Information Security Technology—Security Requirements for Cryptographic Modules" (GB/T 37092—2018). Requirements for key management parties refer to Appendix B of "Information Security Technology—Basic Requirements for Cryptographic Application in Information Systems" (GB/T 39786—2021).

7. Application of Blockchain Technology in Digital Copyright Protection

Network audio-visual work infringement occurs frequently, seriously damaging creators' rights. For film and television drama producers, secondary editing-related disputes and lawsuits occur frequently, but face high rights protection costs, difficult evidence collection, and low rights protection benefits. Blockchain features consensus mechanisms, smart contracts, distribution, timestamps, and tamper-proofing. First, blockchain technology can be used to establish digital asset copyright trading platforms for intellectual property transactions through blockchain platforms, ensuring transparency and credibility throughout the process and protecting the rights of all parties. Second, blockchain technology combined with Content Delivery Networks (CDN) can reduce traditional distribution costs—Youku's use of blockchain technology for distribution can reduce costs by 90% compared to traditional methods. In broadcasting digital copyright management and protection, blockchain technology can effectively address network audio-visual work infringement issues from the source. Specifically, this can be implemented through three levels: content identification on-chain, distribution data on-chain, and decentralized supervision [15].

Content Identification On-Chain: On-chain data requires multi-level review and dynamic authorization through authorized official regulatory platforms within the consortium chain. The review process adopts an automated decision-making framework based on blockchain smart contracts, including 传播合法性验证 (transmission legality verification), dynamic planning of transmission paths, and revenue distribution rules. Simply put, it determines whether content can be transmitted, how to transmit it, and how to distribute transmission benefits. For content that can be legally transmitted, timestamps and digital fingerprints are added for data traceability and evidence preservation. Video materials in the network audio-visual field have copyright holders stipulating transmission scope and benefit distribution through smart contracts. Generally, an improved

PBFT algorithm can be used within the consortium chain to generate tamper-proof time vouchers, while SHA-3 algorithms build digital fingerprints of content feature vectors, with their hash values written into blockchain ledgers as unique identifiers to achieve full lifecycle traceability and evidence preservation. This provides content production users with legal usage channels, fundamentally eliminating infringement of audio-visual works, especially secondary editing of film and television dramas [16].

Distribution Data On-Chain: On-chain transaction behaviors and information are fully recorded, enabling supervision of copyright content distribution destinations. By setting transmission parameters through smart contracts, geographic fence restrictions can be implemented based on IP address databases, device fingerprint binding can be ensured through IMEI/MAC address encryption verification, and timeliness control can be implemented through timestamp services, etc. If a work is only directed to transmit on a specific platform, that platform is responsible for ensuring its reasonable transmission. Once early leakage or piracy occurs, distribution data can be traced from pirated video content for legal accountability. Since all distribution operations generate composite digital fingerprints based on content hashes and distribution path metadata, traceability and evidence solidification of infringement behaviors can quickly locate leakage nodes by comparing on-chain data hash fingerprints. In judicial practice, distribution data can be directly used as evaluation criteria for determining infringement compensation amounts [17].

Decentralized Supervision to Eliminate Short Video Infringement Chaos: Broadcasting regulatory departments, as one of the on-chain nodes, face all users and establish an automated review rule library through smart contracts and multi-dimensional automated review rules including ideological review (such as politically sensitive word filtering), copyright ownership verification (based on blockchain evidence-stored copyright registration information comparison), and content compliance detection (using OpenCV algorithms to identify violent and bloody scenes). This review mechanism transforms traditional centralized review processes into on-chain multi-node collaborative verification, retaining administrative regulatory authority while empowering users to create through technology. Broadcasting officials play the role of review gatekeepers on the platform but do not hinder user production—only providing a legal environment for user production. Digital content distribution users can directly transmit rights and responsibilities to usage users, who can avoid infringement behaviors caused by unclear rights constraints during secondary editing or transmission, fundamentally enhancing users' copyright protection awareness.

8. Practice and Summary

Traditional broadcasting and media convergence platforms' audio-visual program copyrights and user information authentication use centralized symmetric encryption methods through user passwords, data certificates, identity tokens,

and biometric features to confirm user identity, with relatively low authentication security levels. Using blockchain technology's security authentication mechanism, data is first timestamped in chronological order to become permanent information that cannot be modified reversibly. Then this data is "fragmented" to form a distributed ledger system dispersed across different nodes. Finally, through optimized domestic commercial cryptographic technology authentication, broadcasting media information data security can be better guaranteed [18].

Blockchain technology is a decentralized, distributed shared data ledger with characteristics of full traceability, tamper-proofing, traceability, collective maintenance, and P2P file transmission, subverting traditional HTTP-mode Internet. Additionally, the IPFS protocol can resist DDoS attacks, prevent network "堰塞湖" (dam lake) occurrences, automatically retrieve and delete duplicate audio-visual programs or user data, thereby saving substantial storage space [1].

Using blockchain technology's consensus mechanism and adopting public, independent distributed accounting methods to store audio-visual program libraries and databases can ensure data consistency and validity, quickly detecting tampering, deletion, and configuration operations. Using timestamps and traceability technologies can identify "internal ghosts," and using "Byzantine" fault-tolerant consensus protocol functions can correct erroneous information data on the platform. This can solve problems of low sharing efficiency, severe data fragmentation, insecure transmission processes, insufficient personal information protection, and lack of data integrity verification when audio-visual program libraries and databases become increasingly large. It can also address excessive demands on storage and bandwidth resources. Blockchain technology can utilize distributed management methods to achieve full-process dynamic automated access control for big data resources [8].

We practically built a blockchain technology platform applied to digital copyright management and protection for media convergence platforms. Practice has found that blockchain technology's decentralization, anonymity, and smart contract characteristics can solve the following specific information security issues:

(1) For the most common SQL injection vulnerabilities, blockchain technology can protect data integrity due to the absence of central points. Centralized information structures are easily stolen, and hacker attacks destroying central node systems can easily cause data incompleteness. In decentralized information structures, all independent nodes have complete information. Even if hackers attack certain nodes, other nodes still retain complete information and can quickly detect hacker attacks and promptly prevent hackers from entering, thereby ensuring data integrity.

(2) Cross-site scripting (XSS) attacks are also among the top 10 attack methods, preventing XSS attacks, webpage tampering, and black chain hanging. If all audio-visual programs and user information of broadcasting

media convergence platforms converge on a central node, once the central node is breached or implanted with malware, the media convergence center faces security threats affecting safe broadcasting. In blockchain systems, platform decentralization can better solve the problem of illegal tampering leading to broadcasting security issues.

(3) Anonymity, smart contract transactions, and P2P transmission can ensure transaction security.

(4) Due to the simplicity and convenience of smart contracts in transaction methods, transactions are relatively independent without third-party intervention, enabling intelligent P2P transactions that save substantial transaction resources while improving transaction efficiency and information security.

References

[1] Feng Qing, Xue Jingxia, Wu Zhongle, et al. Research on Secure Application of Blockchain in Broadcasting and Television [J]. Broadcasting and Television Technology, 2020, 47(4): 16-19.

[2] Yang Jinghua. Research on Security Strategy and Architecture of Blockchain in Converged Media Platforms [J]. Broadcasting and Television Technology, 2021, 48(10): 57-61.

[3] Business Department of China Broadcasting Network Co., Ltd. Discussion on Application of Blockchain Technology in Cable Television Networks [J]. Cable Television Technology, 2017(7): 16-19.

[4] Chen Xiaofeng, Wang Zixin, Xie Qing. Research on Application of Blockchain Technology in Broadcasting and Television Content Review Scenarios [J]. China Media Technology, 2021(11): 7-9.

[5] Discussion on Application of Blockchain Technology in Cable Television Networks [J]. Cable Television Technology, 2017(7): 16-19.

[6] Fang Jie, Jiang Zhengxu. Research on International Application of Blockchain Technology in Media Scenarios [J]. News and Writing, 2020(1): 21-26.

[7] Zhou Wanyi, Chen Xiaofeng, Xie Qing. Research on Application of Blockchain Technology in Digital Copyright Scenarios in the Broadcasting Industry [J]. China Media Technology, 2021(11): 10-12.

[8] Lan Luo Haozhan, Zhang Weixuan, Xie Qing, et al. Research on Application of Blockchain Technology in Broadcasting Content Collaborative Creation Scenarios [J]. China Media Technology, 2021(11): 13-15.

[9] Yang Jinghua, Zhu Meibin. Research on Security Strategy and Architecture of Blockchain-based Broadcasting and Media Convergence Platforms [J]. Television Technology, 2021, 45(1): 9-13, 45.

[10] Zhongguancun Information Security Assessment Alliance. Information Security Technology—Cybersecurity Classification Protection Blockchain Security Extension Requirements: T/ISEAA 003-2023[S]. Beijing: Zhongguancun Information Security Assessment Alliance, 2023.

[11] Wang Yinsi. Research on Secure and Efficient Traceability Solutions Based on Blockchain [D]. Xi'an: Xi'an University of Posts and Telecommunications, 2023.

[12] Wang Nuosi. Value Interpretation and Implementation Path of Blockchain Empowering Business Government Environment Construction [J]. Journal of Yantai University (Philosophy and Social Sciences Edition), 2023(4): 112-120.

[13] Zha Xuan, Cui Xiaofei, Wei Liang, et al. Blockchain Infrastructure Security Analysis and Protection [J]. Information and Communications Technology, 2019(6): 45-51.

[14] Wei Bin, Liu Xiaofeng, Gou Hang. Research on Distributed On-Chain Energy Trading Model Based on Public Chain [J]. Journal of Changchun Normal University, 2019(2): 60-71.

[15] Shi Ying. Research on Digital Interface Content Protection System Based on Consortium Chain [D]. Xi'an: Xidian University, 2022(6): 23-32.

[16] Li Shuilin, Chen Guangyong. Compilation Ideas and Key Points Analysis of "Guidelines for High-Risk Judgment of Cryptographic Application in Information Systems" [J]. Information Network Security, 2021(12): 1-8.

[17] Li Chenyuyan, Zhang Caiming. Review and Development of Blockchain Accounting Research from a Big Data Perspective [J]. Science and Technology Think Tank, 2022(2): 81-92.

[18] Zha Xuan, Meng Nan. How to Address Security Risks in Blockchain Infrastructure [J]. People's Posts and Telecommunications, 2020(1): 78-86.

Author Profile: Xue Jianxia (1980—), female, from Hezhou, Guangxi, Senior Engineer at Production Center of Guangxi Radio and Television Station, Bachelor of Engineering, Member of the Network Audio-Video Professional Committee of the Third Science and Technology Committee of Guangxi Radio and Television Bureau, research direction: broadcasting information security technology.

(Editor in Charge: Li Yansong)

Note: Figure translations are in progress. See original paper for figures.