Intelligent and Converged Networks
2023, 4(2): 142−157

ISSN 2708-6240
DOI: 10.23919/ICN.2023.0015

A new media content trusted dissemination architecture based on AV-blockchain and ChinaDRM

Wenqian Shang* **and Zaifu Yu**

Abstract: The diffusion of all-media content plays a vital role in guiding public opinion and ideology. However, at present, most of the media content exists on all kinds of mainstream media platforms, which poses great challenges to the effective supervision of relevant departments and society. This has led to arbitrary charges, chaotic media content, difficulties in supervision and evidence collection, and infringements of the rights and interests of original content creators. To address these problems, this paper constructs a trustworthy propagation architecture that supports multi-platform media content sharing. This architecture collaboratively builds an audio-visual blockchain through public and consortium blockchains, coupled with an improved ChinaDRM to provide digital rights management and content encryption. Simultaneously, we employ an enhanced Diffie−Hellman key agreement protocol to offer distributed encryption and decryption for media content. Within this model, various media platforms and national regulatory authorities are responsible for content storage and distribution as consortium nodes and public blockchain nodes, respectively. At the same time, users, as light nodes of public chain or service consumers of consortium blockchain, can consume and comment on content. Analysis shows that the trusted communication framework of media content based on the audio-visual blockchain has certain expansibility and practicability. It can facilitate the supervision of mainstream media platforms by national authorities and society through inter-blockchain technology, offering a novel solution for multi-platform trustworthy cooperative information sharing.

Key words: media content dissemination; ChinaDRM; AV-blockchain; trusted communication architecture; inter-blockchain

1 Introduction

At present, the distribution of a large amount of audio and video content is mainly carried out by market-oriented media platforms such as Tencent Video, iQiyi Video, Netflix, and YouTube. At the same time, with the surge in short video users, original short videos are also concentrated on platforms such as Kuaishou and TikTok[1]. Although these platforms are subject to supervision from national authorities and society, there are still such problems as insufficient regulatory measures, vulgar and low-quality content, and large-scale plagiarism that harms the rights and interests of original authors. These phenomena indicate the need for better mechanisms to provide more standardized management of mainstream media platforms.

Blockchain technology is a decentralized infrastructure and distributed computing paradigm that uses encrypted chain structures to validate and store data, consensus algorithms among distributed nodes to generate and update data, and automated script code (smart contracts) to program and operate data[2]. Combining the application advantages of different types of blockchains and the service objects and specific business flows of media content distribution, this article proposes a multi-role trusted audio and video dissemination framework based on public and consortium blockchains, aiming to provide trusted,

• Wenqian Shang is with the State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing 100024, China. E-mail: shangwenqian@cuc.edu.cn.
• Zaifu Yu is with the School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China. E-mail: yzfssg@126.com.
∗ To whom correspondence should be addressed.

Manuscript received: 2023-04-12; revised: 2023-06-10; accepted: 2023-06-14

regulated, and profitable decentralized services to three roles: general users (content consumers and producers), regulatory departments, and media service providers.

China digital rights management (ChinaDRM) is a digital rights management technology that protects the copyright and security of digital content through encryption, authorization, and access control[3]. The main characteristics of ChinaDRM technology include high reliability, good security, difficulty in cracking, and support for multiple digital content formats and various devices. With ChinaDRM technology, users of digital content must go through authorization and encryption verification steps to access and use protected digital content, thereby achieving copyright protection and content security. ChinaDRM technology has a wide range of applications, including audio and video contents, e-books, and game softwares, and can be used for the distribution and management of digital content, such as encryption, decryption, authorization management, and usage statistics of digital content.

Based on the characteristics and advantages of blockchain and ChinaDRM, this article proposes the construction of a trustworthy media content distribution architecture by combining consortium blockchain and public blockchain to form an audio-visual blockchain, and integrating the improved ChinaDRM into the audio-visual blockchain. By utilizing the consortium chain, a consensus can be reached between media content service providers and regulatory authorities, providing users with multi-platform media content viewing services and offering technical support for unified endorsement and authorization management by regulatory authorities. The public chain facilitates communication between users and media content suppliers, where users pay fees to consortium nodes and apply for media content viewing certificates. The consortium nodes are responsible for providing corresponding services as well as public chain full-node services. This architecture not only supports users to enjoy multi-platform resources but also enables the reasonable distribution of profits and coordinated management by regulatory authorities across different platforms. Additionally, the architecture has strong scalability and flexibility, which can support more similar service models.

The innovations and contributions of this paper are as follows:

- Propose a digital copyright protection architecture combining blockchain and ChinaDRM, which enables transparency of rights for users, platforms, and regulatory authorities;
- Utilize consortium blockchain and public blockchain inter-blockchain to build an audio-visual blockchain to realize trusted sharing of multi-platform media content;
- Improve the Diffie–Hellman key exchange protocol for distributed encryption and decryption of media content;
- Introduce decentralized identity construction algorithms and decentralized verifiable credentials.

The main idea of this paper is to combine the public chain and the consortium chain, and on this basis, incorporate ChinaDRM to establish a trustworthy digital copyright protection architecture. First, the advantages of this architecture over current mainstream media content supervision or media content copyright protection methods are introduced. Then, the roles of the public chain, consortium chain, and ChinaDRM in digital copyright protection are presented. The architecture proposed in this paper is equipped with an improved decentralized identity generation algorithm and digital media content encryption and decryption algorithms, making digital copyright protection more efficient and secure. At the same time, this paper analyzes the wide applicability of this architecture, proving the reliability and innovation of the proposed architecture.

The structure of this article is arranged as follows. Section 2 reviews the research work of scholars on the application of blockchain and ChinaDRM in digital rights management protection. Section 3 introduces the mainstream centralized framework for video and audio content distribution. Section 4 proposes an integrated video and audio content distribution model based on improved ChinaDRM. Section 5 introduces decentralized identity and verifiable multi-party credentials. Section 6 introduces distributed encryption and decryption of media content distribution. Section 7 summarizes the content of this article.

2 Related work

Many scholars apply blockchain technology to digital copyright protection and media content distribution. Sun et al.[4] used blockchain and homomorphic encryption technology to implement a copyright auction system. This article mainly compares the performance of homomorphic encryption with other algorithms in terms of key generation, encryption, and decryption. Chen et al.[5] proposed a reliable copyright detection architecture based on blockchain. In this architecture, the detection organization first detects the copyright outside the blockchain and then saves the detection record to the blockchain. This article mainly focuses on hash algorithms and lacks a discussion on the overall digital copyright protection system architecture. Miao et al.[6] designed a digital copyright transaction system model based on the consortium blockchain and implemented copyright registration and transaction, which can ensure that copyright information can be traced and not tampered with. This article mainly focuses on copyright transactions and does not describe other processes, such as copyright registration. Xu et al.[7] proposed a digital copyright protection system based on blockchain technology and the InterPlanetary File System (IPFS) technology, which provides full-process copyright protection services, including confirmation, registration, subscription, purchase, tracking, and querying. Liang et al.[8] proposed a dual-blockchain architecture for digital copyright registration and transaction systems. Based on the blockchain of the digital copyright registration and management chain (RMC) and the digital copyright transaction and subscription chain (TSC), it isolates account information and transaction information to prevent information leakage and improve privacy protection. However, this article focuses on system performance issues. Wang et al.[9] established a model based on smart contracts and IPFS and used an improved ElGamal encryption algorithm to encrypt and protect session data and evaluate the efficiency of the improved algorithm. However, this article focuses on watermarking and simulation to implement copyright protection systems. Chen et al.[10] proposed a trustworthy copyright detection architecture based on blockchain called DCDChain. In this architecture, the detection organization first detects the copyright outside the blockchain and then uploads the detection record to the blockchain. Since the data on the blockchain is public, media providers can verify the correctness of the copyright detection results and resort to smart contracts in case of any objections. Then, the smart contract arbitrates disputes by verifying the correctness of the blockchain data. However, this article mainly focuses on copyright detection issues and lacks research on copyright content encryption. Agyekum et al.[11] constructed an IPFS system in which all digital media files exist as IPFS objects. They also designed a digital fingerprint that reflects the characteristics of digital media files. Finally, all files are recorded on the Fabric blockchain to ensure immutability and source. This article mainly focuses on the storage of digital content and digital fingerprints and does not consider the security of digital content. Ding et al.[12] combined blockchain technology and digital copyright registration technology to design a complete copyright registration protection system. However, this study mainly focuses on digital copyright protection mechanisms and protection processes. Zhao et al.[13] proposed a blockchain-based network image copyright transaction protection method and discuss the advantages of applying blockchain to network image copyright transactions. At the same time, they described the implementation structure of the blockchain-based copyright transaction market and propose specific business plans for image copyright transactions.

Similarly, many scholars applied ChinaDRM to digital rights management protection. Zhou et al.[14] introduced the architecture of ChinaDRM and its application in the transport stream (TS) packaging format. They proposed an analysis method for encrypted TS bitstreams and designed a bitstream parsing system to parse the data of content encryption information (CEI) and ChinaDRM descriptors. Zhou and Lin[15] proposed a method for segmenting and decrypting defined bitstreams and encrypted bitstreams in the "Digital Rights Management Technical Specification for Video and Audio Content Distribution" (GY/T 277-2019) standard. Using this method, the video bitstream after format conversion can be segmented, decrypted, and played to verify whether the transmitted audio and video streams comply with the standard, thereby verifying the correctness of the encryption and modifying existing problems. Zhang et al.[16] mainly focused on the rights of expression and content authorization mechanisms of ChinaDRM. They established a basic model of ChinaDRM rights expression, introduced the format of ChinaDRM licenses, and provided an analysis of a license example.

ChinaDRM technology can convert copyright information of digital content into digital assets and store it on the blockchain, thereby achieving secure protection and regulation of copyright[17]. In addition, blockchain technology can provide reliable information records and audits for the circulation and use of digital content, preventing illegal copying and dissemination. By combining ChinaDRM technology and blockchain technology, the copyright of digital content can be more effectively protected, further safeguarding the legitimate rights and interests of content creators and copyright holders[18]. At the same time, the combination of these two technologies can also promote the healthy development of the digital content market, improving the efficiency and security of digital content transactions.

3 Centralized video and audio content distribution framework

Amazon's digital rights management refers to the requirement for users to obtain authentication from a DRM authorization server before they can use a particular digital work[19]. The basic strategy is to package authentication data and playback file permission data and send them to the content distribution network to provide authentication services. The DRM principle of Amazon is shown in Fig. 1.

Microsoft PlayReady embeds authentication fields into digital publications, enabling multiple devices to use the same license and reducing the need for authentication queries. This makes it easy to port to other platforms[20]. The DRM principles of Microsoft are shown in Fig. 2.

In the "Technical Specification for Digital Rights Management of Video and Audio Content Distribution", the digital rights management system for video and audio content distribution is logically divided into DRM server and DRM client modules[21], as shown in Fig. 3. Each module of the DRM server and DRM client establishes a trust relationship based on public key infrastructure (PKI) technology, and secure communication is established between them based on this trust relationship.

Conventional DRM service providers usually employ a combination of one or several digital technologies to protect digital copyrights. However, there exist certain shortcomings in terms of copyright tracing and anti-counterfeiting. Additionally, centralized services face

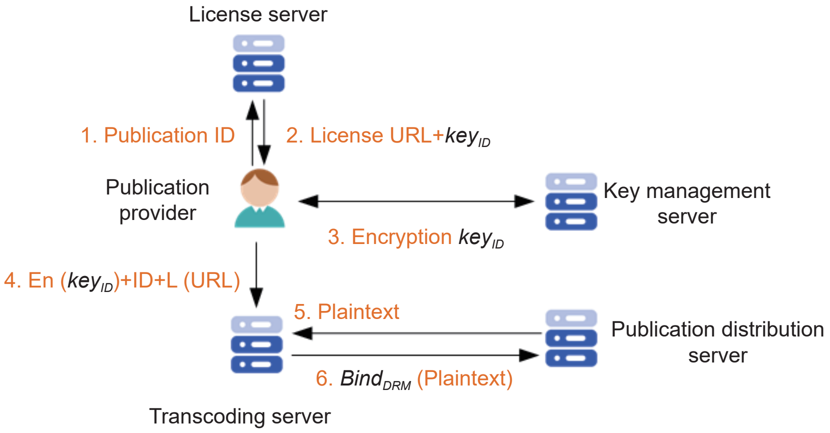

Fig. 1 Schematic diagram of Amazon DRM.

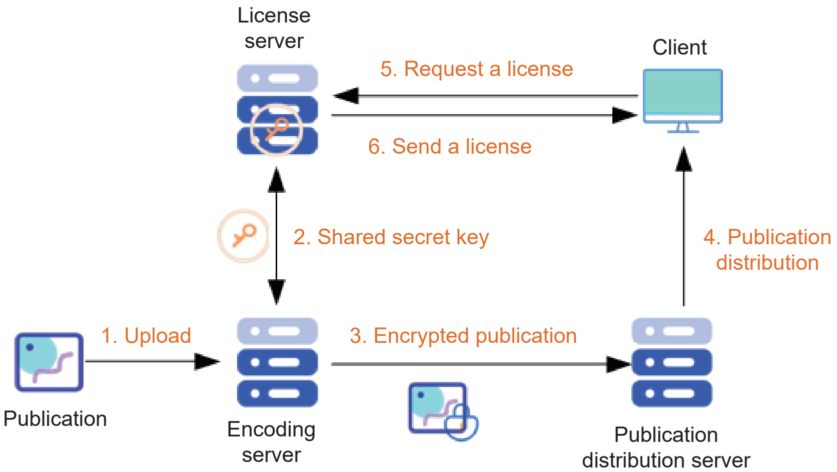

Fig. 2 Schematic diagram of Microsoft DRM.

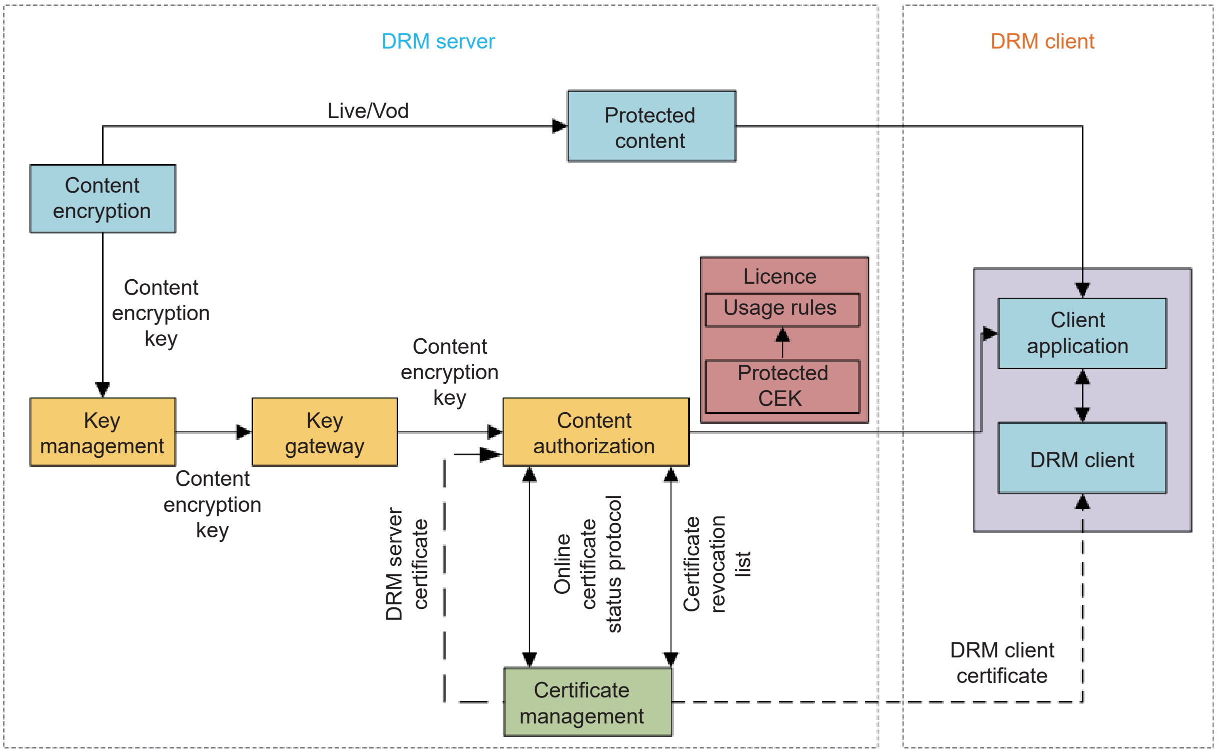

Fig. 3 Digital rights management logic architecture diagram for video and audio content distribution.

significant pressure and are also plagued by monopolistic issues.

3.1 Framework advantage

Currently, mainstream methods of media content supervision or media content copyright protection mainly include:

- **Copyright registration**. Media content creators can register their work with copyright offices or related agencies to prove their ownership of the work.
- **Digital watermarking technology**. By embedding invisible identifiers in media content, it’s possible to track and identify illegally copied and disseminated media content.
- **DRM technology**. This is a technological method that can limit the usage of digital media content, including copying, editing, and playing. For instance, online music and movie streaming services often use DRM technology to protect their media content.
- **Content recognition technology**. Systems like

YouTube's content ID can automatically recognize and manage copyrighted content.

While the above methods have certain effects, they also have some problems. For example, the process of copyright registration and maintenance can be cumbersome and costly; digital watermarking and DRM technology can be cracked; and content recognition technology may have issues with false positives and missed detections.

By combining the consortium blockchain and the public chain, we can construct a media content supervision platform that is efficient, secure, transparent, and reliable, particularly when integrated with ChinaDRM. The key advantages of this architecture include:

- **Efficiency**. The combination of the consortium and the public blockchain facilitates efficient data processing and transaction capabilities. The public chain can extensively obtain and verify information, while the consortium blockchain can swiftly process and confirm transactions.
- **Security**. The adoption of blockchain technology enhances the platform's security. All transactions are recorded on the blockchain, implying that once data is written, it cannot be tampered with or deleted, thereby significantly enhancing data security.
- **Transparency**. Blockchain technology's core strength lies in its transparency. All transactions can be viewed by every participant, ensuring all actions are open and transparent, reducing the potential for fraud and malicious behavior.
- **Trustworthiness**. Due to the distributed nature of the blockchain, decentralized supervision of media content can be realized, allowing every participant to engage in the supervision process, which enhances the platform's trustworthiness.
- **Copyright protection**. When combined with ChinaDRM, the copyright protection of media content can be enforced. ChinaDRM can create a unique identifier for each piece of media content, which can be recorded in the blockchain, ensuring that each piece of media content's copyright is effectively protected.
- **Copyright transaction**. On this platform, copyright owners can trade their copyrights using blockchain technology, which enhances the efficiency and transparency of copyright transactions.
- **Cost reduction**. By leveraging blockchain automation and smart contract technology, the cost of copyright transactions and protection can be reduced, making copyright transactions and protection more affordable.

3.2 Role and advantages of ChinaDRM

In the media content supervision platform built by the combination of the consortium blockchain and public blockchain, ChinaDRM primarily plays a role in copyright confirmation, protection, trading, and supervision, providing an efficient, secure, transparent, and trustworthy copyright management method. Here are some of the main roles and advantages of ChinaDRM:

- **Copyright confirmation**. ChinaDRM can create a unique identifier or "fingerprint" for each piece of media content. This identifier can be written into the blockchain to confirm the copyright ownership of a particular piece of media content. This function plays a crucial role in handling copyright disputes.
- **Copyright protection**. ChinaDRM, through digital watermarking, encryption, and license management technologies, protects media content from being illegally copied and disseminated. With the aid of blockchain, these protective measures can be implemented across the entire network, enhancing the efficiency and effectiveness of copyright protection.
- **Copyright trading**. ChinaDRM can support copyright trading. Copyright owners can trade their copyrights via blockchain, and ChinaDRM provides support for each transaction, including copyright transfer, license issuance, and more.
- **Copyright use supervision**. ChinaDRM can track and monitor the usage of media content, assisting copyright owners in understanding how their content is being used and whether there are instances of illegal usage.
- **Reducing copyright management costs**. Leveraging blockchain's automation and smart contract technology, ChinaDRM can reduce the costs of copyright management. For instance, smart contracts can automatically execute rules for copyright

transactions and usage, reducing the need for manual operations.

- **Enhancing transparency in copyright management**. By recording copyright information on the blockchain, ChinaDRM can enhance the transparency of copyright management. All copyright transactions and usage conditions can be viewed by all participants, thus ensuring openness and fairness in copyright management.

3.3 Broad applicability of the architecture

The proposed architecture has wide applicability and can be used for copyright protection and management in many media content industries. Here are a few potential instances:

- **Music industry**. In the music industry, this framework can be used to record and track copyright information of music works. Creators can write the copyright information of their music works into the blockchain, ensuring their copyrights are protected. At the same time, the copyright of music works can also be traded on the blockchain, enhancing the efficiency and transparency of transactions.
- **Film and television industry**. In the film and television industry, this framework can be used to manage the copyrights of film and television works. Production companies can write the copyright information of their works into the blockchain to prevent illegal copying and dissemination. Simultaneously, the copyrights of film and television works can also be traded on the blockchain, such as transferring or leasing broadcasting rights.
- **Publishing industry**. In the publishing industry, this framework can be used to protect and manage the copyrights of books, magazines, newspapers, and other publications. Publishers and authors can write the copyright information of their works into the blockchain to prevent illegal copying and dissemination. At the same time, the copyrights of publications can be traded on the blockchain.
- **Photography and graphic art industry**. Photographers and artists can write the copyright information of their photos and artworks into the blockchain to prevent illegal copying and usage. Simultaneously, the copyrights of photos and artworks can also be traded on the blockchain.
- **Education and research industry**. Educational institutions and research institutions can write the copyright information of their teaching materials and research results into the blockchain to prevent illegal copying and usage. Simultaneously, the copyrights of teaching materials and research results can also be traded on the blockchain.

These instances demonstrate that this architecture can be widely applied to various media content industries, effectively protecting and managing the copyrights of media content, improving the efficiency and transparency of copyright transactions, and reducing the cost of copyright management.

3.4 Challenges and limitations of the architecture

- **Technical challenges**. Integrating public and consortium blockchains with ChinaDRM may require complex technological development and integration work. Ensuring the security, performance, and scalability of the system is a challenge that requires effective encryption and identity verification mechanisms.
- **Regulatory issues**. When implementing the system, considerations must be given to compliance with relevant laws and regulations. Digital rights management and content sharing involve legal aspects such as copyright law and intellectual property protection, which need to be harmonized with existing regulatory frameworks.
- **Implementation challenges**. Introducing such a system into the real world may face implementation issues. Agreements and collaborations need to be reached with different media companies, content providers, copyright holders, and platforms. Additionally, achieving user acceptance, technological adaptability, and market adoption poses challenges for system popularization and promotion.
- **Data privacy and security**. Data privacy and security are crucial considerations in cross-platform media content sharing. Ensuring the security of user data and contents, as well as preventing unauthorized access and data breaches, require robust security measures and privacy protection mechanisms.

4 Integrated model for distributing audio-visual content based on an improved ChinaDRM

The integrated model of video and audio content distribution based on the improved ChinaDRM utilizes the public blockchain and the consortium blockchain to construct the audio-video (AV)-blockchain and combines the improved ChinaDRM to realize the trusted dissemination of decentralized video and audio content. The overall architecture of the model is shown in Fig. 4.

The model as a whole is divided into three parts:

- Public blockchain-consortium blockchain-DRM integrated server;
- Public chain-DRM integrated client;
- The middle layer that realizes information transmission and data interaction for the integration client and server.

The model can be further divided into the following five subsections.

4.1 DRM client component module

The DRM application module is responsible for integrating DRM functions with media playback applications. The DRM client application module

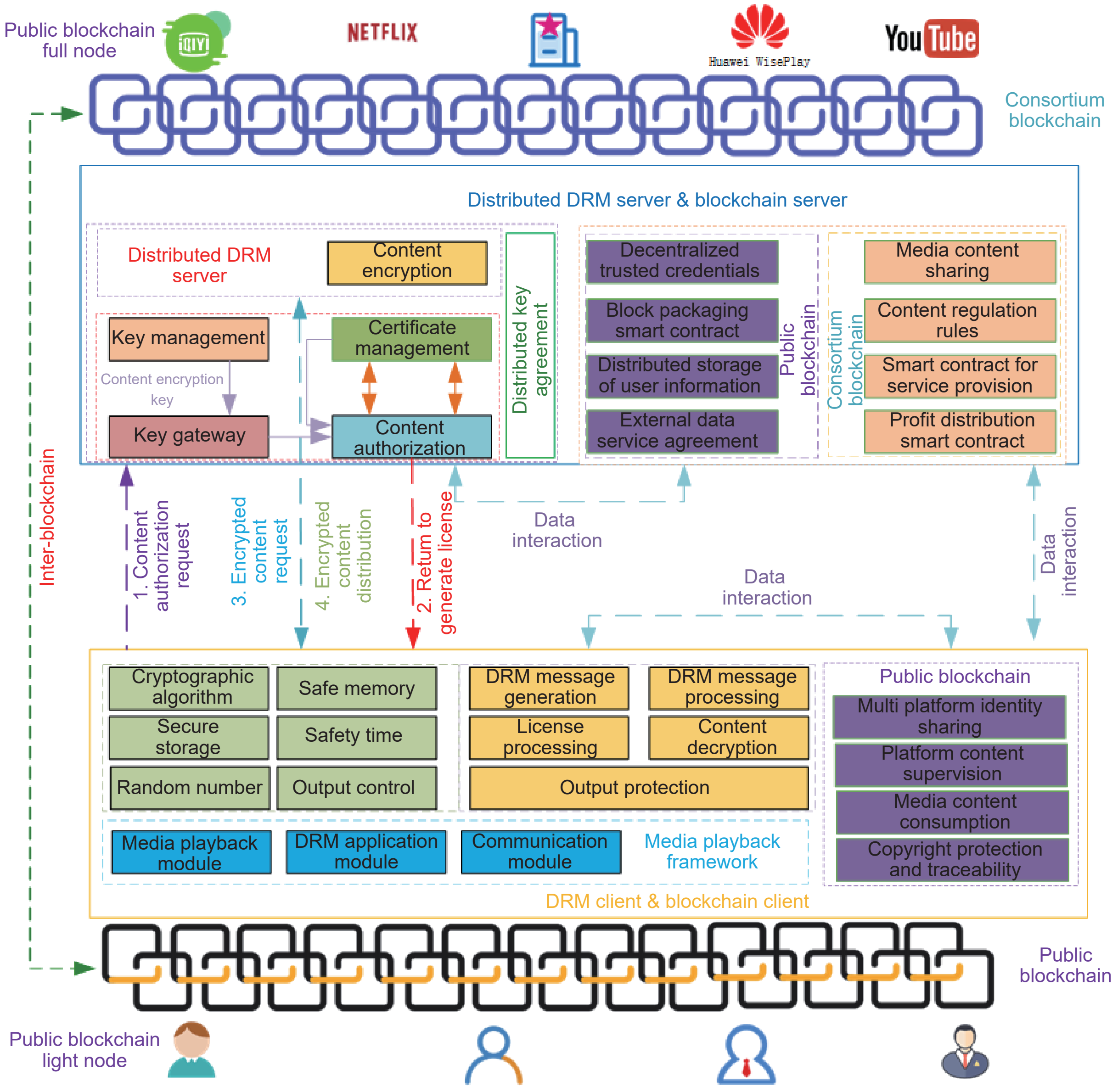

Fig. 4 Integrated model of video and audio content distribution based on AV-blockchain and ChinaDRM.

integrates with the media playback framework to support DRM through the DRM function interface.

The DRM function module provides DRM functionality to the DRM application module. The DRM function module runs in the DRM client runtime environment and implements the core functions of the DRM client by calling the DRM client runtime environment interface.

The DRM client runtime environment provides security capabilities for the DRM function module, establishes the trust and security system of the DRM client, and provides basic security protection for the operation of the DRM client core functions.

4.2 Blockchain client decentralized application

The blockchain client provides users with an entry point to participate in the platform, mainly providing the following functions:

- Decentralized identity sharing across multiple platforms;
- Supervision of mainstream media platforms, where users can supervise platforms through the public blockchain;
- Supervision of media content, where users can provide feedback on supervision through the public blockchain’s full nodes, including mainstream media platforms and national regulatory agencies;
- Ability to track and view the propagation path of original media content and prevent users from leaking media resources.

4.3 Distributed DRM server components

The content encryption module uses content encryption keys to protect audio and video content.

The key management module receives the content-encryption key and is responsible for synchronizing the key with the key gateway.

The key gateway module receives the synchronized key, securely stores the content-encryption key, and receives key queries from the content authorization module.

The content authorization module receives requests from DRM clients, securely sends licenses containing content-encryption keys and key usage rules to legitimate DRM clients. After receiving the license, the DRM client reasonably decrypts the content-encryption key according to the key usage rules and uses the content-encryption key to decrypt the media content for playback.

4.4 Public blockchain server

Decentralized trusted credentials generate decentralized identities for users, which support users to enjoy the same rights on multiple platforms and achieve a universal identity mechanism.

The blockchain consensus algorithm should mainly focus on how media platforms provide services, emphasizing load balancing and data consistency.

User information distributed storage should ensure that user data on various platforms are synchronized through the public blockchain while ensuring the privacy and security of user information.

The external data service protocol aims to negotiate with users the permissions and functions of external services (such as online or offline recommendations and calculations).

4.5 Consortium blockchain server

The consortium blockchain server aims to provide services for media platforms and national regulatory frameworks, including but not limited to the following functions:

Ensuring copyright sharing of media resources across various platforms, allowing users to access media resources on any platform;

National regulatory authorities can supervise media platforms based on content regulation rules;

Media platforms provide services and distribute benefits automatically through smart contracts.

5 Decentralized identity and multi-party verifiable credentials

5.1 Decentralized identity

The primary function of a traditional PKI public key is to bind the identity of the certificate holder and the related key pair, providing users with convenient certificate application and revocation functions and ensuring the integrity, non-repudiation and confidentiality of certificates[22]. The center of the PKI system is the CA server, which is required to be secure and reliable.

Decentralized identity (DID) is a user identity in the blockchain world. DID is a verifiable and tamper-resistant autonomous identity system which embodies the value of users in the blockchain world[23]. Compared with PKI, DID can prevent identity data from being controlled by a single central institution.

Currently, the most well-known standards for DID are the World Wide Web Consortium (W3C) and Decentralized Identity Foundation (DIF) standards. The DID identifier is a string in a specific format used to represent the digital identity of an entity[24]. According to the W3C DID standard, it can be divided into three parts: DID prefix, DID method, and DID unique identifier. An example of a DID instance is shown in Fig. 5.

This paper proposes an algorithm for generating DID, which encrypts the public key using SHA3-256 and Base-58 encryption algorithms. By adding identity type identification and other operations, DID can be generated in six steps. Identity type identification is used to distinguish different types of identities. The flowchart of the DID generation algorithm is shown in Fig. 6.

The decentralized identity DID generation algorithm is shown in Algorithm1.

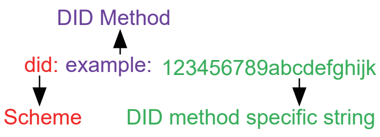
DID Method
did: example: 123456789abcdefghijk
Scheme
DID method specific string

Fig. 5 A DID instance

5.2 Decentralized verifiable credentials

In real life, a credential is used to identify a specific entity or to verify that an individual possesses certain attributes, qualifications, or claims. Credentials have the potential to provide users with greater security, flexibility, and freedom in the digital world[25].

Conventional verifiable credentials consist of four parts: the claim, credential identifier, issuer signature, and credential metadata. The structure of a conventional verifiable credential is illustrated in Fig. 7.

We need to replace the certificate identification code with DID, and improve the traditional verifiable certificate into a decentralized, verifiable certificate. The improved decentralized, verifiable credential structure based on DID is shown in Fig. 8.

Verifiable digital credentials are issued by the issuer and written into the blockchain. The digital credential holder can apply for an updated digital credential from the issuer. The verifier verifies the validity of the digital credential by comparing it with the data on the blockchain[26]. Verifiable digital credentials can enable national agencies to manage identity authorization on mainstream media platforms. At the same time, mainstream media platforms can also use verifiable digital credentials to manage user identity authorization. The primary mode of verifiable digital credentials is shown in Fig. 9.

Decentralized verifiable credentials can serve as universally applicable identity verification credentials

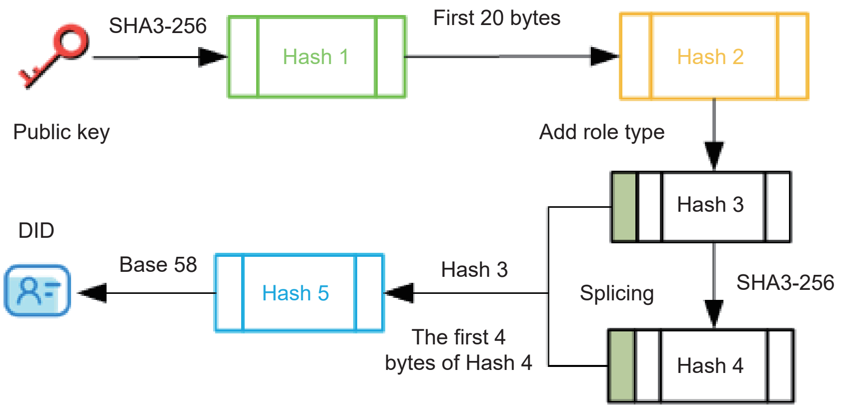

Fig. 6 Flow chart of DID generation process

Algorithm 1 DID generation algorithm

```
procedure GenerateDID (public key)
    Use the hash algorithm to convert the public key to Hash 1
    Intercept the first 20 bytes of Hash 1 as Hash 2
    Add character type bytes before Hash 2 to get Hash 3
    Use the hash algorithm to convert Hash 3 to Hash 4
    Merge the first 4 bytes of Hash 4 with Hash 3 to get Hash 5
    Use Base-58 algorithm to encode Hash 5 to get DID
    return DID
```

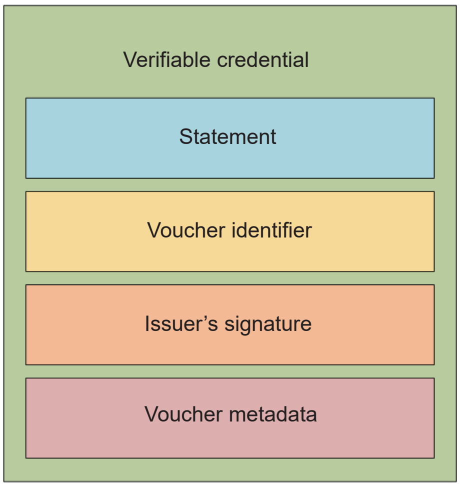

Fig. 7 Conventional verifiable credential structure diagram.

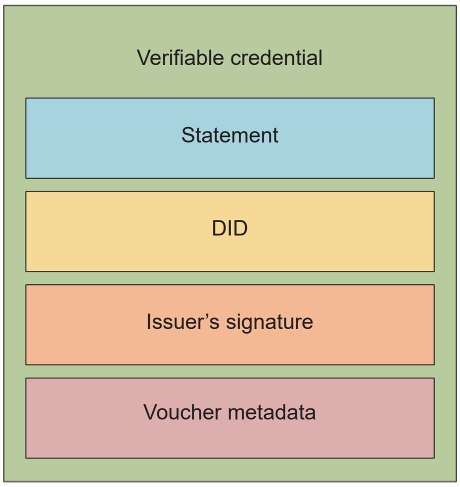

Fig. 8 Structure diagram of verifiable voucher based on DID improvement.

across multiple platforms, supporting unique verification by multiple parties, and can avoid the problems of verification delays, non-recognition of credentials, and information forgery caused by centralized verification[27].

6 Distributed encryption and decryption distribution of media content

6.1 Key negotiation and distributed level encryption

6.1.1 Shamir secret sharing algorithm

The Shamir secret sharing algorithm divides the secret into n sub-secrets[28]. Any k sub-secrets can recover the original secret, but any $k-1$ sub-secrets cannot recover the original secret.

The encryption process is as follows:

- Suppose there is a secret S, S is a number. When the secret is a vector, it needs to be encoded, decoded, split, and concatenated. Choose random numbers $a_1, a_2, ..., a_{k-1}$ and P, P is a large prime, and $S<P$. Construct a polynomial (Eq. (1)), where $a_0=S$.

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1} \bmod (p) \tag{1}$$

- Randomly select n numbers $x_1, x_1, ..., x_n$, Then substitute them into Eq. (1) to obtain $f(x_1)$, $f(x_2)$, $\ldots$, $f(x_n)$. Finally, store $(x_1,f(x_1))$, $(x_2,f(x_2))$, ..., $(x_n,f(x_n))$ in n servers.

The decryption process is as follows:

- Select data $(x_1,f(x_1))$, $(x_2,f(x_2))$, ..., $(x_n,f(x_n))$ from k servers arbitrarily, and replace it with Eq. (1), obtaining Formula (2).

$$\begin{gathered}\begin{pmatrix}1 & x_1 & \cdots & x_1^{k-1}\\ 1 & x_2 & \cdots & x_2^{k-1}\\ 1 & x_k & \cdots & x_k^{k-1}\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_{k-1}\end{pmatrix}=\begin{pmatrix}f(x_1)\\ f(x_2)\\ f(x_{k-1})\end{pmatrix}\rightarrow\\ \begin{pmatrix}a_0\\ a_1\\ a_{k-1}\end{pmatrix}=\begin{pmatrix}1 & x_1 & \cdots & x_1^{k-1}\\ 1 & x_2 & \cdots & x_2^{k-1}\\ 1 & x_k & \cdots & x_k^{k-1}\end{pmatrix}\begin{pmatrix}f(x_1)\\ f(x_2)\\ f(x_{k-1})\end{pmatrix}\end{gathered} \tag{2}$$

- Solve Formula (2) to get $a_1, a_2, ..., a_{k-1}$, and substitute them into Eq. (1). Let $x=0$ to get the original secret $S=a_0$.

6.1.2 Improved Diffie−Hellman key agreement protocol

The Diffie−Hellman key exchange algorithm refers to the generation of a shared secret key between two parties by exchanging publicly available information only. Due to the uncertainty of the identity information between the two communicating parties, the Diffie−Hellman algorithm is susceptible to block

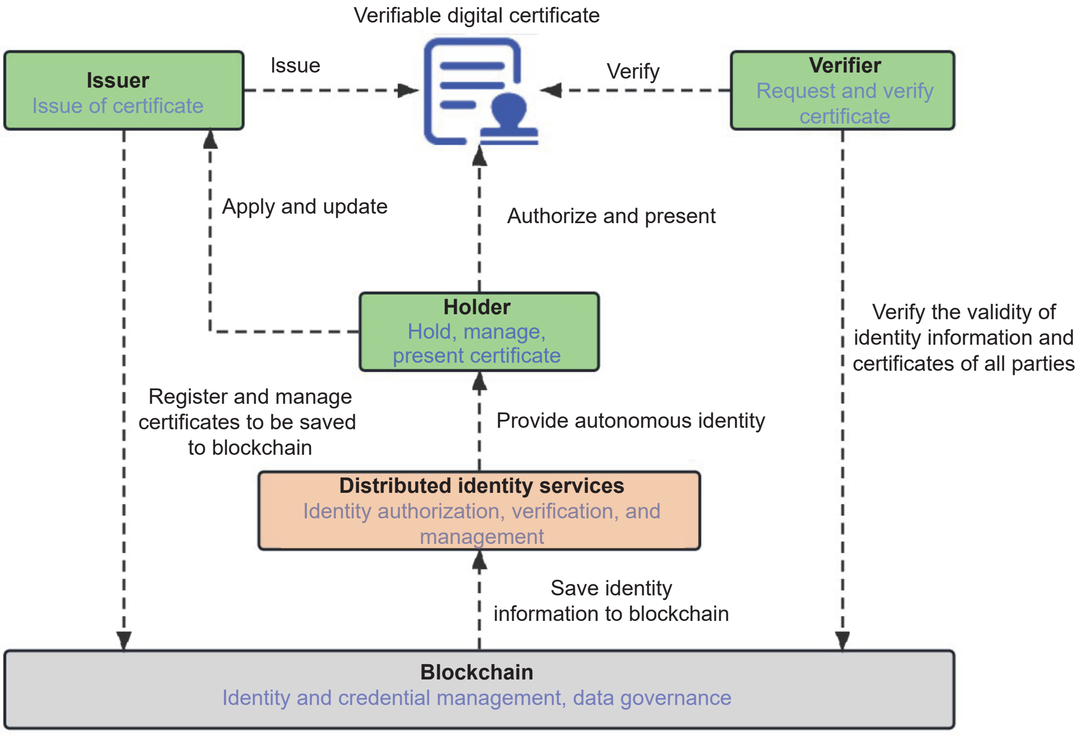
Verifiable digital certificate
Issuer
Issue of certificate
Issue
Verify
Verifier
Request and verify certificate
Apply and update
Authorize and present
Holder
Hold, manage, present certificate
Verify the validity of identity information and certificates of all parties
Register and manage certificates to be saved to blockchain
Provide autonomous identity
Distributed identity services
Identity authorization, verification, and management
Save identity information to blockchain
Blockchain
Identity and credential management, data governance

Fig. 9 Basic schema diagram of verifiable digital credentials.

attacks, replay attacks, and man-in-the-middle attacks[29].

The steps of the improved Diffie–Hellman key exchange are as follows:

- The user and the server negotiate to obtain a large prime number P and a generator G of P, $2 \leqslant G \leqslant P-1$. At the same time, use P to generate Q and $Q^{-1} \bmod (P-1)$, Q and $Q^{-1} \bmod (P-1)$ are coprime. In order to suitable for the characteristics of blockchain, P and Q are generated by Shamir algorithm.
- The user generates a random number A that satisfies the condition $1 \leqslant A \leqslant P-1$. Then calculate $X_1 = G^{A\cdot Q} \bmod P$ and $X_2 = G^{A^2\cdot Q} \bmod P$, send the calculation results to server. The server generates a private random number B, $1 \leqslant B \leqslant P-1$. Then calculate $Y_1 = G^{B\cdot Q} \bmod P$ and $Y_2 = G^{B^2\cdot Q} \bmod P$, send the calculation results to user.
- The user calculates $X = Y_1^{Q-1}$ and $K_a = X^A \bmod P$ to get the secret key K_a. Then calculate $Key_a = \left(\left(Y_2^{Q^{-1}}\right)^A\right)^{Q^{-1}} \bmod P$, send $\text{hash}(Key_a)$ to the server. The server calculates $Y = X_1^{Q^{-1}} \bmod P$ and $K_b = Y^B \bmod P$togetthesecretkeyK_b.Thencalculate$Key_b =$ $\left(\left(X_2^{Q^{-1}}\right)^B\right)^{Q^{-1}} \bmod P$, send $\text{hash}(Key_b)$ to the user.
- The user verifies that $\text{hash}(Key_b)$ and $\text{hash}((K_a)^{A\cdot Q^{-1}})$ $\bmod P$ are equal. The server verifies that $\text{hash}(Key_a)$ and $\text{hash}((K_b)^{B\cdot Q^{-1}}) \bmod P$ are equal.

The improved Diffie–Hellman algorithm is more suitable for the characteristics of blockchain and can prevent man-in-the-middle attacks. By using the improved key negotiation protocol, a mechanism based on the association of hierarchical keys and key usage rules can be achieved to achieve permission authorization for content. Logically, keys can be divided into multiple levels according to the order of encryption protection, and the key that encrypts the current key is called the superior key[30]. Each level of key has corresponding key usage rules, and the current key can only be decrypted under the conditions specified by the superior key usage rules. Each key may have multiple key usage rules, and the key can only be used when all its usage rules are met. The content authorization mechanism of the audio-visual content distribution integrated model is shown in Fig. 10.

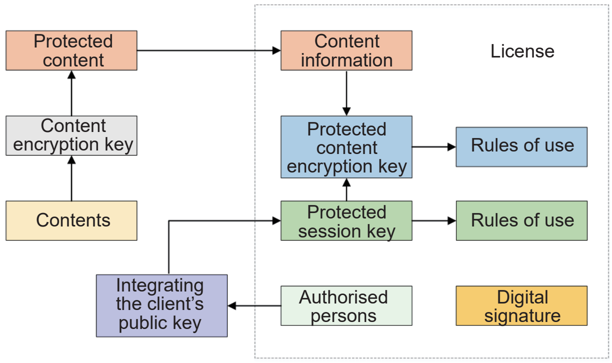

Fig. 10 Content authorization mechanism diagram.

6.2 Key management and video and audio content encryption and decryption

6.2.1 Content authorization mechanism

The integrated model of audiovisual content distribution based on the audiovisual chain has asymmetric key pairs for both the integrated user and service sides. Since blockchain inherently includes an asymmetric key mechanism, the integrated client and integrated service can directly utilize the key mechanism provided by the blockchain. The integrated service side uses a symmetric encryption algorithm to encrypt the content and encapsulates the encrypted content key in the license, which is then sent to the integrated client. The key management mechanism of the audiovisual chain-based audiovisual content distribution integrated model is shown in Fig. 11.

The audiovisual content is encrypted using a symmetric encryption algorithm. The encryption and decryption process of the audiovisual content is as follows:

- The integrated service end generates a session key and uses the session key to encrypt the content-encryption key.
- The integrated service end encrypts the session key using the public key of the integrated client.
- If the content-encryption key needs to be synchronized to the key gateway, the key gateway public key is used for encryption.
- The integrated service end packages the encrypted session and content-encryption keys into a license and sends the package to the integrated client. The license uses a message authentication code to ensure the integrity of the license.
- The integrated client decrypts the session key using the private key of the integrated client after receiving the license and then uses the decrypted session key to decrypt the content-encryption key.
- The integrated client decrypts the content-encryption key and uses it to decrypt the content, achieving decoding and playback.

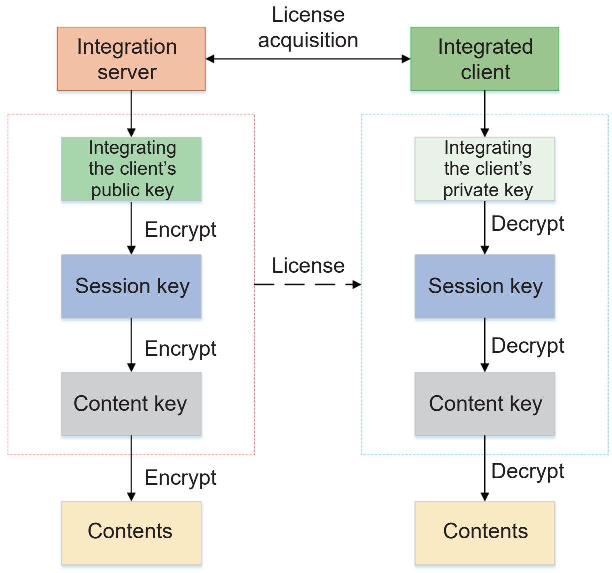

Fig. 11 Diagram of key management mechanism.

6.2.2 License structure

The license for digital rights management is composed of a license index unit, content unit, authorized object unit, content encryption key unit, key usage rule unit, session key unit, message verification code key unit, and digital signature unit. The license architecture is shown in Fig. 12.

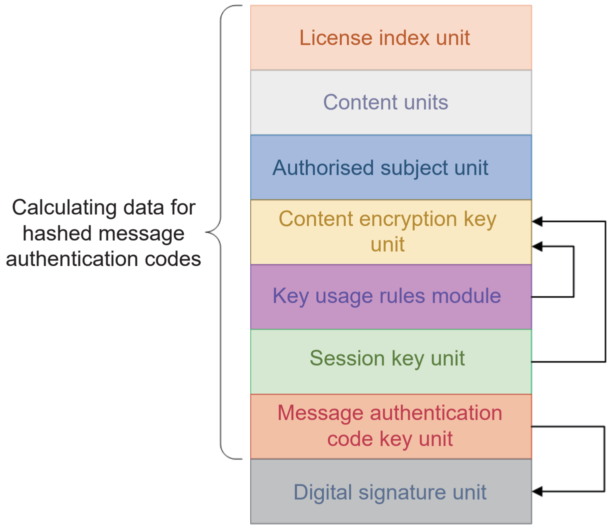
License index unit
Content units
Authorised subject unit
Content encryption key unit
Key usage rules module
Session key unit
Message authentication code key unit
Digital signature unit
Calculating data for hashed message authentication codes

Fig. 12 License architecture diagram.

- License index unit. The license index unit includes a version number, license number, basic unit quantity, and timestamp. The license comprises multiple independent units with different types and quantities identified by the license index unit.
- Content unit. This unit includes data length, content identification, and unique identification of the key unit. Multiple key units can correspond to a content unit.
- Authorized object unit. The authorized object is the bearer of the specified content-related rights. The authorized object is described by its unique identification. The authorized object unit includes the authorized object type and authorized object.
- Content encryption key unit. The key unit includes the key algorithm, key data, key type, key identification, and information about the key type and key identification used to encrypt the key.
- Key usage rule unit. The key usage rule specifies that the authorized object should use the key reasonably according to the key usage rule. The key usage rule unit includes key identification and usage rule. The key usage rule unit corresponds to the key unit through the unique identification of the key unit.
- Session key unit. The integrated server generates a random session key, a symmetric key used to encrypt the content-encryption key.
- Message verification code key unit. Generate a random message verification code key, use this key to generate a hashed message verification code, and protect the integrity of the license.
- Digital signature unit. The digital signature unit signs all the previous unit data to ensure data integrity.

7 Conclusion

This paper proposes a video and audio content distribution integration model based on the audio-visual blockchain and an improved version of ChinaDRM, which binds multiple media platforms with the national supervisory agency to form an consortium node. In order to ensure user rights and support multi-platform identity sharing, the paper proposes to coordinate the consortium chain and public blockchain to achieve inter-blockchain information interaction. By utilizing the inherent security mechanisms of blockchain, such as keys and certificates, the authors improve ChinaDRM and implement a trusted media content propagation framework. Through analysis, the proposed model in this paper has strong practicality and can solve some problems existing in the field of audio-visual. In the future, the proposed model architecture will be applied in practice to achieve trusted media content propagation and multi-platform resource sharing.

Acknowledgment

This work was partly supported by the Fundamental Research Funds for the Central Universities (No. CUC230A013).

References

[1] S. Yang, Y. Zhao, and Y. Ma, Analysis of the reasons and development of short video application——Taking Tik Tok as an example, in *Proc. 9th Int. Conf. Information and Social Science* (*ICISS 2019*), Manila, Philippines, 2019, pp. 12–14.

[2] F. Casino, T. K. Dasaklis, and C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics Inform.*, vol. 36, pp. 55–81, 2019.

[3] Y. Zhai and L. Zhao, DRM licensing design for interactive rebuilding of DTV in China, in *Proc. 2010 7th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, 2010, pp. 1–5.

[4] W. Sun, H. Fang, S. Zheng, and Q. Qian, Blockchain and homomorphic encryption for digital copyright protection, in *Proc. 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking* (*ISPA/BDCloud/SocialCom/SustainCom*), Exeter, UK, 2021, pp. 754–761.

[5] Z. Chen, Y. Wang, and T. Ni, DCDChain: A credible architecture of digital copyright detection based on blockchain, arXiv preprint arXiv: 2010.01235, 2020.

[6] F. Miao, W. Yang, W. Fan, Y. Xie, Q. Guo, Y. You, Z. Liu, and L. Liu, Digital copyright works management system based on DOSA, in *Proc. 2nd Int. Conf. Computer Science and Application Engineering*, Hohhot, China, 2018, pp. 1–9.

[7] Z. Xu, L. Wei, J. Wu, and C. Long, A blockchain-based digital copyright protection system with security and efficiency, in *Proc. 3rd CCF China Blockchain Conf.*, Jinan, China, 2020, pp. 34–49.

[8] W. Liang, X. Lei, K. C. Li, Y. Fan, and J. Cai, A dual-chain digital copyright registration and transaction system based on blockchain technology, in *Proc. 1st Int. Conf. Blockchain and Trustworthy Systems*, Guangzhou, China, 2019, pp. 702–714.

[9] P. Wang, Y. Li, F. Li, X. Dong, and P. Chen, Secure and traceable copyright management system based on blockchain, in *Proc. 2019 IEEE 5th Int. Conf. Computer and Communications* (*ICCC*), Chengdu, China, 2020, pp. 1243–1247.

[10] Z. Chen, Y. Wang, T. Ni, and H. Zhong, DCDChain: A credible architecture of digital copyright detection based on blockchain, arXiv preprint arXiv: 2010.01235, 2020.

[11] K. O. B. O. Agyekum, Q. Xia, Y. Liu, H. Pu, C. N. A. Cobblah, G. A. Kusi, H. Yang, and J. Gao, Digital media copyright and content protection using IPFS and blockchain, in *Proc. 10th Int. Conf. Image and Graphics* (*ICIG*), Beijing, China, 2019, pp. 266–277.

[12] Y. Ding, L. Yang, W. Shi, and X. Duan, The digital copyright management system based on blockchain, in *Proc. IEEE 2nd Int. Conf. Computer and Communication Engineering Technology* (*CCET*), Beijing, China, 2020, pp. 63–68.

[13] C. Zhao, M. Liu, Y. Yang, F. Zhao, and S. Chen, Toward a blockchain based image network copyright transaction protection approach, in *Proc. 2nd Int. Conf. Security with Intelligent Computing and Big Data Services*, Guilin, China, 2018, pp. 17–28.

[14] Y. Zhou, W. Lin, H. Wang, and P. Jiang, A TS bitstream parsing system for ChinaDRM, in *Proc. 2019 IEEE/ACIS 18th Int. Conf. Computer and Information Science* (*ICIS*), Beijing, China, 2019, pp. 279–284.

[15] Y. Zhou and W. Lin, Partitioning and decryption methods for ChinaDRM standards-compliant encrypted bitstreams, in *Proc. 2020 Int. Conf. Culture-oriented Science & Technology* (*ICCST*), Beijing, China, 2020, pp. 468–472.

[16] J. Zhang, W. Lin, and W. Shang, A rights expression model and a license structure for ChinaDRM, in *Proc. 2019 IEEE/ACIS 18th Int. Conf. Computer and Information Science* (*ICIS*), Beijing, China, 2019, pp. 360–365.

[17] National Library of Standards, *Technical specification of digital rights management for internet television*, GY/T 277-2014, 2014.

[18] T. Jiang, A. Sui, W. Lin, and P. Han, Research on the application of blockchain in copyright protection, in *Proc. 2020 Int. Conf. Culture-oriented Science & Technology* (*ICCST*), Beijing, China, 2020, pp. 616–621.

[19] Amazon, Digital rights management, https://docs.aws.amazon.com/pdfs/elastictranscoder/latest/developerguide/elastictranscoder-dg.pdf#drm, 2023.

[20] Microsoft Corporation, PlayReady Specification for Windows Media DRM 10, 2022.

[21] W. Lin, N. Zhang, and S. Liu, A metadata-based interoperable digital rights management system architecture, in *Proc. 3rd Int. Joint Conf. Computational Science and Optimization* (*CSO 2010*), Huangshan, China, 2010, pp. 432–434.

[22] E. F. Kfoury, D. Khoury, A. AlSabeh, J. Gomez, J. Crichigno, and E. Bou-Harb, A blockchain-based method for decentralizing the ACME protocol to enhance trust in PKI, in *Proc. 2020 43rd Int. Conf. Telecommunications and Signal Processing* (*TSP*), Milan, Italy, 2020, pp. 461–465.

[23] D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller, CanDID: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability, in *Proc. 2021 IEEE Symp. Security and Privacy* (*SP*), San Francisco, CA, USA, 2021, pp. 1348–1366.

[24] W3C, Decentralized identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/, 2022.

[25] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, Digital identities and verifiable credentials, *Bus. Inf. Syst. Eng.*, vol. 63, no. 5, pp. 603–613, 2021.

[26] R. Mukta, J. Martens, H. Y. Paik, Q. Lu, and S. S. Kanhere, Blockchain-based verifiable credential sharing with selective disclosure, in *Proc. 2020 IEEE 19th Int. Conf. Trust, Security and Privacy in Computing and Communications* (*TrustCom*), Guangzhou, China, 2021, pp. 959–966.

[27] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, and F. Matthes, DID and VC: Untangling decentralized identifiers and verifiable credentials for the web of trust, in *Proc. 2020 3rd Int. Conf. Blockchain Technology and Applications*, Xi’an, China, 2020, pp. 61–66.

[28] P. Barrett, Implementing the rivest Shamir and adleman public key encryption algorithm on a standard digital signal processor, in *Proc. 6th Annu. Int. Cryptology Conf.*, Santa Barbara, CA, USA, 1986, pp. 311–323.

[29] U. M. Maurer and S. Wolf, The diffie-hellman protocol, *Des. Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 147–171, 2000.

[30] G. Ateniese, A. De Santis, A. L. Ferrara, and B. Masucci, Provably-secure time-bound hierarchical key assignment schemes, in *Proc. 13th ACM Conf. Computer and Communications Security*, Alexandria, VA, USA, 2006, pp. 288–297.

Wenqian Shang received the BS degree from Southeast University, China, in 1994, the MS degree from National University of Defense Technology, China, in 1999, and the PhD degree from Beijing Jiaotong University, China, in 2008. She finished the postdoctoral work in Communication University of China in 2013. Her current appointment is a professor at the Communication University of China. She is the program chair of IEEE/ACIS ICCIS 2019, and the conference chair of CSII 2021. She has published more than 60 journal/conference papers, such as *Expert Systems with Applications*, *Journal of Computer Research and Development*, and so on. Her current research interests include artificial intelligence (AI), machine learning, and NLP.

Zaifu Yu received the BS degree in computer science and technology from Northeast Petroleum University, China, in 2020. He is currently pursuing the MS degree in big data technology at Communication University of China. He has engaged in knowledge graph research during undergraduate studies and blockchain research during postgraduate studies, with a total of 6 published papers. His current research interests include blockchain, privacy protection, and data copyright protection.