Research on the Application of Blockchain in Copyright Protection

Tao Jiang
School of Computer Science and Cybersecurity
Communication University of China,
Beijing, China
jiang.tao@cuc.edu.cn

Aina Sui*
School of Computer Science and Cybersecurity
Communication University of China,
Beijing, China
aina@cuc.edu.cn

Weiguo Lin
School of Computer Science and Cybersecurity
Communication University of China,
Beijing, China
linwei@cuc.edu.cn

Pengbin Han
School of Computer Science and Cybersecurity
Communication University of China,
Beijing, China
1083854239@qq.com

Abstract—In recent years, the total number of digital media works issued has continued to increase. Due to the easy copying and dissemination of digital copyright works, digital copyright infringement has become increasingly serious. Because of the security, traceability, distribution, and programmable features of blockchain technology fully meet the needs of copyright protection, research on copyright protection based on blockchain technology has gradually become a popular research direction for many scholars. This article introduces the principles, characteristics and classification of blockchain technology in detail. It also deeply analyzes the research status, key technologies and research difficulties of copyright protection technology. In addition, this article has conducted a detailed study on the copyright protection technology based on the blockchain, and implemented a safe, efficient, and lightweight copyright protection system based on the alliance chain.

Keywords-component; Blockchain; Digital rights management; Copyright protection; Copyright forensics;

I. RESEARCH ON BLOCKCHAIN TECHNOLOGY

A. The development of blockchain

The concept of blockchain was first proposed by Satoshi Nakamoto in 2008 [1]. After the publication of Satoshi Nakamoto's paper, the world's first crypto currency appeared in 2009: Bitcoin, which is completely anonymous in the Bitcoin system. Network users have realized point-to-point transactions [2].

Up to now, the development stage of blockchain can be summarized as the following three: blockchain 1.0, 2.0 and 3.0 [3]. In the era of blockchain 1.0, crypto currency was deployed as a peer-to-peer transaction system. It provided a solution to the decentralization of currency and payment. The typical application of blockchain during this period was various types of digital currencies. In the blockchain 2.0 era, more widely used blockchain applications are realized through the invocation of "intelligent contracts". Blockchain 2.0, represented by Ethereum, provides a trusted execution environment for intelligent contracts, making automatic and intelligent operation of contracts possible. Since then, blockchain has realized the true programmability. The blockchain 3.0 era is an idealized vision of the future digital currency economy. In Blockchain 3.0, assets can be truly on-chain, and the blockchain can create a trustless, decentralized, and computing-capable automation platform to promote large-scale collaboration in the fields of government affairs, science, health, education, culture, and arts. Blockchain technology is currently in the stage of development from 2.0 to 3.0.

B. Blockchain principle and characteristics analysis

Blockchain is a distributed database system involving multiple nodes [4]. In this system, each node exists independently and jointly maintains the ledger. In the blockchain, all transactions are packaged as data blocks according to specific rules, and each block contains transaction data, time stamp, and the hash value of the previous block. A record chain is formed between each block according to the cryptography principle. All transaction data in the blockchain is organized into an ordered block list, and the submitted block information can no longer be tampered with in any way [5]. Blockchain is essentially a software solution for transmitting and recording data: it can realize the real-time, security and credibility of data recording in a large-scale unreliable distributed network. The characteristics of blockchain are analyzed as follows:

1) Distributed and decentralized

Compared with the traditional server and client request calling mode, the blockchain system uses a distributed storage model, which has better security and resistance to attack.

2) Security and tamper-proof

All blocks are linked based on cryptographic hashing algorithm, and the data in the block is stored using the Merkle tree model, which guarantees the security and non-tampering of the data on the chain [6].

3) Traceability

Every block in the blockchain system has a time stamp. Since the creation block, every transaction in the system has been saved in the block after adding the time dimension. All transactions in the system are traceable.

4) De-trust mechanism

In the blockchain transaction system, both parties to the transaction can complete the transaction point-to-point without relying on trusted third parties to establish trust in advance. The consensus algorithm and transaction data between the systems are completely transparent, ensuring the security and trust of the transaction.
5) Programmability

Since blockchain 2.0, the blockchain system has provided a trusted operating environment for smart contracts, and supported the development of decentralized application layer service scripts on the chain, which has achieved on-chain programmability [7].

C. Blockchain classification

According to the access mechanism, the blockchain can be divided into three types: "public chain", "private chain" and "alliance chain".

"Public chain" allows all individuals or organizations to use and participate in maintenance freely. The information is completely open and transparent. It is a completely decentralized distributed network. The topological relationship between all nodes on the public chain is the same level and flat. The Bitcoin network is a typical representative of the public chain. In certain application scenarios, the public chain has defects that are difficult to supervise.

"Private chain" is a completely privatized blockchain. It uses a consensus mechanism to complete the bookkeeping work. The account book is only open to private personnel. In the private chain, the bookkeeping rights are completed by the nodes designated by the system. Such a network is only partially decentralized and has the characteristics of high efficiency, but it does not completely solve the problem of trust.

"Alliance chain" is between "public chain" and "private chain". It is usually controlled by multiple authoritative centers designated by the system, with high access threshold and access control. Every node in the alliance chain needs to register and participate, part of it is decentralized, part of the data is public, it has the characteristics of distributed, decentralized, tamper-proof and easy to supervise, which is the current mainstream development direction of blockchain.

II. RESEARCH ON DIGITAL COPYRIGHT PROTECTION TECHNOLOGY

A. Current research

In recent years, the media industry has been booming, and the distribution of digital media content has become more and more widespread. Digital media content usually refers to electronic content such as video, audio, text, and pictures. It has the characteristics of high production cost and low forwarding cost. The piracy and infringement of digital media products greatly damage the creative enthusiasm and economic interests of copyright creators, and have a great negative impact on the economic and cultural of the whole society [8].

With the continuous development of the digital media industry, Digital Right Management (DRM), which combines technology, law, business and other multi-level concepts, has also been proposed by scholars for the protection of digital content copyright [9]. Most of the original digital copyright protection technologies focused only on encryption and authorization technologies, and now digital copyright protection has transitioned to the protection of the overall distribution process of media products to ensure that digital content is legally used throughout the life cycle. Up to now, many technology companies at home and abroad have launched copyright protection products, such as foreign Microsoft, Inter, IBM, Adobe, domestic Huawei, Peking University Founder, etc. In addition, domestic universities and scientific research institutions represented by Tsinghua University, Peking University, the Academy of Broadcasting Sciences of the National Radio and Television administration, and the Institute of Computing Technology of the Chinese Academy of Sciences are also actively exploring in the field of digital copyright protection.

B. Key technologies of digital copyright protection

At present, digital copyright protection technology can be roughly divided into two categories: one is to encrypt digital content, and use encryption technology to cooperate with the power grant mechanism to achieve the safe distribution of copyright works and use [10]. Typical application cases include Microsoft's WMRM, ChinaDRM program proposed by the Academy of Broadcasting Sciences, etc. Another kind of copyright protection technology is to trace and anti-counterfeit identification of copyright works through digital identification. Representative applications include digital watermarks, digital fingerprints, Digital Object Unique Identifier (DOI) standards, and Digital Copyright Identifier (DCI), etc.

The first copyright protection method for encrypting digital content acts on the entire life cycle of copyright product distribution. The core idea is to use cryptography technology to protect the legal use of copyright works by using digital licenses. For example, ChinaDRM copyright protection scheme is based on cryptography, PKI (Public Key Infrastructure) technology and authorization technology to define the logical architecture, content authorization method, key management method, security mechanism and trust model of digital rights management server and client. Furthermore, a set of digital rights management system for video and audio content distribution from server to client is constructed.

The full-cycle digital copyright protection technology which relies on digital licenses has good protection effects, but it also has high design and use costs. At the same time, full-cycle copyright protection products are mostly devoted to copyright protection in the process of work distribution, and it is difficult to provide support for copyright protection needs that have traceability and evidence collection requirements. The current copyright market also has a great need for high-performance, lightweight and low-cost digital copyright protection systems. The digital copyright protection method based on blockchain technology is usually a lightweight copyright protection scheme based on digital identifiers to achieve anti-counterfeiting and traceability of copyright.

C. Research on the Difficulties of Copyright Protection

The difficulties in copyright protection mainly lie in the four aspects of copyright establishment, infringement detection, evidence collection, and judicial rights protection.
In terms of copyright establishment, the traditional method is to determine the copyright by a credible third-party copyright center, but this method generally has the problems of complicated verification process, long verification time and high cost.

In terms of infringement detection, the current mainstream method is through the combination of human and AI (Artificial Intelligence) detection. Although the introduction of artificial intelligence detection technology has greatly improved the efficiency and accuracy of manual detection, infringement detection still has the problems of high difficulty in monitoring and difficulty in tracking cross-region overseas storage.

In terms of evidence collection, the traditional methods are mostly accompanied by notaries. Self-forensic behavior is generally not certified. Under traditional methods, the cost of obtaining evidence by impartial personnel and professional legal services is generally high and the timeliness is difficult to be guaranteed.

In the process of judicial rights protection, the traditional practice is usually through civil, criminal, administrative means to solve in the form of litigation. Among them, there is the problem that ordinary rights holders lack awareness and ability to defend rights, and the lawsuit means to defend rights also require more time and economic costs.

III. DIGITAL COPYRIGHT PROTECTION BASED ON BLOCKCHAIN

A. Current research

Since the blockchain technology was proposed, because of its safe and reliable, tamper-proof, traceable characteristics and the ingenious fit of copyright requirements, research on copyright protection based on blockchain technology has been a popular research direction of many experts and scholars. In the past three years, famous universities and technology companies such as Wuhan University, Beijing University of Posts and Telecommunications, Shenzhen University, Alibaba, Iqiyi, and Hangzhou Qulian Technology have made remarkable achievements in the research on the copyright protection scenarios of blockchain technology landing. Major domestic universities have always maintained research on the underlying consensus mechanism and encryption algorithm of the blockchain, and many universities have established their own copyright protection systems based on the public chain and alliance chain technology.

Based on blockchain technology, Jiang Ming and others from Beijing University of Posts and Telecommunications proposed a digital copyright protection scheme that supports high-trust content protection and information traceability[11]. The copyright protection scheme uses two independent application interfaces to separate the protected copyright content plain text and the summary information of the works are stored on the chain to achieve efficient and safe copyright certificate storage and privacy protection. At the same time, the scheme is also based on ring signatures and other cryptographic knowledge technologies to achieve identity authentication and license authorization, Copyright tracing and other businesses are a reliable, efficient and safe practice of blockchain technology in the field of copyright protection. The Shenzhen University Blockchain Technology Research Center started with the underlying technology of the blockchain, based on advanced knowledge of cryptography such as zero-knowledge proofs and ring signatures, combined with discrete hash hashes, reversible Bloom lookup tables, SDN and other network technologies. A high-performance licensed public chain, supplemented by digital fingerprint technology, the team realized the functions of displaying, depositing and distributing digital works in this public chain environment. Alibaba company has now launched a blockchain protection solution for commercial use. Its solution relies on Alibaba Cloud deployment and is based on the ant blockchain baas architecture. It provides users with original registration, copyright monitoring, electronic evidence collection and notarization. The whole process of copyright protection such as judicial litigation. Iqiyi company has also launched a blockchain-based copyright certification function, which is based on blockchain technology and AI technology. Non-tampering and high credibility, providing safe and reliable copyright protection services for original works.

B. Advantages

Using the anti-tampering feature of the blockchain, it is possible to secure the forensics and traceability of work copyright. Using smart contract technology can effectively realize the copyright transaction business, which can further promote the commercialization of copyright content. On the premise of solving data integrity and privacy protection[12], digital fingerprints of electronic data should be stored on the chain beforehand to facilitate verification when disputes arise. Compared with traditional copyright protection technology, blockchain can realize copyright traceability, certificate storage and anti-counterfeiting requirements more efficiently, lightly and cost-effectively.

The advantages of blockchain in the field of copyright protection are summarized as follows:

a) Multi-center, information cannot be tampered, and credibility of deposit certificate.
b) All transaction data and copyright data is stored on the chain with the time dimension, which can be traced accurately.
c) The digital fingerprint of the work can be uploaded at the creation stage of the work, and the copyright of the work is protected throughout the creation cycle.
d) Each node can have a ledger, the data is more transparent[13].
e) Smart contracts support efficient digital copyright transactions and multiple distributions[14].
f) Based on the alliance chain technology, it can communicate with the upstream and downstream of the industry, which is convenient for monitoring and more open[15].
The system is automatically executed, and the decentralization of some links greatly reduces the cost of copyright protection.

IV. DESIGN AND IMPLEMENTATION OF DIGITAL COPYRIGHT PROTECTION SYSTEM BASED ON BLOCKCHAIN

A. Development framework analysis

Different development frameworks will support different consensus algorithms and privacy protection mechanisms. Currently in the blockchain development framework that supports smart contracts, Ethereum and Fabric are the two mainstream development frameworks. For the digital copyright protection scene, this article focuses on comparing Ethereum and Fabric.

Ethereum technology is based on open source distributed public chain network, following the concept of unauthorized, public, private, developers can use intelligent contracts to build decentralized applications in Ethereum. Ethereum based on public chain is difficult to monitor, there are also many hidden dangers in privacy protection. The consensus mechanism of Ethereum is based on the proof-of-work mining mechanism. All nodes, regardless of whether they participate in a particular transaction or not, must agree on a common ledger, which will adversely affect the processing performance of some nodes [16].

Fabric is an authorized and privatized blockchain application framework based on the alliance chain. It adopts a loosely coupled design and modularizes components such as consensus mechanism and identity verification. In terms of consensus mechanism, Fabric has a more elaborate design and provides a wide range of consensus understanding. It divides the role of nodes and provides more fine-grained access control. Fabric introduces the concept of channels, and access to transactions is limited to related parties, achieving consensus at the transaction level, maximizing privacy protection and improving node performance.

Combined with the above research, in terms of copyright protection application scenarios, Fabric is the most suitable open source framework at the moment.

B. System architecture design

Based on the idea of copyright protection for depositing evidence in advance and going to the blockchain for evidence collection when disputes arise, the copyright protection system implemented this time should be able to achieve the core functions of user registration, copyright work deposit, copyright work transaction, copyright work query and transaction records.

In this experiment, the design of the blockchain-based copyright protection system uses a four-layer structure: access layer, business layer, blockchain layer, and middleware. The access layer provides the system's visual interaction function; the business layer realizes the copyright preservation business through the execution of copyright registration and trading operations; the blockchain layer relies on the Fabric alliance chain technology to manage identity, account books, transactions and other information; Middleware is responsible for providing information storage function. Such a system design can not only realize the on-chain certification and traceability of important fingerprint information of copyright works, but also can view the content of copyright works in the media database through middleware.

For the division of functional modules, this experiment designed a front-end display module, a blockchain interaction module, and a database storage module. The front-end display module is responsible for the visual display of data, the blockchain interaction module is responsible for certificate management of important copyright information, and the database storage module is responsible for local storage of copyright works. The interactive relationship between each functional module is shown in the following figure.

C. Chain code design

The programmability of Blockchain 2.0 is directly reflected in the smart contract. Based on the call of the smart contract, the blockchain system can realize the automatic operation. In the design of the smart contract, the business entity needs to be abstracted and the business logic should be reasonably functionalized. In Fabric, chain code is the smart contract. This experiment abstracted three entities implemented in the Fabric chain code layer, namely: user, work, and transaction record.

Users refer to person who are allowed to enter the system to view copyright works and participate in transactions. Users have attributes such as {Name, Id, Works}. Name is the user's Name. Id is the unique identifier of the user in the
system, which is given by the system. Works is a list of all copyright works owned by the user.

A work refers to a digital copyright work existing in the system, which has attributes such as {Name, Id, Metadata}. Name is the name of the work. Id is the unique identifier of the work. Metadata is an extended property field that contains information such as a work's digital fingerprint, type of work, trading rights, creation time, etc.

The transaction record has attributes such as {WorksId, OriginOwnerId, CurrentOwnerId}. WorksId is the Id of the currently traded work. OriginOwnerId is the Id of the originator of the traded work; CurrentOwnerId is the Id of the person to whom the work is traded.

Based on the above three entities, the following seven function functions are abstracted in the chain code to realize the transaction function of digital works in the blockchain environment, so as to meet the needs of copyright deposit and traceability.

a) userRegister(name, Id): Used to realize the registration of new users of the system, the Id is automatically assigned by the system.

b) userDestroy (Id) : Used to log off system users, Id is the Id of the user who needs to log off.

c) workEnroll (workName, workId, Metadata, ownerId) : Used to realize the registration of copyright works.

d) workExchange (ownerId, workId, currentOwnerId) : Used to trade the copyright of the work.

e) queryUser (ownerId) : Used to query information about users and their copyrighted works.

f) queryWork (workId) : Used to query detailed information of copyrighted works.

g) queryWorkHistory (workId) : Used to query all transaction records of a copyrighted work.

Among the above functions, the core and the most complicated should be the trade the copyright of the work (work information registration can be regarded as the original owner's empty transaction registration), and the pseudo code of the copyright transaction function is as follows:

```go
workExchange(ownerId, workId, currentOwnerId)/
newOwner=currentOwnerId; // Obtain copyright assignor
oldOwner=ownerId; // Acquire copyright purchaser
deleteoldOwner.list(); //Update transferor copyright list
changeOwnerOfWork.Owner==newOwner; // Works copyright transfer
updatenewOwner.list(); //Update the buyer's copyright list
updateWorkHistory(); //Update work change records
```

D. System implementation

1) Blockchain deployment environment

The experiment was completed on the PC with an operating system of Ubuntu 16.0. The experiment selected the fabric alliance chain as the implementation platform. The chain code was written based on the Go. The front-end interface used the Golang SDK to complete the message interaction with the blockchain system. Before building the blockchain network, we need to complete the deployment of the development environment in advance. First, download the go language development kit, fabric source code, Fabric Golang SDK, and docker image to the local environment.

2) Blockchain creation configuration

The creation configuration of the blockchain network includes the steps of configuring user node certificates, generating genesis blocks, and building channel transactions. Among them, user node certificate configuration needs to configure CA certificate, encrypted communication certificate, signature certificate and other different types of certificates.

After deploying the basic environment required by the Fabric network, compile and generate the Cryptogen program, and use Crypto-config.yaml and Configtx.yaml files to complete the configuration of the node certificate. The Crypto-config.yaml file is used to configure the number of organization nodes and the number of users in each organization. The blockchain network needs to use this file to configure user certificates. The Configtx.yaml file is used to configure the organization information in the blockchain, such as the organization name and corresponding certificate location. For order nodes, it is also necessary to configure the consensus mechanism, the size of each block, and the number of transactions in this file. Afterwards, the genesis block is generated and the transaction channel is constructed by command line.

3) Blockchain network construction

After completing the genesis configuration of the blockchain network, the blockchain network needs to be built. This part includes operations such as creating channels, adding nodes, installing chain codes, and instantiating chain codes. The construction of the blockchain network needs to be completed in the cli container. After entering the cli container, we need to create a channel by using the command line and add the peer node to the channel. Then we just need to deploy the chain code we completed in advance to the node to complete the instantiation. After the interactive test of the chain code, the copyright registration results and transaction record query results are shown in the figure. So far we have completed the storage and query of the copyright key information on the blockchain.

![Create genesis block](image3.png)

Figure 3. Create genesis block

![Copyright work registration](image4.png)

Figure 4. Copyright work registration

![Transaction record query](image5.png)

Figure 5. Transaction record query
4) Blockchain system interaction

The front-end interface is based on the Gin framework and the Golang SDK to achieve interaction with the blockchain network. After running the Fabric client code to generate the business remote interface, we need to set the route for the function in the smart contract. The front-end page can realize the business function in the smart contract through the interface and routing request to the blockchain network. The front-end display page of the experiment was completed based on technologies such as Html,Css, and JavaScript. Front-end certificate deposit page is displayed as follows. Users can directly send requests to the blockchain system through the front-end interface to complete functions such as on-chain certificate storage and query of copyright information and transaction information.

![Front-end certificate deposit page](image)

Figure 6. Front-end certificate deposit page

5) Experimental summary

Combining with copyright protection business scenarios, starting with key points such as system architecture, development framework, and smart contracts, this article elaborates the design ideas of each link in detail. And based on the blockchain have achieved a set of lightweight and efficient copyright protection system. This experiment fully proved the practical use of blockchain technology in the field of copyright protection. The innovations of this system are as follows:

a) Based on blockchain technology, the system realizes the secure and distributed storage of copyright key information, as well as the forensics and traceability of copyright information on the blockchain.

b) Use the identity control mechanism and channel division technology under Fabric to strictly control the security of the nodes in the system, so that only nodes in the same channel have the complete account of the channel, which improves the security and privacy protection of the system.

CONCLUSION

The copyright protection technology has tended to be systematic and mature roughly ten years ago. The emergence of blockchain technology has opened up a new way of realizing copyright protection. This article cuts in from blockchain technology, deeply studies the principles and characteristics of blockchain technology, and makes a careful exploration of the classification and research difficulties of digital copyright protection technology. After that, this article made a detailed analysis of the landing advantages of blockchain in the field of copyright protection, and implemented a high-performance, lightweight, and low-cost alliance chain copyright protection system. The system introduced in this article is still in the prototype stage, and we will continue to improve it in the future. Blockchain technology is still in the stage of being explored. It is believed that with the deepening of research, blockchain technology can achieve more remarkable achievements in copyright protection and other application fields.

ACKNOWLEDGMENT

This work was supported by the Fundamental Research Funds for the Central Universities.

REFERENCES


