Copyright Certificate Storage and Trading System Based on Blockchain

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

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

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

Chaonan Gu
School of Computer Science and Cybersecurity, Communication University of China, Beijing, China
15732116238@163.com

***Abstract*—In the era of digitalization and networking, the high cost and long time of traditional centralized copyright protection methods make the copyright of digital works cannot be well protected and the infringement phenomenon be serious. Blockchain, as a decentralized distributed database, can store the copyright information of works. This paper researches and analyzes the advantages of blockchain in copyright protection and the current research status, and finally a copyright certificate storage and trading system based on blockchain is designed. In this system, registration confirmation, transaction certificate, and dispute protection are researched as a complete process. And the certificate storage data on the blockchain are precisely designed, which greatly reduces the time and cost of rights protection. What's more, the copyright of digital works is divided by studying laws related to copyright in China, which makes this system more suitable for practical applications.**

Keywords—blockchain, fabric, copyright transaction, copyright certificate storage

I. INTRODUCTION

A lot of digital works are spread by some digital publishers who are not authorized, which brings more serious economic losses to copyright owners than traditional piracy [1]. According to relevant statistics, since the Beijing People's Court tried online copyright dispute cases in 1999, the number of cases handled by it has increased from an initial number of cases per year to thousands of cases per year [2]. Copyright protection in Chain has always been closely linked with copyright registration agencies. Although online registration services are provided, complicated copyright review processes and registration costs cannot be exempted. This centralized copyright protection method has been difficult to meet the needs of copyright protection in the digital era. With the emergence of blockchain technology, the copyright protection of digital works has a new method. At present, there are still few research results and advanced applications in the field of copyright protection in the world, and successful projects put into practice are more or less defective. The use of blockchain technology for digital copyright protection remains to be studied and explored [3]. Based on the consideration of media content security, Esteban Ordano proposed the core technology of blockchain "Proof of Existence" [4]. Some industry organizations such as the American data Marketing Association and other blockchain service providers, Consen-Sys and MetaX jointly launched the advertising chain registration system ACR based on blockchain technology [5]. In foreign countries, the starting point of these researches is commercial interests, rarely starting from the copyright protection, and these research contents are relatively single and one-sided. In the aspect of copyright registration, they are not divorced from the inherent process. Some digital copyright protection and trading systems based on blockchain have also been proposed in China, but they all have some shortcomings. For example, the data of copyright certificate storage of digital works on the blockchain are simple, and few transaction records are stored. In addition, the copyright was treated as a whole, and the copyright transaction does not indicate the specific rights of the transaction in these systems. According to China's copyright law, some copyrights belong to the copyright owner and cannot be traded or inherited. In the application of copyright protection, these problems are all needed to be studied and solved. Based on the research on these issues, this paper proposes a new copyright certificate storage and trading system based on blockchain(hereinafter referred to as system).

II. BLOCKCHAIN AND DEVELOPMENT PLATFORM ORIENTED DIGITAL COPYRIGHT PROTECTION

A. Blockchain analysis

Blockchain technology links each block by hash value, and traces the content of previous blocks from the last block. All information on the block is managed by all participating nodes or several authoritative nodes. The node can only modify the data on the blockchain when it has more than 51% of the global computing power. This is very difficult in the current actual situation. For digital works, important information related to the works can be saved on the blockchain. The current main practice is to store the unique identifiers of the digital works such as hash values on the block, and the work files themselves are stored elsewhere [6]. When copyright disputes occur, the certificate information can be read directly from the blockchain, or each step of the circulation of the copyright can be traced, which makes it possible to solve the problem by using limited time and low cost.

Blockchain are usually divided into three types, which are "public blockchain", "private blockchain", and "consortium blockchain". In the public blockchain system, the use of virtual currency transactions is its main feature.

The private blockchain system is only open to individuals, internal users are completely isolated from the outside, and there are few services that can be provide. Due to the prohibition of virtual currency transactions and the high degree of government participation in social activities in China, the current research mainly focuses on consortium blockchain for the copyright protection that don't needs virtual currency [7].

B. Blockchain development platform analysis

At present, the underlying development platform of consortium blockchain mainly includes fabric provided by hyperledger and BCOS [8]. BCOS has friendly development interface and complete technical components [2]. However, fabric has better security and more powerful functions. Without querying blocks, it can obtain the latest transaction information. Meanwhile, it provides strict restrictions on the access of organizations, only the organization with qualified certificates can join the consortium. Therefore, this system chooses fabric as the development platform of the bottom network of blockchain.

In this system, the creator of the work can initiate digital copyright registration and transaction proposal through the interface provided by the fabric SDK. After a series of operations, such as endorsement, sorting and accounting, some key information is saved on the blockchain, and the latest status of the transaction in the status database will be updated at the same time. The smart contract [9] module is responsible for providing API to application modules, including contract deployment, invocation, execution and cancellation, the administrator can interact with the smart contract by the interface provided by the SDK to obtain key information that provide evidence for copyright disputes from the block, and the latest status of transactions can be read from the status database.

III. SYSTEM ANALYSIS AND DESIGN

A. System architecture

By abstracting business requirements and functional requirements, the system determines three major modules to realize system functions, which are: user management module that manages the operations related to users, work management module that manages the operations related to works and transaction record management module that manages the operations related to transaction records. The detailed division of each module is shown in TABLE I:

TABLE I. DETAILED DIVISION OF SYSTEM FUNCTION

Module	Detailed Division of Each Module
user module	user login, user registration, user personal information modification, user logout
work module	work copyright registration, work information browsing, work copyright transaction
transaction module	transaction record registration, transaction record viewing

From the perspective of hierarchy, the system is divided into four parts: access layer that provides the interface of access the system business, business layer that processes the system business, blockchain and middleware. The services selected by users through the access layer interface are submitted to the business layer for processing, and finally the processing results are stored in the blockchain and middleware. The blockchain stores key information, and the middleware stores detailed information. The system hierarchy is shown in Fig. 1:

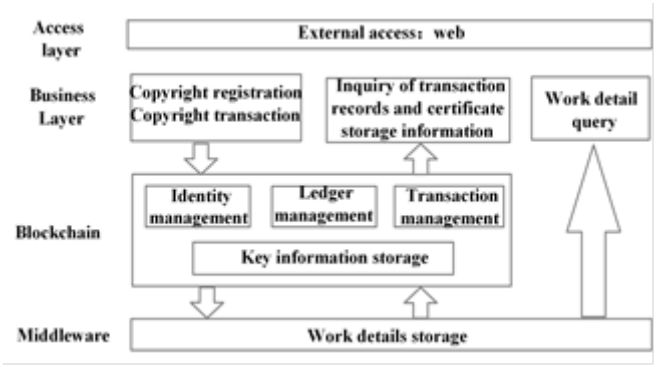

Fig. 1. System hierarchy

B. System running process

The running process of the system is shown in Fig.2. In this system, the key information of some key operations is saved on the blockchain from the time of user registration and login. These information can be used for both copyright certificate and traceability. In case of copyright disputes, the certificate information can be read, or each step of copyright circulation can be checked.

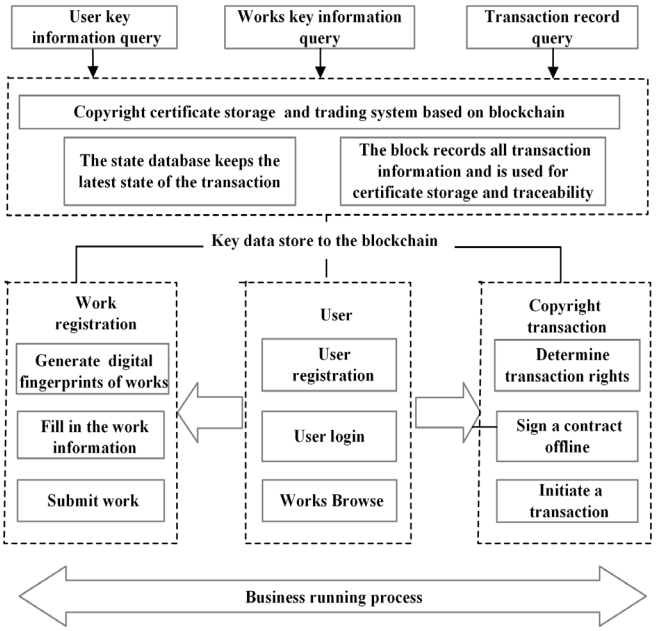

Fig. 2. System running process

C. Rights division of digital works

The existing copyright protection system takes copyright as a whole, without further subdivision, and without the rights to specific transactions in copyright transactions. According to the copyright law, copyright includes personal rights and property rights. The personal rights, only belong to the author, can't be traded, and property rights can be traded and inherited. But when the work becomes work for hire, only the right of authorship belongs to the author, and the remaining rights are enjoyed by the author unit. In this system, in order to make copyright transactions comply with legal requirements, copyright rights are divided into two

types- tradable and nontradable. The specific division is shown in TABLE II:

TABLE II. DIVISION OF COPYRIGHT RIGHTS OF DIGITAL WORKS

Transaction Type	Work Type	Including Rights
nontradable	work of hire	the right of authorship
	other works	personal rights
tradable	work of hire	property rights, publication right, revision right, works integrity right
	other works	property rights

In this system, all the rights of the works are stored on the block according to the classification. When carrying out copyright transactions, only the tradable rights can be traded and the transaction records are saved on the block.

D. Blockchain certificate storage data

Some key data can be saved on the blockchain, which can be used as the certificate storage and traceability of copyright. Considering the reliability of the certification data and the convenience of traceability, business entities of this system are abstracted into users, digital works, and transaction records, and the key information of them is saved on the blockchain. The specific information is shown in TABLE III:

TABLE III. BLOCKCHAIN CERTIFICATE STORAGE DATA

Entity	Certificate Data
user	unique identifier of user, username, user works list
work	unique identifier of work, work name, unique identifier of work owner, supplementary attributes
transaction record	unique identifier of work , work right of transaction, the owner of the work right before the transaction , the owner of the right work after the transaction

The unique identifier of the user is a series of digital identifiers automatically generated by the system when the user registers. The unique identifier of the work is a unique digital fingerprint generated by the system when the work is registered. The supplementary attributes include the registration time of the work, the right information of the work, etc. Through the storage content of digital work entity and user entity, copyright can be confirmed, and the storage content of transaction record entity can be used to check every step of copyright circulation.

E. System smart contract

The smart contract plays an important role in the whole blockchain project. It can receive data or return data according to the request. The operations such as data linking and data reading from the blockchain are completed by the smart contract. This system mainly designs seven functions for the smart contract, which are user information registration, user information deletion, user information query, work information registration, work information query, transaction record registration and transaction record query. The specific design is shown in TABLE IV:

TABLE IV. SMART CONTRACT FUNCTION DESIGN

Function	Input Parameter
user information registration	unique identifier of user, username
user information query	unique identifier of user
user information delete	unique identifier of user
work information registration	unique identifier of work, work name, unique identifier of work owner, supplementary attributes
work information query	unique identifier of work
transaction record registration	unique identifier of work , work right of transaction, the owner of the work right before the transaction , the owner of the right work after the transaction
transaction record query	unique identifier of work

The information registration function mainly saves the key information on the blockchain. The query function mainly reads the key information and checks every step of copyright circulation. When the user logs off in the system, the user information deletion function is called to delete the user information in the state database, but not the information on the block.

IV. SYSTEM IMPLEMENTATION

A. Development environment deployment

The development environment of this system is personal PC, and the operating system is Ubuntu 16.0.4. The fabric project provided by hyperledger is used as the development platform of bottom network of blockchain. What's more, the go language is used to develop the chaincode (smart contract). The user can use the go SDK provided by fabric to interact with the blockchain network. Some development tools, such as the go language development package, fabric source code, fabric go SDK, docker, docker-compose and the image needed by this system, need be downloaded to the local area in the environmental preparation stage. At the same time, the cryptogen and configtxgen files are placed in the bin directory of the project folder. Finally, cryptoconfig.yaml and configtx.yaml files are configured according to the needs of the system.

B. Blockchain network construction and chaincode installation

After the successful deployment of the system development environment, the underlying network of the blockchain will be started to build. First, the cryptogen and cryptoconfig.yaml files are used to generate certificates for each organization and corresponding nodes. The configtxgen file is used to generate the original transaction of the origination block and channel and anchor node for each organization. After starting the network, the channel can be created in the container, and the peer node is added to the channel. Finally, the primary node is set for each organization. Through a series of operations, the underlying network of the blockchain is built. Next, the business chaincode wrote by developer need to be installed into this network and instantiated. After the chaincode is instantiated successfully, it can be found in the var/hyperledger/ production/chaincode folder of the node container.

C. System interaction

To interact with the blockchain network, the head webpage and fabric client need be developed. The user initiates the request through the head webpage. The client receives the processing request, and interacts with the blockchain according to the result of the request. The client uses the gin framework provided by golang and the interface provided by fabric golang SDK to develop. The remote interface of the business system is generated by running the fabric client code, as shown in Fig.3:

```
[GIN-debug] POST   /users                    --> main.userRegister (3 handlers)
[GIN-debug] GET    /users/:id                --> main.queryUser (3 handlers)
[GIN-debug] DELETE /users/:id                --> main.deleteUser (3 handlers)
[GIN-debug] GET    /assets/get/:id           --> main.queryAsset (3 handlers)
[GIN-debug] POST   /assets/enroll            --> main.assetsEnroll (3 handlers)
[GIN-debug] POST   /assets/exchange          --> main.assetsExchange (3 handlers
)
[GIN-debug] GET    /assets/exchange/history  --> main.assetsExchangeHistory (3 h
andlers)
[GIN-debug] Environment variable PORT is undefined. Using port :8080 by default
[GIN-debug] Listening and serving HTTP on :8080
```

Fig. 3. Business system remote interface

The client sets a route for each function request of the head webpage, and the front-end page can perform relevant functions with the route through the remote interface provided by the back-end. In Fig.3, from the top to the bottom, seven function request routes are set, which are user information registration, user information query, user information deletion, work information query, work information registration, transaction record registration, and transaction record query. These routes will be bound with the head webpage respectively. In this system, the head webpage is developed by html, css and js. As shown in Fig.4, the successful login user needs to register the copyright of the work and can send a request through the head webpage. After receiving the registration request, the fabric client will process it, and save the key information of the work to the blockchain according to the processing results.

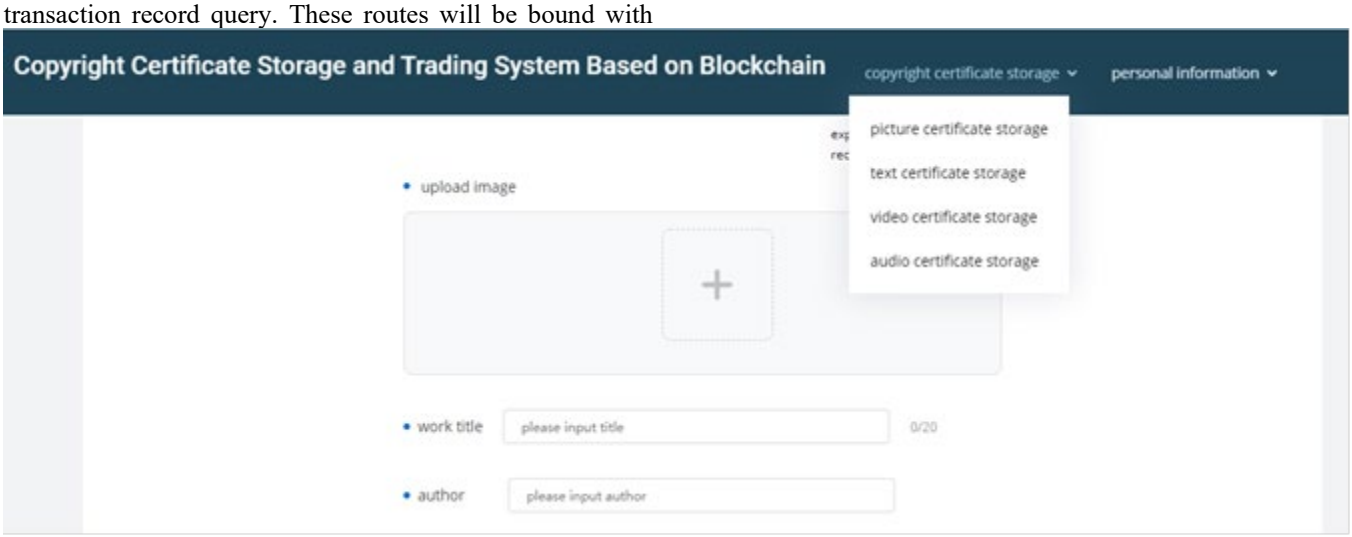

Fig. 4. Work information registration

V. System Security Analysis

Combining blockchain and copyright protection can provide a reliable security guarantee for the copyright protection system. This system is a consortium blockchain system based on fabric. Using this system can guarantee system security in the following aspects.

A. Privacy security

This system realizes the protection of privacy by dividing the channels. All nodes of the system can save the same account book, or some nodes can save the same account book. The nodes saving different account books belong to different channels, and the same node can belong to multiple channels. The nodes belonging to the same channel can only be saved the ledger data of this channel and other channels are completely transparent to these nodes. The privacy is protected by the division of channels

B. Certificate storage data security

In this system, the identity of the organizations joining the consortium is strictly controlled, so that the organizations joining the consortium are trusted with each other. There is hardly evil organization, which ensures the authenticity and reliability of the data on the blockchain. In addition, the consensus algorithm used in fabric can allow a certain number of evil nodes to exist. As long as $n \geq 3F + 1$, it can still ensure the authenticity and reliability of data on the blockchain, where n is the total number of nodes in the consortium, and F is the total number of malicious nodes in the consortium. Through their combination, the security of the data on the blockchain can be guaranteed to a large extent.

VI. Conclusion

Blockchain technology can provide a decentralized registration for copyright protection of digital works. The

data on the blockchain cannot be arbitrarily modified, which makes it believable to be used as certificate information of copyright confirmation. This paper presents the design and implementation of the copyright certificate storage and trading system based on blockchain. In this system, the complete services, such as registration confirmation, transaction certificate storage, and dispute protection, are provided. Based on the China's copyright law, the copyright of digital works is divided into two categories- nontradable and tradable. Digital fingerprint technology is used to make the digital works unique. The user information, work information and transaction records are saved on the blockchain, which makes certificate storage data is comprehensive. In a word, this paper provides a digital copyright certificate storage and trading alliance chain system based on fabric. This system has the characteristics of tamper- proof, copyright traceability, short registration time and low cost, which provides an effective method for the copyright protection of digital works.

ACKNOWLEDGMENT

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

REFERENCES

[1] Jian Wu, Li Gao, Jingning Zhu. Digital copyright protection based on blockchain technology [J]. Radio and television information, 2016 (07).

[2] Chao Li, Bingrong Dai, Hongji Wang, Xiaoqiang Wang. Digital copyright protection and trading system based on blockchain [J]. modern computer (Professional Edition), 2018 (29): 80-84.

[3] Pu He, Ge Yu, Yanfeng Zhang. Prospective overview of blockchain technology and applications [J]. Computer Science, 2017, 44 (4): 1-7..

[4] R. Dennis,G. Owenson, B. Aziz. A Temporal Blockchain: A Formal Analysis[C]. International Conference on Collaboration Technologies and Systems. IEEE, 2017:430-437.

[5] A. Hari. The internet blockchain: A distributed, tamper-resistant transaction framework for the internet[C]. Proceedings of the 15th ACM Workshop on Hot Topics in Networks. Atlanta, GA, USA: ACM Press, 2016: 204-210.

[6] Z. Meng, T. Morizumi, S. Miyata and H. Kinoshita. Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Tokyo, 2018, 359--364.

[7] Hyperledger. Hyperledger Whitepaper [EB/OL].

[8] Three mainstream platform models of blockchain [J]. Information Construction, 2018 (07): 4-6.

[9] K. Christidis and M. Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. in IEEE Access, vol. 4, 2292--2303, 2016.