Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.029693
Article

Tech Science Press

Blockchain-Enabled Digital Rights Management for Museum-Digital Property Rights

Liutao Zhao[1,2], Jiawan Zhang[1,3,*] and Hairong Jing[4]

[1]College of Intelligence and Computing, Tianjin University, Tianjin, 300350, China
[2]Beijing Computing Center Co., Ltd., Beijing, 100094, China
[3]Tianjin Cultural Heritage Conservation and Inheritance Engineering Technology Center and Key Research Center for Surface Monitoring and Analysis of Relics, State Administration of Cultural Heritage, China, Tianjin, 300350, China
[4]Beijing Planetarium, Beijing, 100044, China
*Corresponding Author: Jiawan Zhang. Email: jwzhang@tju.edu.cn
Received: 09 March 2022; Accepted: 20 April 2022

Abstract: With the rapid development of digitization technology, digital copyright of museum has become more and more valuable. Its collections can be opened to and shared with the people through the Internet. However, centralized authorization, untransparent transaction information and risk of tampering data in traditional digital rights management have a strong impact on system normal operation. In this paper, we proposed a blockchain-based digital rights management scheme (BMDRM) that realizes a distributed digital rights management and authorization system by introducing non-fungible tokens (NFTs) and smart contracts. To ensure the security and efficiency of transactions and authorization, we store all processing data in a high-security distributed ledger based on cryptographic signatures. We test our scheme on Ethereum private network and the experimental results show that BMDRM is feasible and secure for digital rights management in museums.

Keywords: Museum; blockchain; non-fungible tokens (NFTS); smart contract; digital rights management (DRM)

Abbreviations:
Abbreviations are used in this paper and listed as follows:

q	A $k-bit$ prime number
$GF(q)$	Finite group q
E	The elliptic curve defined on finite group q
G	A generating point based on the elliptic curve E
k_x	A random value on the elliptic curve
(r_{C-A}, s_{C-A})	Elliptic curve signature value of x
(x_{A-C}, y_{A-C})	An ECCDSA signature message of x
ID_x	An identity of x
BCA_x	A blockchain address of x

Enc_x	Encrypted message using key of x
$Cert_x$	A digital certificate of x
$Utoken_x$	An authentication of x
$h()$	Hash function

1 Introduction

Museum has a wealth of cultural heritage for display, research, education and dissemination of human history. These cultural relics can be transformed into text, image and video through digital scanners and cameras which are considered as copyrighted digital files finally. With the rapid development of museum digitization and application of related digital technologies, museum digital data is constantly becoming more valuable and convenient for people to feel the charm of cultural relics in digital museums. Although the digitization of cultural relic assets has brought new vitality to museums, it is also facing great challenges in sharing and disseminating digital copyright through Internet securely [1].

Reasonable digital rights management (DRM) technology has been a hot issue in academic and industrial research. Chen [2] studied the application of digital rights management (DRM) in mobile network field and built a digital rights management system for mobile network service. Zhao et al. [3] applied digital watermarking technology in digital rights management system to ensure the security of digital rights. Since blockchain technology was proposed in 2008 [4], it has been widely used in food traceability [5], medical data [6,7] and smart city [8,9] because of the advantages of decentralization, transparency, non-tampering and traceability. In the field of digital rights management, Wang et al. [10] combined digital watermarking and smart contract technology to achieve digital asset management and ensure the security of digital assets. Ma et al. [11] proposed a digital rights management platform based on privacy protection technology and blockchain to achieve access control with multi-signature technology. Ma et al. [12] designed a layered computing and storage model to make blockchain-based digital rights management platform more efficient in the 5G network. Lu et al. [13] described the application of blockchain technology in digital design management platform detailly. Wang et al. [14] used proxy re-encryption technology and blockchain technology to realize the application in the museum. However, none of them paid attention to the application of reliable transaction data of the blockchain platform. With the rise of encrypted digital artworks, NFT has gradually become popular increasingly receiving attention in research. NFTs are widely used in digital artworks such as digital collectibles, encrypted artworks and games. Because of the uniqueness of NFT, it was also used in some complex systems such as secure authentication and authorization for IoT devices [15], security and trust between hardware and software [16] and community-based infrastructure transaction systems [17]. Although NFTs have a wide range of applications, few people have studied the application of NFTs in digital rights management in museum.

In order to solve the reliable and efficient operation of digital rights management, in this paper, we proposed a blockchain-based digital rights management scheme (BMDRM), we introduced non-fungible tokens (NFT) to realize distributed digital rights issuance. Authentication, ownership and authorization information can be stored in smart contracts through NFT and smart contracts can make transaction and issue authorized digital rights automatically. There are two main types of tokens used in smart contracts: Fungible tokens (FTs) and Non-Fungible Tokens (NFTs). Their differences depend on the asset they represent. FTs can be used as the base currency for copyright transactions and licensing. In the digital copyright mechanism, museums can express their ownership of cultural relic copyrights by creating NFTs and applicants can purchase authorized NFTs through FT to obtain authorization certificates.

The main contributions of this paper are the following:

(1) We proposed a scheme (**BMDRM**) for interaction between cash flow and digital assets in museum digital rights management based on digital signature and encryption technology. It can be easily extended.

(2) **BMDRM** constructs a complete trading scheme and a token generator scheme based on the smart contract algorithm and implements a trading platform with three basic participants: content center, museums, and applicants. The digital assets and authorization are encapsulated in a blockchain token structure with token level consensus policies

(3) We compared our scheme with others in public authentication, traceable, decentralization and gas cost, the results show that BMDRM can effectively improve security and flexibility of digital rights management in museums.

The rest of this article is organized as follows. Section 2 provides background of the research. Section 3 deals with the proposed museum-digital rights management mechanism. Section 4 presents an analysis of the proposed scheme. In Section 5, the discussions and comparisons are given. Finally, we conclude this study.

2 Background

2.1 Ethereum Blockchain and Smart Contracts

Blockchain is defined as a distributed shared digital ledger for transactions. It applied public key cryptography to ensure the identity and pseudo-anonymity of all participants and decentralized consensus algorithms to maintain the ledger and verify any transaction. Ethereum [18] is one of the most widely adopted blockchain platforms because of the ability of storing state data and executing smart contracts. The program is known as smart contracts proposed by Szabo [19] and can be executed automatically. Generally, smart contracts are predefined and deployed on blockchain and each node of the network will execute the smart contract when received transaction data and enough gas fee.

2.2 Tokenization for Ethereum

In the blockchain domain, a token can be used to represent some crypto-currencies, such as Bitcoin or Ether [20]. The cryptocurrencies and tokens used in blockchain applications represent a viable solution for establishing accounting and billing transactions. There are two main types of tokens, FTs and NFTs. In Ethereum, the most prevailing token standard comes from ERC20 [21]. It is identical to one another and can be divided into smaller units which does not affect their values. In contrast, ERC721 token standard [22] are non-fungible token which cannot be divided in nature. It can represent anything from virtual artifacts to physical artifacts. And another standard ERC1155 [23] extends both fungible and non-fungible tokens. It offers an interface to denote an NFT in a fungible way. The combination of these token standards is the foundation to enable the transaction platform: FTs provide a simple and fast transactional currency, while NFTs offer the verifiable immutability and authenticity of digital right ownership and authorization.

2.3 IPFS

IPFS (Inter Planetary File System) [24] is a distributed storage system. Compared with blockchain high costing of storing fees, IPFS is suitable for storing large files such as video and picture. After uploading a file on IPFS, an encrypted hash value is calculated based on the content of the file. When IPFS is required to provide a file, it uses a distributed hash table to find the node where the file is located and then retrieves the file.

3 Method

3.1 System Structure

In this study, we use ECDSA [25], blockchain, smart contracts, FTs and NFTs to design a traceable transaction platform for the digital content resources of a museum. There are four parties involved in this study: Museum (M), Content Center (CC), Applicant (L) and Bank (B). The system architecture is shown in Fig. 1.

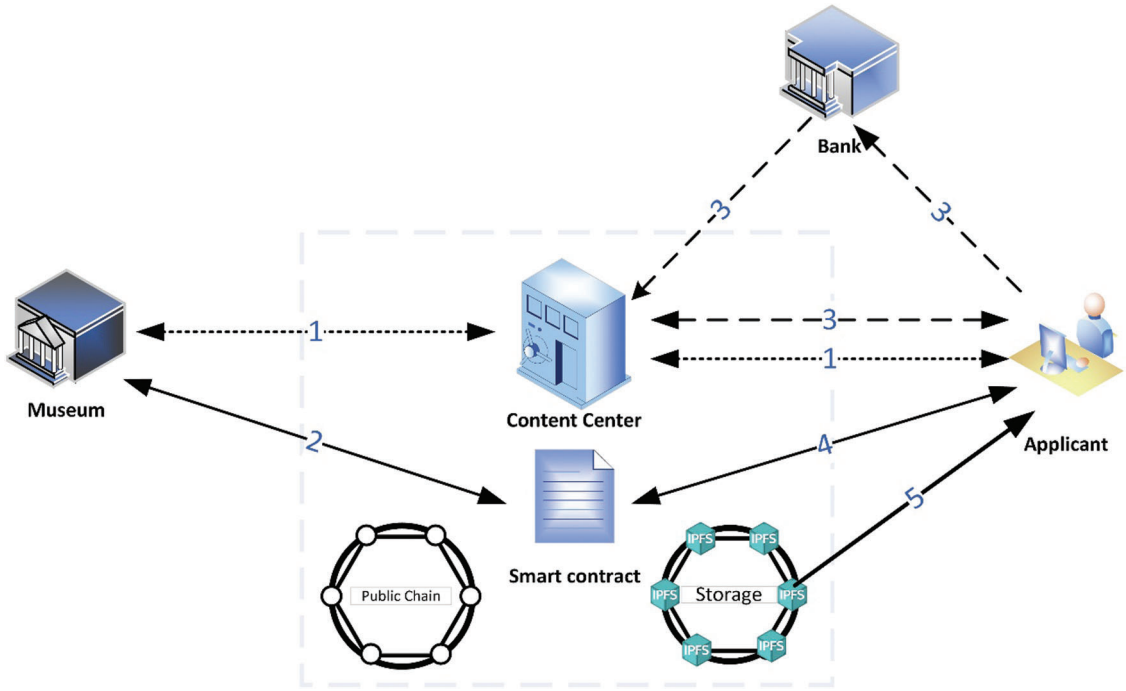

Figure 1: System architecture diagram

(1) Applicant(A) —— Citizens or institutions who want to access the digital content resource of the museum and buy authorization NFT and Mt token by smart contract.

(2) Museum (M) —— The museum is the owner of the digital content. They send classified digital content resource to content center and content center sends back a copyright NFT which represents the ownership of the digital content.

(3) Content Center (CC) —— Content Center is the manager of smart contract that can create NFTs and FTs. Content Center accepts the parties' registration and sends public/private key pair to each party.

(4) Bank (B) —— The applicant pays for MT tokens to content center via bank.

We briefly illustrate the scenarios in the following steps:

Setp 1: System initialization

Applicant, museum, and content center need to register in the blockchain and get their public/private key and blockchain account (BCA). Applicant and museum also get identity certificate and public/private key pair from the content center which deployed smart contracts for creating token and decentralized trade.

Setp 2: Copyright NFT production phase

The museum will upload the sorted digital resources to the digital content center and the digital content center will encrypt the content into protected digital resources. Then content center will store them in IPFS and send the unique identifier of the NFT to the data owner.

Setp 3: Fungible Token purchase phase

The applicant can buy tokens from the digital content center. When content center verified the money from the applicant via bank, content center will send MT tokens to the applicant's address.

Setp 4: Authorization Token purchase phase

The applicant can purchase authorizations from the digital content center and use tokens to pay authorization fees through smart contracts. The smart contract will automatically send the Authorization NFT to the applicant's address if the account has enough tokens.

Setp 5: Digital content browsing phase

The applicant submits its authorized NFT to the content service provider and accesses the protected digital content in an authorization policy

3.2 Smart Contract Initialization

The NFT-based smart contract was developed by Solidity. In the proposed architecture, we use smart contract functions to implement a transaction platform. The main functions are described as below:

constructor (*initialSupply*): The constructor of a smart contract and it will set the initial number of MT tokens.

MTtransfer (*address, amount*): The caller will send the *amount* of MT tokens to the *address*. If the balance of the message caller is insufficient, the transaction will be canceled

mint_copyrightNFT (*address, info*): the function can only be called by the owner of the smart contract and the owner will send a copyright NFT with information to the *address*.

mint_authorizationNFT (*address, info*): the function can only be called in an internal mode which means no one can call the function directly. The result of the function is to send an authorization NFT to the *address*.

buyAuthNFT (*address, info*): The applicant can call the function to buy an authorization NFT and need to pay enough MT tokens so that the function can execute successfully.

QuerNFTbyID (*tokenID*): The function can be called by everybody to query information about an authorization NFT marked with *tokenID*.

3.3 System Initialization

3.3.1 Registration Phase

Museum, applicant and content center register in the blockchain to obtain the public key and private key pair. Meanwhile applicant and museum apply for identification $(PK_u, SK_u, Cert_u)$ from the digital content center. Museum, applicant and content center will get Blockchain Address (BCA) from blockchain platform shown in Fig. 2. The identification and BCA are used to make transaction on blockchain.

Setp 1: The private key address is mapped into a 64-byte public key by the elliptic curve algorithm (ecdsa-secp256k1).

Setp 2: Algorithm keccak-256 is used to hash the public key and convert the public key into 32 bytes.

Setp 3: The last 20 bytes of the hashed public key serves as the account address

Figure 2: Blockchain address (BCA)

3.3.2 Smart Contract Deployment

The digital content center deployed smart contracts on the blockchain to obtain addresses and management rights. At the same time, Content center call the constructor function to obtain the supply of the museum token. The museum token can be transferred to any account through the smart contract. Applicant and museum can apply for exchange of the museum token and use MT token to pay the fee of authorization and copyright NFT. The description of MT token is shown in the Tab. 1.

Table 1: Information of museum token

Item	Information
Token name	Museum token
Symbol	MT
Total supply	1000000000
Decimal	8
Contract address	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

3.4 MT Token Purchase Phase

An applicant can purchase MT tokens from the content center to pay the authorization fee. The applicant transfers *payment* to the content center through bank and sends the *payment* and *address* information to content center. Content center will send a certain amount ($amount = money * q$) of tokens to the applicant address. The detail will be shown as follow:

Setp 1 Applicant generates a random value k_{A-C}, calculates:

$$z_{A-C} = h\left(ID_A, M_{A-C}, Cert_A, Bank_{pay}, TxID_A, Ts_{A-C}, address_A\right), \tag{1}$$

$$(x_{A-C}, y_{A-C}) = k_{A-C}\, G, \tag{2}$$

$$r_{A-C} = x_{A-C} \bmod n, \tag{3}$$

$$s_{A-C} = k_{A-C}{}^{-1}(\, z_{A-C} + r_{A-C} d_A) \bmod n, \tag{4}$$

$$Enc_{A-C} = E_{PK_C}\left(ID_A, M_{A-C}, Cert_A, Bank_{pay}, TxID_A, Ts_{A-C}, address_A\right), \tag{5}$$

And applicant will send ID_A, Enc_{A-C}, (r_{A-C}, s_{A-C}) to the content center.

Sept 2 Content center first decrypt the encrypted data by private key and obtain the information $ID_A, M_{A-C}, Cert_A, Bank_{pay}, TxID_A, Ts_{A-C}, address_A$. Then content center will confirm the validity of the timestamp by Ts_{A-C}, verification of $Cert_A$ with PK_A and correctness of the ECDSA signature:

$$\left(ID_A, M_{A-C}, Cert_A, Bank_{pay}, TxID_A, Ts_{A-C}, address_A\right) = D_{SK_C}(Enc_{A-C}) \tag{6}$$

$$z'_{A-C} = h\left(ID_A, M_{A-C}, Cert_A, Bank_{pay}, TxID_A, Ts_{A-C}, address_A\right), \tag{7}$$

$$u_{A-C1} = {s_{A-C}}^{-1} z'_{A-C} mod\ n, \tag{8}$$

$$u_{A-C2} = {s_{A-C}}^{-1} r_{A-C}\ mod\ n, \tag{9}$$

$$\left(x'_{A-C}, y'_{A-C}\right) = u_{A-C1} G + u_{A-C2}\, Q_{SK_C}, \tag{10}$$

$$x'_{A-C} \overset{?}{=} r_{A-C}\ mod\ n \tag{11}$$

If the verification is passed, content center will upload signature into the blockchain and get transaction information ($Bank_{pay}, TxID_A$) with blockchain address of applicant ($address_A$). After payment was confirmed, content center will call smart contract function MTtransfer ($address_A$, $amount$) to send tokens to $address_A$. The transaction will be stored in blockchain which is recorded by a hash value of the transaction Tx_{C-A}.

Setp 1: Then content center generates a random value k_{C-A}, calculates:

$$z_{C-A} = h(ID_C, M_{C-A}, Cert_C, Ts_{C-A}, Tx_{C-A}), \tag{12}$$

$$(x_{C-A}, y_{C-A}) = k_{C-A}\, G, \tag{13}$$

$$r_{C-A} = x_{C-A}\ mod\ n, \tag{14}$$

$$s_{C-A} = {k_{C-A}}^{-1}(\, z_{C-A} + r_{C-A} d_C) mod\ n, \tag{15}$$

$$Enc_{C-A} = E_{PK_A}(ID_C, M_{C-A}, Cert_C, Ts_{C-A}, Tx_{C-A}) \tag{16}$$

And content center will send ID_C, Enc_{C-A}, (r_{C-A}, s_{C-A}) to applicant:

Setp 2: Applicant decrypts the encrypted data by private key and obtains the information ($ID_C, M_{C-M}, Cert_C, Ts_{C-M}, addres_M, Tx_{C-A}$). Then applicant confirms validity of the timestamp by Ts_{C-A}, verification of $Cert_C$ with PK_C and correctness of the ECDSA signature :

$$(ID_C, M_{C-A}, Cert_C, Ts_{C-A}, Tx_{C-A}) = D_{SK_A}(Enc_{C-A}) \tag{17}$$

$$z'_{C-A} = h(ID_C, M_{C-A}, Cert_C, Ts_{C-A}, Tx_{C-A}), \tag{18}$$

$$u_{C-A1} = {s_{C-A}}^{-1} z'_{C-A} mod\ n, \tag{19}$$

$$u_{C-A2} = {s_{C-A}}^{-1} r_{C-A}\ mod\ n, \tag{20}$$

$$\left(x'_{C-A}, y'_{C-A}\right) = u_{C-A1} G + u_{C-A2}\, Q_{SK_A}, \tag{21}$$

$$x'_{C-A} \overset{?}{=} r_{C-A}\ mod\ n \tag{22}$$

Applicant will upload signature into the blockchain.

3.5 Copyright NFT Production Phase

Museum institutions collect a large number of collections that can be converted into digital content, such as calligraphy and painting. Museum transforms these contents into digital content files and publishes them as NFT through content center. Since blockchain is not suitable for storing large files (video, audio, e.g.), we store digital files on IPFS. We will introduce the process of creating the NFT digital content shown in Fig. 3.

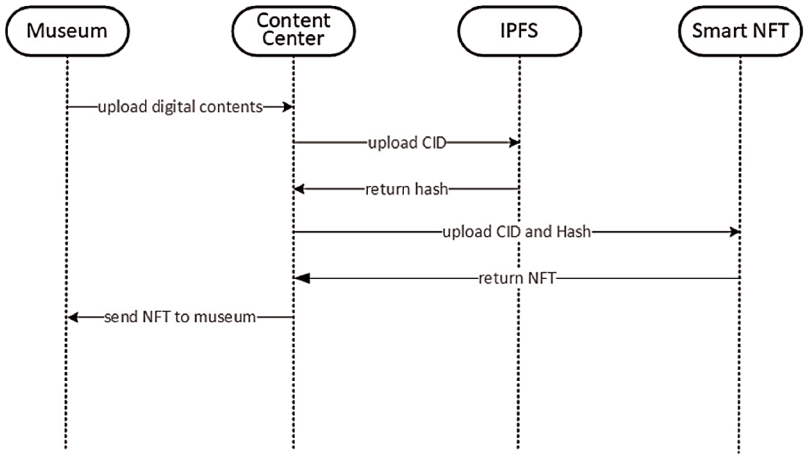

Figure 3: Copyright NFT production sequence diagram

Step 1: Museum first classifies their digital contents and uploads digital contents with information of museum address and public key to content center. Then content center will return a unique identity C_{ID} for each digital content.

Step 2: Content center encrypts the digital content and uploads the encrypted file to IPFS which will return digital content hash value h_{dc}. The content C_{ID} and h_{dc} will be stored in content center and some information about the content NFT will be sent to the museum address.

The detail of Copyright NFT production phase are shown as follow:

Setp 1: Museum generates a random value k_{M-C} , calculates:

$$z_{M-C} = h(ID_M, M_{M-C}, Cert_M, Ts_{M-C}, address_M), \tag{23}$$

$$(x_{M-C}, y_{M-C}) = k_{M-C}\, G, \tag{24}$$

$$r_{M-C} = x_{M-C}\, mod\ n, \tag{25}$$

$$s_{M-C} = k_{M-C}{}^{-1}(\, z_{M-C} + r_{M-C} d_M) mod\ n, \tag{26}$$

$$Enc_{M-C} = E_{PK_C}(ID_M, M_{M-C}, Cert_M, Ts_{M-C}, address_M), \tag{27}$$

And museum sends ID_M, Enc_{M-C}, (r_{M-C}, s_{M-C}) to content center.

Step 2: Content center first decrypts the encrypted data by private key and obtains the information $(ID_M, M_{M-C}, Cert_M, Ts_{M-C}, addres_M)$. Then it confirms validity of the timestamp by Ts_{M-C}, verification of $Cert_M$ with PK_M and correctness of the ECDSA signature :

$$(ID_M, M_{M-C}, Cert_M, Ts_{M-C}, addres_M) = D_{SK_C}(Enc_{M-C}) \tag{28}$$

$$z'_{M-C} = h(ID_M, M_{M-C}, Cert_M, Ts_{M-C}, address_M), \tag{29}$$

$$u_{M-C1} = s_{M-C}{}^{-1}\, z'_{M-C}\ mod\ n, \tag{30}$$

$$u_{M-C2} = s_{M-C}{}^{-1}\, r_{M-C}\ mod\ n, \tag{31}$$

$$\left(x'_{M-C}, y'_{M-C}\right) = u_{M-C1} G + u_{M-C2}\, Q_{SK_C}, \tag{32}$$

$$x'_{M-C} \stackrel{?}{=} r_{M-C} \bmod n \tag{33}$$

If the verification is passed, content center uploads signature into blockchain and gets digital file information uploaded by the museum ($address_M$) firstly. Then content center encrypts the digital file and uploads it to IPFS and IPFS hashes it to generate a URL with digital fingerprint that represents the location of the digital content. The content center will receive the URL and call smart contract function *mintCRNFT* ($address_M$, *info*) to send a copyright NFT to the museum ($address_M$). The transaction will be hashed (Tx_{C-M}) and uploaded into blockchain. The copyright NFT description information is shown in the Tab. 2.

Table 2: Information of copyright NFT

Item	Information
Token ID	A unique identifier of the token
CID	ID of digital content
Resource URI	A string representing the resource to be accessed
Owner	The address of owner
PK	The public key of owner
ID	The ID of owner
Timestamp	Create time of the NFT
Price	Price of a day

Then content center generates a random value k_{C-M}, calculates:

$$z_{C-M} = h(ID_C, M_{C-M}, Cert_C, Ts_{C-M}, NFT_M), \tag{34}$$

$$(x_{C-M}, y_{C-M}) = k_{C-M}\, G, \tag{35}$$

$$r_{C-M} = x_{C-M} \bmod n, \tag{36}$$

$$s_{C-M} = {k_{C-M}}^{-1}(\, z_{C-M} + r_{C-M} d_C) \bmod n, \tag{37}$$

$$Enc_{C-M} = E_{PK_M}(ID_C, M_{C-M}, Cert_C, Ts_{C-M}, NFT_M) \tag{38}$$

And content center sends ID_C, Enc_{C-M}, (r_{C-M}, s_{C-M}) to the museum.

Then museum first decrypts the encrypted data by private key and obtains the information $(ID_C, M_{C-M}, Cert_C, Ts_{C-M}, NFT_M)$. Then it confirms validity of the timestamp by Ts_{C-M}, verification of $Cert_C$ with PK_C and correctness of the ECDSA signature:

$$(ID_C, M_{C-M}, Cert_C, Ts_{C-M}, NFT_C) = D_{SK_M}(Enc_{C-M}) \tag{39}$$

$$z'_{C-M} = h(ID_C, M_{C-M}, Cert_C, Ts_{C-M}, NFT_C), \tag{40}$$

$$u_{C-M1} = {s_{C-M}}^{-1}\, z'_{C-M} \bmod n, \tag{41}$$

$$u_{C-M2} = {s_{C-M}}^{-1}\, r_{C-M} \bmod n, \tag{42}$$

$$\left(x'_{C-M}, y'_{C-M}\right) = u_{C-M1} G + u_{C-M2}\, Q_{SK_M}, \tag{43}$$

$$x'_{C-M} \overset{?}{=} r_{C-M} \bmod n \tag{44}$$

Museum will upload signature into the blockchain.

3.6 Authorization Token Purchase Phase

An applicant can obtain the token ID and price of a copyright NFT when browsing the contents in the copyright NFT market and calculate the payment for the authorization by:

$$payment = price * days \tag{45}$$

After purchasing MT tokens from content center, the applicant can call the smart contract function ***buyAuthNFT***(*tokenid , days, id, pk*) to obtain Authorization NFT. When function ***buyAuthNFT*** is called, smart contract will check the balance of the applicant blockchain address and query the price of the copyright NFT:

$$balance\_MT_A \overset{?}{\geq} price * days \tag{46}$$

If the balance of the applicant's MT token is greater than or equal to the payment, the authorization NFT will be sent to the applicant and the payment will be transferred to the owner address of the copyright NFT. Otherwise the transaction will be canceled. Algorithm 1 introduces the process of buying authorization NFT:

Algorithm 1: buyAuthNFT

```
function buyAuthNFT(token_id, days,id, pk)
    rightToken = _queryRightTokenById(token_id)
    price = rightToken.price
    right_owner=rightToken.owner
    payment = price * days
    require(balance_MT[msg.sender]> payment)
    MTtransfer (right_owner, payment)
    mint_AuthNFT(msg.sender,pk, token_id,id,days)
```

After the authorization NFT is paid, the applicant blockchain address will receive an authorization NFT sent by ***mint_AuthNFT***. The Authorization NFT provides the owner's information and validity time as show in Tab. 3.

Table 3: Information of authorization NFT

Item	Information
TokenID	A unique identifier of the token
CID	A ID of digital content
Right_token	Token id of copyright token.
Owner	The address of owner
PK	The public key of owner
ID	The ID of owner
Timestamp	Create time of the NFT
Validity period	Validity period of authorization

3.7 Digital Content Browsing Phase

After purchasing the authorization NFT through smart contract, applicant can provide it to content service provider for access digital content stored in IPFS. In our scheme, we use Authorization NFT and ID as access control of the digital content. The applicant commits $TokenID_{request}$, $CID_{request}$, $Utoken_{request}$ and $ID_{request}$. $ID_{request}$ to content service provider. $Utoken_{request}$ and UToken have been previously stored in content center. The detailed procedure of browsing is as follows:

Content center first verifies whether the identifier is valid by comparing $ID_{request}$ and $Utoken_{request}$ via querying the stored token in database:

$$ture \overset{?}{=} Utoken_{request} \wedge Query\left(ID_{request} \right) \tag{47}$$

If the applicant request is valid, content center will query authorization information by $Utoken_{request}$:

$$(CID_{Token}, Validity\ period_{Token}, ID_{Token},) = Query\left(TokenID_{request} \right) \tag{48}$$

Then content center agent checks whether the access control policy is satisfied

$$access = (CID_{token} \wedge CID_{request}) \wedge \left(ID_{token} \wedge ID_{request}\right) \wedge (Validity\_period_{token} > Ts\_now) \tag{49}$$

Content center provides the digital content to the applicant if *access* is true.

4 Analysis

4.1 Public Authentication

Our scheme mainly has two parts of authentication process: (1) the purchase of transaction tokens and the creation of copyright NFTs, (2) the automated trade on the blockchain. In off-chain situation, sender signs the message with ECDSA and receiver verifies the correctness of the message. All signature information will be uploaded to the blockchain. Each newly generated block is a verification of previous block data. When using smart contract transactions on the blockchain, participants initiate transactions through their own blockchain accounts (BCA) and each transaction is stored in the blockchain with a transaction hash. Subsequent transactions will also verify correctness of previous transactions.

4.2 Traceable

Once the digital content of museum is uploaded on the blockchain, copyright information is stored as NFT on the blockchain permanently and cannot be tampered. And all authorization and authentication transaction generated by smart contract are stored on the blockchain. We can query the issuance record of authorized NFT as a digital certificate in preventing torts on preventing loss from extending.

4.3 Decentralization

There are three advantages of the digital right management scheme proposed in this paper: (1) digital NFT is stored on the distributed storage system (IPFS). (2) all transactions are stored on the blockchain. (3) the trading platform uses smart contracts without participation of a third party. It is safer, applicable and convenience because of precluding a single point of failure in system.

5 Discussion and Comparisons

5.1 Gas Cost

Most of the smart contracts that run in the Ethereum are programed by Solidity and every line of code in Solidity requires a certain amount of gas to be executed. It depends on the priority and size of the transaction and computational cost of the function. The gas consumption of function is shown in Tab. 4. The most expensive function is *Deployment* because it needs to upload the whole smart code and execute constructor function. The *buyAuthNFT* function consume less gas than *mint_copyrightNFT* because some params can be queried in the blockchain rather than uploaded.

Table 4: Information of gas cost

Function	Gas consumption
Deployment	1947639
MTtransfer	52758
mint_copyrightNFT	296706
mint_authorizationNFT	169551
buyAuthNFT	241704

5.2 Experiments

We write smart contracts by solidity and tested the function in Ethereum private network by Remix [26]. We will briefly describe the test process:

As shown in Fig. 4, the owner of the smart contract deployed it on the blockchain with a supply of 1,000,000,000 MT tokens for operation of the decentralized trade platform. Then when content center made a charge of token fee, it called *transfer* to send tokens to the applicant. As shown in Fig. 5, the owner sent 50000 tokens to the address *0x5A86858aA3b595FD6663c2296741eF4cd8BC4d01*. The Fig. 6 illustrates a transaction to product a copyright NFT. The museum set the price of copyright 10 tokens per day and it consumed the most gas because of more inputs. The applicant bought Authorization NFT through *buyAuthNFT* by address *0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db* and applied for a 3-days authorization to browse the digital right content. We can easily calculate the amount of tokens (30) that needed to pay. Then the applicant's address remained 49970 tokens in total as shown in Figs. 7 and 8.

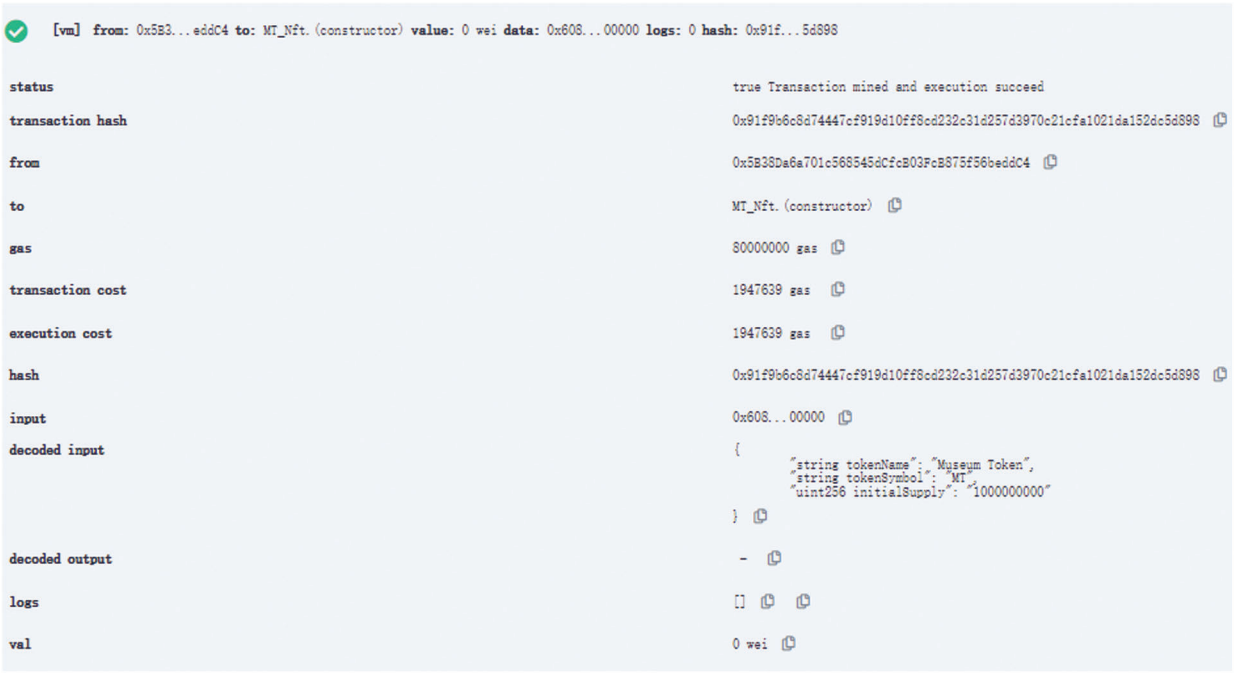

Figure 4: Deployment of MT smart contract

Figure 5: MT token transfer

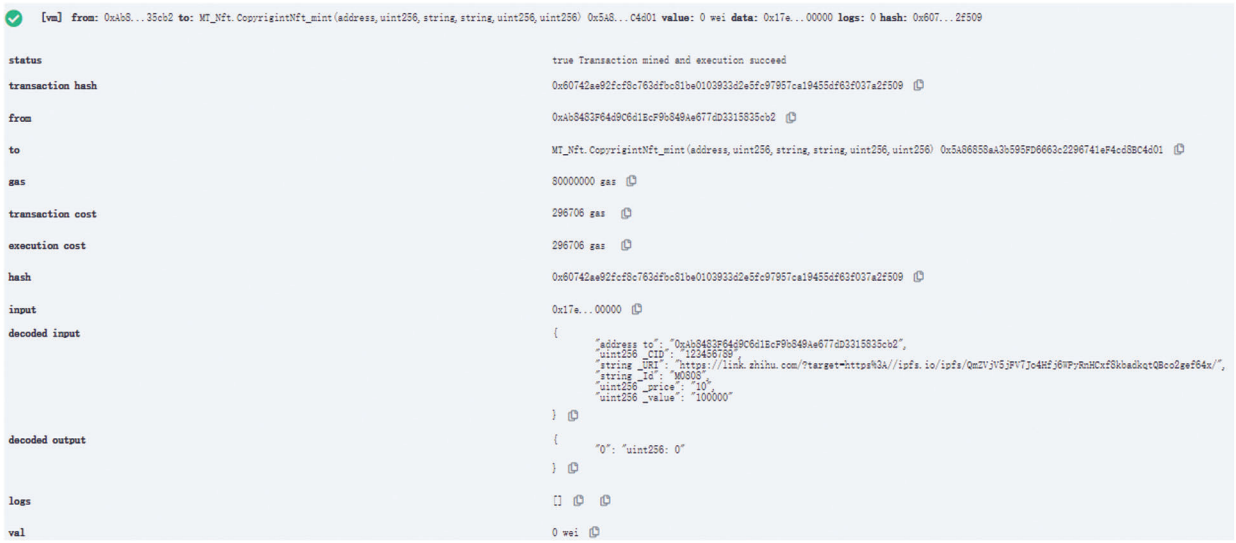

Figure 6: Copyright NFT mint

Figure 7: Authorization NFT transaction

5.3 Comparison

Tab. 5 shows the comparison of our scheme with existing smart contract technologies.

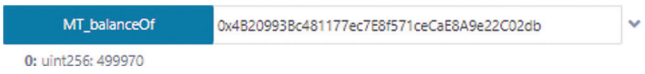

Figure 8: The balance of applicant

Table 5: Comparison of the proposed digital right management surveys

Method	Description	Blockchain based	Authentication	Traceable	Cash flow	NFT support	Automatic transaction
Zhao et al. [3]	Combined digital watermarking technology in digital rights management system	**N**	**Y**	**N**	**N**	**N**	**N**
Ma et al. [11]	Blockchain based DRM with efficient and secure authentication, privacy protection	Y	Y	N	N	N	N
Ma et al. [12]	Blockchain based DRM platform with high-level credit and security	Y	Y	Y	N	N	N
Lu et al. [13]	A scheme for digital rights management for design works.	Y	N	Y	N	N	N
Wang et al. [14]	An authorization of the museum's collections.	Y	Y	Y	Y	N	N
Ours	Blockchain based museum-digital right platform with NFT and FT	Y	Y	Y	Y	Y	Y

6 Conclusions and Future Works

The digitization and decentralized trade platform of museum provided great help for culture dissemination and economic benefits. We propose a museum digital asset management mechanism based on smart contract, FT and NFT. This mechanism is used for decentralized trading of museum digital assets. MT tokens is the circulating currency of the trade platform and copyright and authorization NFT provide certificates of digital assets. We made a detailed analysis of the data and cash flow interact with blockchain and tested the functions on the decentralized trading platform. The case study demonstrated the feasibility of the proposed framework in museum digital right management. For future work, we plan to explore more areas in which we can use NFT to track entities in the world and design more detailed control policy with securer encryption technology.

Acknowledgement: The authors gratefully acknowledge the experiment suggestions from lab mates. The authors are also grateful to the anonymous referees for their insightful comments and suggestions.

Funding Statement: This work was supported by the study and demonstration application of organization and service of cultural heritage knowledge graph, National Key Research and Development Program of China (Grant No.2019YFC1521200).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Cloud Gate Company, 2021. [Online]. Available: https://www.cloudgate.org.tw/en/cg/about/cloud-gate Accessed on 7 January 2021.

[2] C. L. Chen, "An all-in-one mobile DRM system design," *International Journal of Innovative Computing Information & Control IJICIC*, vol. 6, no. 3, pp. 897–911, 2010.

[3] B. Zhao, L. Fang, H. Zhang, C. Ge, W. Meng *et al.,* "Y-DWMS: A digital watermark management system based on smart contracts," *Sensors*, vol. 19, no. 14, pp. 3091, 2019.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electroniccashsystem," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf (accessed 6 May 2021).

[5] J. Liu, X. Sun and K. Song, "A food traceability framework based on permissioned blockchain," *Journal of Cyber Security*, vol. 2, no. 2, pp. 107–113, 2020.

[6] M. Uddin, M. S. Memon, I. Memon, I. Ali, J. Memon *et al.,* "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2377–2397, 2021.

[7] L. Zhang, M. Peng, W. Wang, S. Cui and S. Kim, "Secure and efficient data storage and sharing scheme based on double blockchain," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 499–515, 2021.

[8] Z. Dlimi, A. Ezzati and S. B. Alla, "A lightweight blockchain for IoT in smart city (IoT-smartchain)," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 2687–2703, 2021.

[9] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for internet of things (IoT) in smart cities," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2509–2524, 2021.

[10] Y. C. Wang, C. L. Chen and Y. Y. Deng, "Authorization mechanism based on blockchain technology for protecting museum-digital property rights," *Applied Sciences*, vol. 11, no. 3, pp. 1085, 2021.

[11] Z. Ma, M. Jiang, H. Gao and Z. Wang, "Blockchain for digital rights management," *Future Generation Computer Systems*, vol. 89, no. 5, pp. 746–764, 2018.

[12] Z. Ma, W. Huang, W. Bi, H. Gao and Z. Wang, "A master-slave blockchain paradigm and application in digital rights management," *Communications China*, vol. 15, no. 8, pp. 174–188, 2018.

[13] Z. Lu, Y. Shi, R. Tao and Z. Zhang, "Blockchain for digital rights management of design works," in *Proc. of the 2019 IEEE 10th Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, China, pp. 596–603, 2019.

[14] Y. C. Wang, C. L. Chen and Y. Y. Deng, "Authorization mechanism based on blockchain technology for protecting museum digital property rights," *Applied Sciences*, vol. 11, no. 3, pp. 1085, 2021.

[15] A. S. Omar and O. Basir, "Capability-based non-fungible tokens approach for a decentralized AAA framework in IoT," in *Blockchain Cybersecurity, Trust and Privacy*, vol. 79, pp. 7–31, 2020.

[16] J. Arcenegui, R. Arjona, R. Román and I. Baturone, "Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFS," *Sensors*, vol. 21, no. 9, pp. 3119, 2021.

[17] N. Karandikar, A. Chakravorty and C. Rong, "Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure," *Sensors*, vol. 21, no. 11, pp. 3822, 2021.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[19] N. Szabo, "The idea of smart contracts," 1997. [Online]. Available: http://szabo.best.vwh.net/smart contracts idea.html (accessed 6 May 2021).

[20] P. Katsiampa, "Volatility co-movement between bitcoin and ether," *Finance Research Letters*, vol. 30, no. 4, pp. 221–227, 2019.

[21] F. Vogelsteller and V. Buterin, "ERC 20 token standard," 2015. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

[22] W. Entriken, D. Shirley, J. Evans and N. Sachs, "ERC-721 non-fungible token standard," 2018. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md.

[23] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet *et al.,* "ERC-1155 multi token standard," 2018. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1155.md.

[24] J. Benet, "IPFS-content addressed, versioned, P2P file system," arXiv preprint arXiv,1407.3561, 2014.

[25] W. Han and Z. Zhu, "An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem," *International Journal of Communication Systems*, vol. 27, no. 8, pp. 1173–1185, 2012.

[26] Remix IDE Online, "Available online: https://remix.ethereum.org/ (accessed on 22 April 2021).