Journal of Cultural Heritage 59 (2023) 69–82

Contents lists available at ScienceDirect

Journal of Cultural Heritage

journal homepage: www.elsevier.com/locate/culher

Original article

A Blockchain-Based cryptographic interaction method of digital museum collections

Liutao Zhao[a,b], Jiawan Zhang[a,c,*], Hairong Jing[d], Jianping Wu[e], Yanjun Huang[f]

[a] *College of Intelligence and Computing, Tianjin University. Tianjin 300350, China*
[b] *Beijing Computing Center Co., Ltd, Beijing 100094, China*
[c] *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*
[d] *Beijing Planetarium. 138 Xizhimenwai street, Beijing 100044, China*
[e] *Beijing Academy of Science and Technology. No.27, West 3rd Ring Rd North, Beike Building, Beijing 100089, China*
[f] *Beijing Museum of Natural History. 126, Tianqiao ST, Beijing,100050,China*

ARTICLE INFO

Article history:
Received 5 April 2022
Accepted 7 November 2022
Available online 25 November 2022

Keywords:
Digital collections
Blockchain
SM2 Public key cryptographic
Ethereum
Non-Fungible tokens

ABSTRACT

We constructed a cryptographic interaction method museum art exchange protocol (MAXP) for museum digital collections on the basis of blockchain technology. Using our method, we build a digital collection exchange system on Ethereum to realize the digital collection's online exchange between two museums. Compared with the traditional centralized collection digital resource database method, MAXP can avoid the security risks caused by subjective factors and force majeure factors in the exchange process of digital collections, such as hackers and network viruses. In our exchange system we have built, the expression of content covered by digital collections is more convenient, and copyright disputes can be quickly resolved. Concurrently, given the decentralization and anonymity of the blockchain, a regulatory mechanism has been added to MAXP to avoid fraud, illegal fundraising, money laundering and smuggling. The regulatory mechanism we constructed is a dual receiver public key encryption scheme based on the Diffie-Hellman algorithm and the SM2 elliptic curve public key encryption algorithm. The sender encrypts the collection data, and both receivers can decrypt the messages using their respective private keys. One of the receivers is the museum that obtained the collection information, and the other receiver is the regulator. These two receivers can decrypt simultaneously, and the regulator can regulate the information exchange on the blockchain. The Beijing Planetarium and the Beijing Museum of Natural History have completed the exchange of collections through the system we have built. The analysis results show that the regulatory scheme based on the exchange blockchain system of the museum's digital collections proves to be feasible, with security and expansibility. Our new encrypted exchange management method of digital collections in museums can effectively promote the exchange of collections between museums, and is of great significance to the promotion of cultural heritage and the dissemination of scientific knowledge.

1. Introduction

Compared with traditional digital collection systems that rely on the Internet for data management and exchange, digitization of museum collections can maximize the cultural, scientific, and economic values [18]. In the traditional model, data exchanges are easily collapsed, especially in the case that the stored exchange data are tempered by untrusted internal users or attacked by external hackers. A 2011 survey by Advisory Services to the World Heritage Convention and United Nations Educational, Scientific and Cultural Organization has revealed that up to 60% of museum collections are endangered globally. Storage overloads, poor conditions for conservation and budget constraints contribute to risk factors. 95% of a museum's collections are kept in storage. Billions of objects are kept away from public sight [1]. In Germany, it is regarded as a landmark case. Following what seemed to be an open and shut case of the digital theft of one of the most famous ancient Egyptian artefacts in the West, a legal judgement has been

[*] Corresponding author.
E-mail addresses: zhaolt@tju.edu.cn (L. Zhao), jwzhang@tju.edu.cn (J. Zhang), hrjing@bjp.org.cn (H. Jing), wujp1979@163.com (J. Wu).

https://doi.org/10.1016/j.culher.2022.11.001
1296-2074/

made with implications for the whole of the museum sector. A scan was supposedly illicitly made of the world-renowned Nefertiti bust, a jewel in the crown of the Neues Museum in Berlin. The museum's authorities had long prevented visitors to the institution from capturing any pictures of the bust in an effort to retain control over its image rights. This meant that the taking of any kinds of photographs was banned. Given that the Nefertiti Bust is one of the museum's highlights, some attendees were surprised by the museum's decision to ban photography. Overall, the rules at the museum appeared to have been fairly universally adhered to. That all changed in 2016 when a pair of artists, wearing trench coats to conceal their activities, visited the German museum. The duo was able to sneak 3D scanning apparatus into the museum and set it up undetected in the room containing the Egyptian sculpture. Despite the less than scientific conditions for generating a 3D scan of the bust, the artists were able to produce a perfect digital reproduction of the artwork [4].

Therefore, the traditional digital collection management system has the problems of low security and low efficiency problems. The digital collections actualize their value through exchange, whereas blockchain technology can guarantee the security and traceability of data value exchange [19]. For example, the Byzantine Mural Foundation records the background information about the return of cultural relics on the blockchain through blockchain technology, and realizes the transactions between two antiquity markets [21]. Blockchain technology also significantly impacts the transportation of cultural heritage, offering the real-time and dynamic remote management for the transportation of cultural relics [24], and providing regulatory for the exchange transportation of physical collections. Traditionally, three ways exist to use blockchain technology to record copyrights. The first is to record copyrights for off-chain design schemes [20], using a decentralized data management framework to protect users' privacy. The second is to control the copyright of user data protocol records by the master-slave paradigm [16], to realize the management of digital copyrights. The third is the encryption algorithm recording copyright [23], which uses digital watermarking technology to enhance the robustness of the encryption algorithm, building a digital copyright blockchain management scheme. Although a series of digital copyright protection schemes for museums have been put forward on the basis of blockchain technology, the regulatory mechanism for the exchange of digital collections is not perfect. Three typical methods are relatively mature in the research on blockchain regulatory technology: blockchain transaction traceability mechanism [25], blockchain address gathering mechanism [22], and blockchain certificate management mechanism [9]. The above three mechanisms have respectively designed a regulatory mechanism from the process of the blockchain application layer, the data transmission of the network layer, and the protocol of the contract layer. The regulatory mechanism has not yet been designed in terms of the encryption algorithm included in the data layer of the blockchain architecture. To solve the problems of trust, security and regulatory in the exchange of museum digital collections, we carried out the MAXP (Museum art exchange protocol), an encrypted exchange protocol for museum digital collections. We use the SM2-based dual receiver public key encryption algorithm to build a regulatory mechanism at the data encryption level, and created a regulated blockchain digital collection NFT (Non-Fungible Tokens) trading system. The digital collections in museums can realize data NFT casting [7], exchange, storage, and transmission on a regulated blockchain to finalize the transaction. We have completed the following work:

(1) A blockchain-based museum digital asset encryption exchange protocol is constructed, coupled with the Diffie-Hellman and the SM2 algorithms, and a double-receiver public key encryption scheme is designed as well.

(2) An encrypted exchange system for museum digital collections is constructed on the basis of Ethereum, through which museums can cast digital collection NFT, realizing the transfer usage rights of data collection NFT under the regulatory mechanism.

2. Research aim

Our goal is to establish a new digital collection exchange protocol for the cultural exchange of digital collections and he safe and efficient exchange of data between museums, with a transaction regulatory mechanism. Our method is designed to protect the museum's digital collections and to regulate anomalies and even illegal behaviors during the exchange process. Digital collections can exchange data in a safe, stable, and efficient blockchain system. The regulator can monitor the transaction process and its data content, and be interrupted in the event of data anomalies to realize in-transaction regulatory, post-transaction proof saving, and traceability.

3. Material and methods

The blockchain-based encryption exchange protocol we have designed starts with the design of the encrypted exchange process for digital collections, establishes a blockchain-based digital collection exchange mechanism, and then analyzes the existing blockchain regulatory mechanism. The encryption algorithm improves the regulatory mode, adds a regulatory mechanism to the exchange process, and adopts IPFS distributed storage to ensure the security and reliability of the scheme.

3.1. Exchange method

The basic principles of the exchange method include: blockchain is adopted as the base technology, establishing the collection exchange specification, the on-chain data storage standard specification, and the museum digital collection management specification.

3.1.1. Blockchain-based digital collection exchange specification

To ensure the security and reliability of the collection data exchange process, we have built a blockchain-based peer-to-peer network management solution, which uses an authorized blockchain to manage the transaction process, consensus, and access. Considering the data are HD images, 3D models [3], and the like, we used the IPFS decentralized storage model. Each NFT cannot be split or merged, allowing for good mapping of digital collections. Reference is made to museum collection data standards to create the essential information for the data. In terms of security, we encrypted the content for access control and authority management to ensure that access permissions will not be extended externally, and the data will not be misused or distributed freely. Particularly, we have added a regulatory mechanism to the blockchain. Improvements to the encryption algorithm can realize access approval, on-chain data auditing, supervision and prompt interruption during the transaction, which allow for real-time supervision and post-audit traceability.

3.1.2. On-chain storage standard and specification

The ERC-721 standard is applied to the digital collection NFT, and URLs are used for access to collections, rather than direct uploading of digital works.

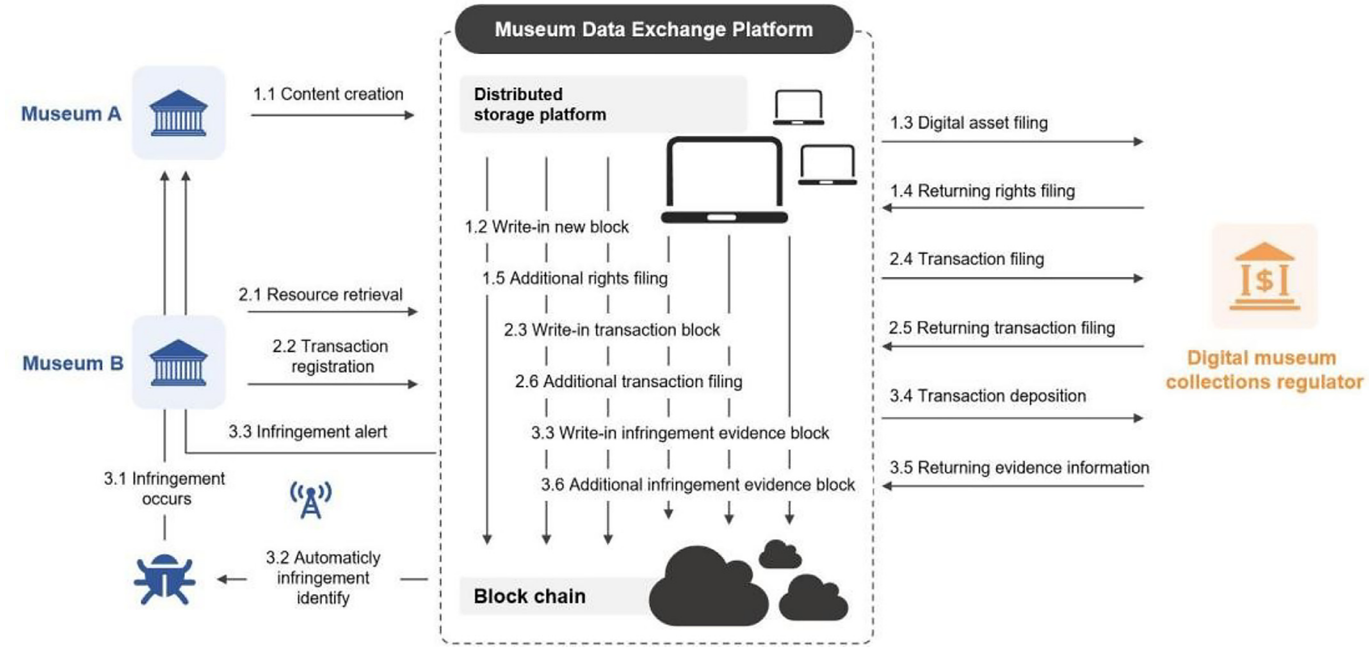

Museum Data Exchange Platform
Museum A
1.1 Content creation
Distributed storage platform
1.3 Digital asset filing
1.4 Returning rights filing
1.2 Write-in new block
1.5 Additional rights filing
2.1 Resource retrieval
2.4 Transaction filing
Museum B
2.2 Transaction registration
2.3 Write-in transaction block
2.5 Returning transaction filing
Digital museum collections regulator
2.6 Additional transaction filing
3.4 Transaction deposition
3.3 Infringement alert
3.3 Write-in infringement evidence block
3.1 Infringement occurs
3.6 Additional infringement evidence block
3.5 Returning evidence information
3.2 Automaticly infringement identify
Block chain

Fig. 1. System workflow

3.1.3. Blockchain-based collection data management layered architecture specification

(1) Vetted nodes can act as generators of data blocks, and the overall structure provides trust management, security proofs, timestamps, and logs.

(2) Content encryption and access control for conditional access to data. A distributed trust ledger was created with distributed storage by decentralization and a multi-participant design.

(3) Given that museum digital collections belong to public cultural resources, and most of the collected data is of high value, so it has relatively high requirements for data quality. This requires that its open sharing must be authorized by the museum and the assessment into the chain must be under the approval of the regulatory authorities as well. For the data exchange between Museums A and B, the distributed storage mode of multiple data centers is used via the museum data exchange platform, and the transaction processing flow of the intermediate layer is processed by the blockchain, as shown in Fig. 1.

User roles in Fig. 1 include: museums, regulatory agencies. Museums: Upload data, store tokens, and perform transactions and exchanges. Regulators: Assess and perform access, and regulate data and transactions. Platform builders may choose entities with corresponding credibility / qualifications as regulators based on law. Issue transaction tokens. The basic process of the exchange protocol is as follows:

- 1.1-1.5: Right confirmation and registration procedure of digital museum collections;
- 2.1–2.6: Use right transaction procedure of digital museum collections;
- 3.1–3.6: Infringement evidence preservation procedure of digital museum collections.

(1) Managing objects: Digital collections management is vertically divided into on-chain rights validation, access rights exchange, maintenance, tracking, and supervision. The system mainly manages the exchange processes created by the museum with clear digital copyrights.

(2) Restrictions on access: The method is primarily available to museums of all categories at all levels, and is based on the existing alliance of museums. According to the level of trust, technical ability, and participation, users are required to set individual permissions for block writing, information access, and transaction limits in the system.

(3) Technical system architecture: With each museum as a node, establish a distributed storage network and introduce other relevant alliance chains of regulatory or trading institutions to provide validation, usage, and maintenance of digital collection rights, as well as other auxiliary services.

The steps of digital collection exchange are shown in Fig. 2:

1. The collection data are uploaded to the storage system through MAXP.
2. The collection data are registered on the MAXP blockchain, and one or more NFT tokens are cast.
3. The regulator conducts operations such as regulatory, review and approval, and so on.
4. During the exchange process, the NFT tokens of the collection data are transferred.
5. The owners holding NFT tokens can access exhibition data.

Create IPFS and store digital museum asset data on distributed storage. Transactions are verified on the blockchain with our model, allowing users to store large amounts of data on the chain. The museum generates NFTs of digital assets as part of a blockchain security product through a decentralized security protocol. The data exchange sequence diagram is shown in Fig. 3.

The four subjects involved in the exchange in Fig. 3 include: platform system, blockchain system, storage system and regulatory systemss. In response to the potential risk that authorization information might have tampered in the scenario of regulator authorizing museums to cast NFT, the MAXP provides solutions to achieve the following functions:

i) The digital collection information cannot be maliciously tampered with, and the digital assets already obtained by the museum recipient cannot be transferred or maliciously destroyed by attackers, and the canceled and expired subscriptions by the recipient will be invalid.

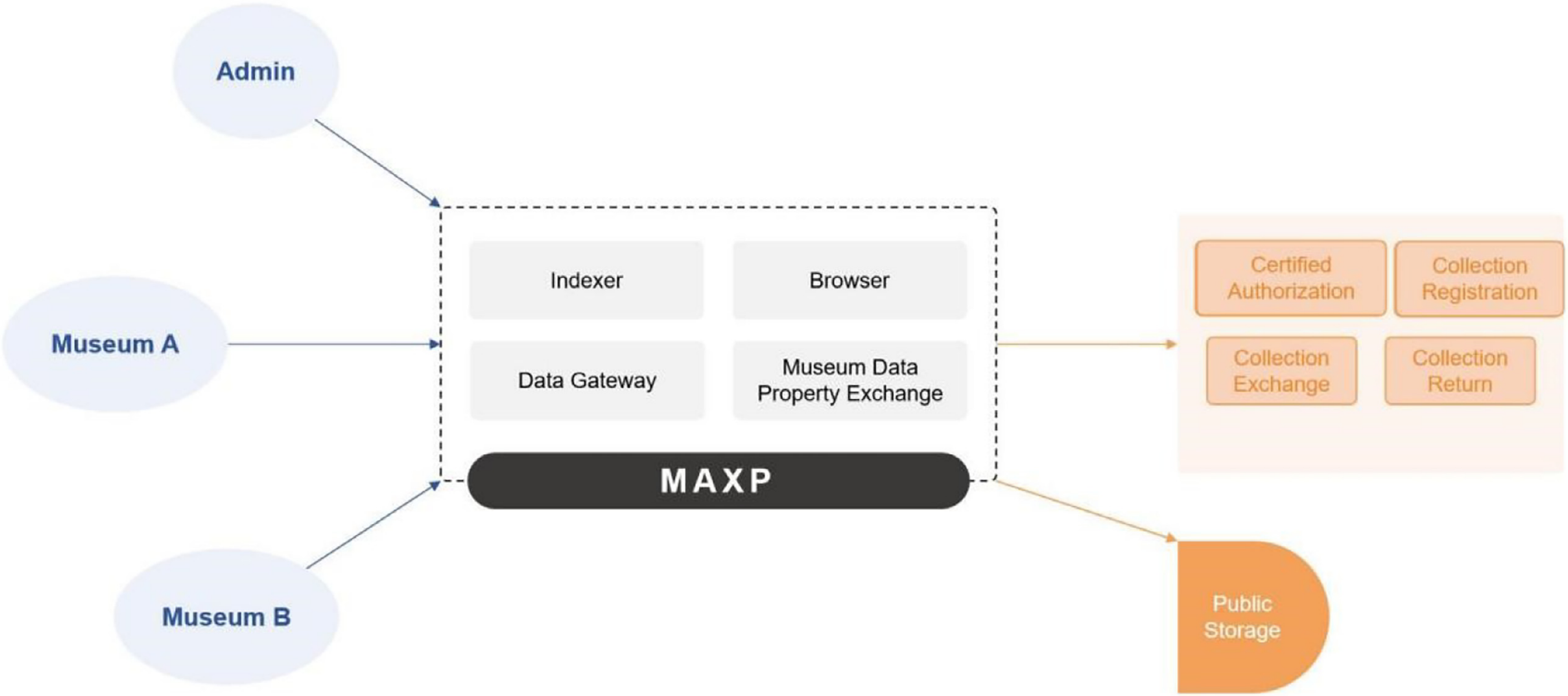


Fig. 2. Trading structure.

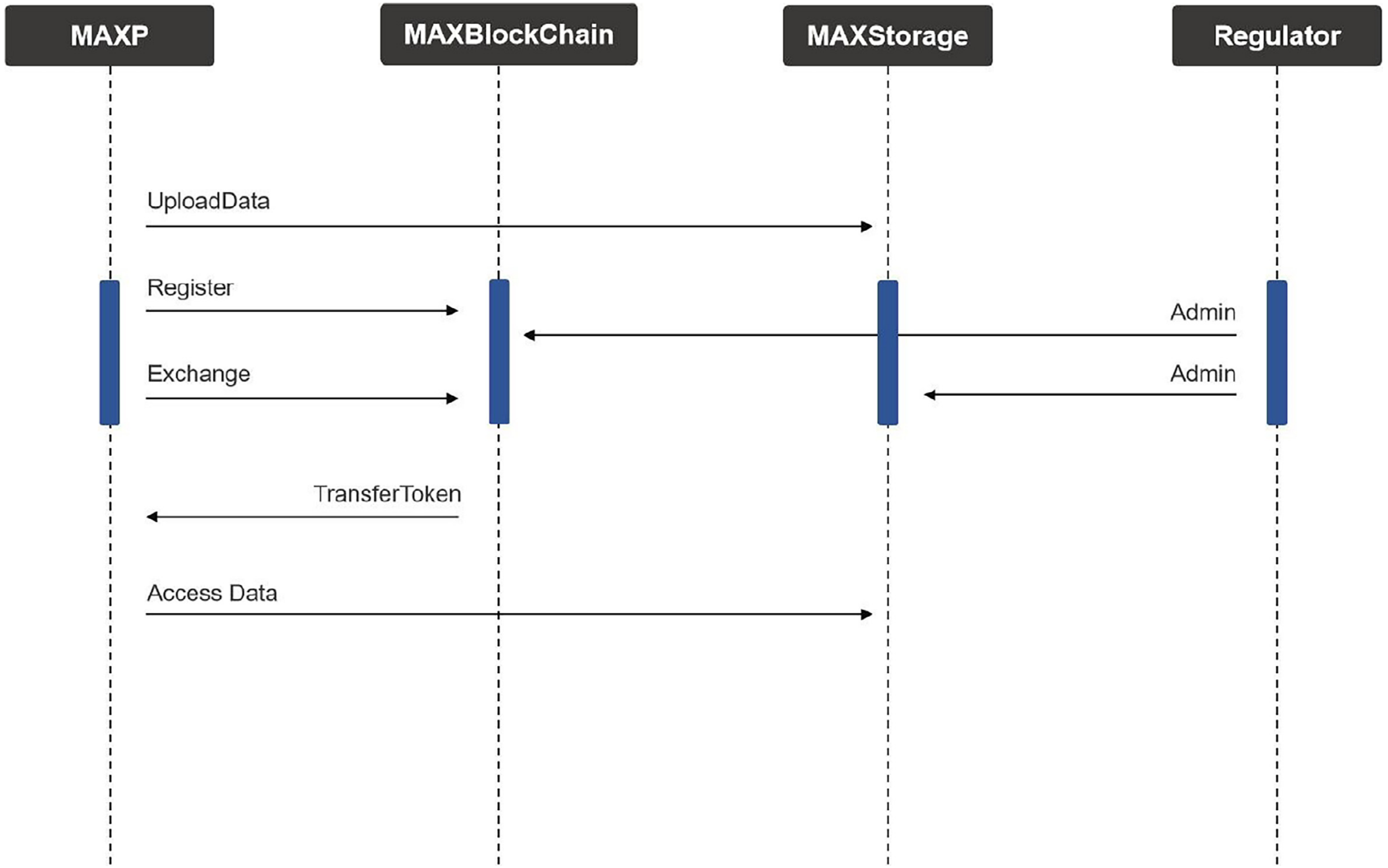


Fig. 3. Basic exchange Sequence of Exhibition Data Exchange on MAXP.

ii) The operation of the recipient and sender of the museum should be simple enough so that the recipient is free to purchase, cancel in advance and receive a refund. Museums are able to query the subscription status, activate upcoming subscriptions, and permanently invalidate the subscriptions after they expire.

iii) The digital collection subscription will take effect regularly. Before it takes effect, the museum recipient can cancel the subscription and get a refund; after it takes effect, the museum recipient will have no permission to operate the subscription. During the validity period, only the museum sender can perform operations on the subscription. After it expires, it becomes permanently invalid.

3.2. Analysis of blockchain regulatory methods

As we mentioned above, the three regulatory technologies that are relatively familiar to the blockchain currently have regulatory characteristics. However, theoretical security and efficiency problems persists in the cryptogram method. How to realize the privacy protection of transaction user identities and the audit regulatory of behavior simultaneously, and solve the conflicts between the two, are problems that must be solved before the blockchain can be implemented in major fields. The blockchain transaction traceability mechanism is implemented at the network layer. On the basis of its principle, probe nodes are arranged at the network layer and used to gather the transmitted information of blockchain at the network layer to analyze and determine the dissemination path of the transaction and to infer the originating node thereof; then, the anonymous address of the transaction is associated with the IP address of the originating node. Pustogarov [13] used the general way of Tor hidden services to analyze the Bitcoin network, enabling the attacker to reach specific Bitcoin transactions by providing a limited level of anonymity level. The blockchain address clustering mechanism is implemented at the data layer. According to its principle, the characteristics of blockchain transaction data are analyzed to obtain the correlations between different addresses. Different transaction addresses of the same trader are inferred by the discovery of the identity information of an address in a cluster. An address set concerning the I/O addresses in a trading slip is created, and classified pursuant to clustering rules upon traversal. Maesa et al.[5] clustered user behaviors, analyzed properties that are strictly related to the nature of Bitcoin, and assessed a classic characteristic model that measures the network richness of Bitcoin. The blockchain certificate management mechanism is implemented at the data layer. Based to its principle, a trusted certificate management authority, e.g. Public Key Infrastructure (PKI), is added to the blockchain operating mechanism, or some powerful super nodes are arranged with the function of awarding certificates, and the registration step of chain users is added to enable the certificate authority to trace any illegal user according to the registered identity information of the user in case of any unusual transaction. Given the attacks in malicious collusion with regulators, Li et al [14] put forward a concise proof scheme that can trace the Borromean range on the basis of Borromean ring signatures, sTBoRP, and an improved proof scheme that can trace the range of Bulletproofs, jTBuRP. Our design method is based on the improvement of the cryptographic algorithm implemented by the data layer, because cryptography is the core of the blockchain security system and the basis for the establishment of the blockchain system. We use NFT to record the copyright of digital collections, which can enhance the positivity of exchange and guarantee the security of data output and transmission, and support the sharing function [15]. Through the improvement of the cryptographic protocol, we realize the high-performance and regulatory requirements of blockchain applications, and provide cryptographic theoretical support and technical reference for the application of blockchain in museums.

3.3. Regulatory method design

We have constructed a dual-receiver public key encryption scheme in the MAXP on the basis of the bilinear mapping. We have defined three roles: Museum A, Museum B, and Regulator C in the following two typical application scenarios.

(1) Suppose Museum A needs to encrypt and send the same Data m to Museum B and Regulator C. In this case, A has to use the public keys of B and C for encryption and prove that the messages m contained in the two ciphertexts are equal by using the zero-knowledge proof protocol. Thus, ensuring that B and C will receive the same message is possible. This process will result in less efficiency as users will have to perform complex zero-knowledge proofs and conduct prolonged data sending and storage.

(2) In a typical regulatory cryptosystem, Sender A encrypts message m and sends it to receiver B. Suppose the administrator needs to view the ciphertext data of B. In this case, A must encrypt and send the message m to the administrator by using his public key and attaching a piece of zero-knowledge proof data, which leads to inefficiency.

Diament et al. [8] suggested a dual-receiver public key cryptographic scheme that uses a bilinear mapping over two groups. Our scheme is the extension of the three-method round Diffie-Hellman key exchange protocol to the ElGamal dual-recipient public key encryption scheme [10]. Therefore, for the two typical application scenarios described above, there exists no need to employ a zero-knowledge proof if A sends data encrypted to B and C, or if sender A delivers data to receiver B and token depositor C [12]. This reduces the computational complexity and data length, allowing for a more efficient operation of the protocol. In the scheme proposed by Diament et al., the encryption and decryption processes need bilinear mapping. We extended the algorithm SM2, and achieved dual receivers, with no need of bilinear mapping calculation in encryption and decryption processes, thereby, improving encryption and decryption speed. Moreover, in our scheme, the sender uses the public keys of two independent receivers to encrypt a message, and the two receivers both can decrypt the message with their private key. This process does not require the message consistency to be proved by the zero-knowledge proof protocol. The encryption scheme has two independent receivers. Receiver 1 can serve as the transaction receiver; Receiver 2 can serve as the regulator. Thus, in case that the transaction initiator encrypts exchange data, Receiver 1 can decrypt it and conduct a transaction. In addition, Receiver 2 can independently decrypt ciphertext information. In the blockchain transaction system, Receiver 2 can serve as the regulator of digital museum assets. Therefore, the museum regulator can independently regulate the blockchain transaction system. In the process, users can not collude with the museum regulator for any illegal transactions. The entire transaction system has a fine supervision effect, which can be applied to the exchange system of digital museum collections.

The flow of the algorithm is shown in Fig. 4, where the system parameters are consistent with the SM2 encryption scheme; the sender, receiver, and regulator generate their own private and public keys respectively; the sender enters its private key, the public keys of receiver and monitor, and the message, creates and signs the ciphertext, and then send it; the recipient decrypts the ciphertext with the private key; the regulator decrypts the ciphertext with the private key.

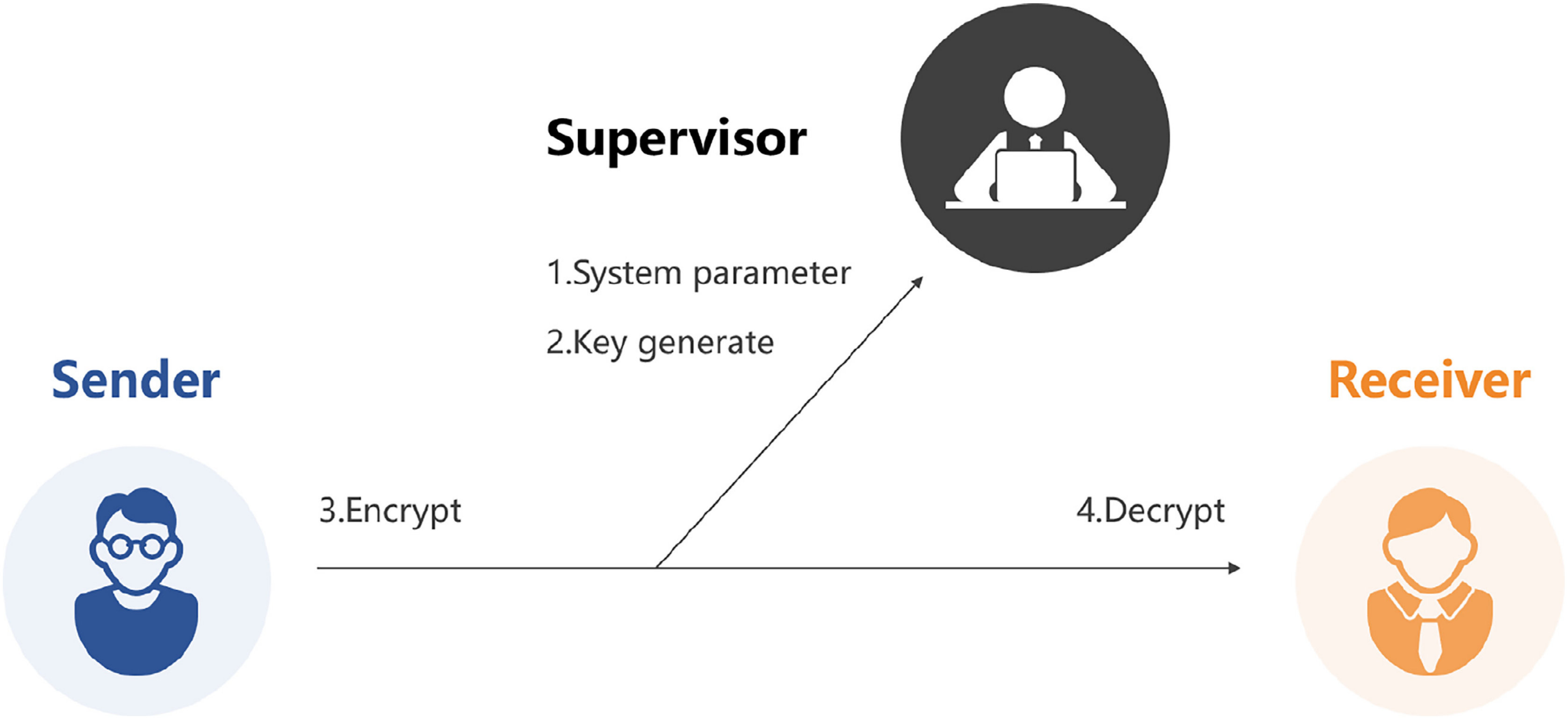


Fig. 4. Data encryption and decryption process.

3.4. Copyright registration method

The NFT copyright registration determines the ownership of the private right, such as intellectual property right through timestamps, Hash encryption technique and third-party authority certification, which defines the right constitution of the right owner and cooperative right holder of digital collections, and gives a clear indication of the right type, the term of validity and other basic right information [11]. Copyright is updated in the blockchain ledger. After writing a new block into the blockchain, users can enter the next right use procedure. The certification information of the regulator is the authoritative confirmation of intellectual property, and the synchronous propelling of right confirmation by the regulator and the application of intellectual property can effectively improve the transaction efficiency of intellectual property. On the basis of the standard requirements for data structure, numerical data and data content of collections, we have defined digital collections in the method, including collection name, collection number, collection type, collection source, age information, material information, quality information, collection volume information, completeness degree, preservation state, quantity of collection types, number of similar collections, collection time range, and 2D images, a total of 14 core elements. Heritage collection level, heritage collection type, age, material type, mass range, completeness degree, and collection time range can be chosen from the options provided in the standard [2]. The MAXP method supports museums in creating digital collections. The museum first selects the corresponding data type in the selection panel according to the data content, after which the image and video data are uploaded. The casting of the NFT then begins and is confirmed by the regulator. Once the casting is complete, the relevant permissions can be granted on the basis of the digital collection exchange requirements. The uploaded digital collection includes a detailed description of the contents of the collection, its creation history, transaction history, and so on. Consequently, the museum can get a better use experience after casting the NFT. During the casting process, it must be ensured that the collection data is intact, and the transmission network, exchange, and preservation process of collection data handling is secure. Data cannot be arbitrarily altered and deleted, and the privacy and sensitive information of the users will not be compromised. Comply with museum regulatory in managing data and ensuring the functioning of museum web services. Digital collection data is an asset, and mutual trust between the two parties must be addressed in the data casting and exchange. The recipient cannot maliciously shirk responsibility for data leaks. Moreover, both parties quickly reach consensus through smart contracts to avoid multi-party copyright declaration issues and ensure data copyright is not infringed.

3.5. Storage function

We have used the IPFS solution to create a distributed storage system. The data structure employs DHT as the underlying architecture. IPFS is a peer-to-peer distributed file system that connects all computing devices with the same file system. A unique identifier, CID [6], will be returned when a digital collection is uploaded to IPFS, and the museum recipient is required to provide the exact CID to download the corresponding file from IPFS. Fig 5 illustrates the storage model architecture. Using content-based addresses instead of domain-based addresses enables users to search directly for content stored somewhere with only the hash of the content to be verified. As a result, the web is faster, more secure, and more persistent. The characteristics of the storage are as follows:

(1) Each file and all blocks within it are given a unique fingerprint called a cryptographic hash.
(2) Eliminated duplicate files on the network.
(3) Each network node stores only the content it is interested in, as well as indexing information.
(4) When queried, the file is found by a unique hash value on the node where it is stored.
(5) Each file is autonomous using the decentralized naming system of IPFS.

Fig. 5 illustrates the processes, such as index creation, search procedure, index storage, and caching. Steps 1–4 are the index creation and storage, and steps a-e are the searching processes. The IPFS data acquisition process includes creation and storage, searching, and invoking. The CID is the unique identifier returned by the system for files uploaded to the IPFS system for storage. It must be provided correctly for downloading the corresponding file from IPFS. DHT (Distributed Hash Table), distributed storage model [17]. Without a server, each client is responsible for routing a small area and a minor portion of data, ultimately presenting the entire DHT network for addressing and storage.

4. System implementation

On the basis of the MAXP method, we use Ethereum to build an encrypted exchange system for digital collections. By using Our system, Beijing Planetarium has exchanged with 5 sets of digital collections of Beijing Museum of Natural History, realizing the quick and safe transfer of temporary use rights of digital collections.

Museums that cast NFT in the system can obtain original NFT certificates, and support the traceability of museums to blockchain browsers. Fig. 6 is the main interface of the system, in which, the thumbnails of digital collections recently released by the museum can be previewed, so that users can select the digital collections that must to be exchanged.

The system shown in Fig. 6 is a publicly released sharing platform. The main interface guides users to quickly locate and search for the concerned digital collection, to facilitate the subsequent exchange. The casting process of the digital collection is: entering the digital collection information - storing it on IPFS - casting the digital collection NFT - complete the casting process to generate a non-homogeneous token.

Fig. 7 shows the NFT of the Protoceratops skeleton model of the Beijing Museum of Natural History, including thumbnails of digital collections, related introductions, and historical log information. The digital collection exchange is carried out in a traceable, fully auditable, and traceable environment, and borrowing and returning of digital collections can greatly improve the efficiency. If the borrower applies, the lender reviews the release, and the borrower has a token for access to the data.

The Beijing Ancient Observatory, which was built in the seventh year of the Ming dynasty (1442 CE), is part of the Beijing Planetarium. The digital collections we have created include five imposing and superbly cast astronomical observation instruments of the Qing Dynasty in Beijing Planetarium (the hash value shown in Table 1): Elliptic Armilla, Celestial Globe, New Sextant, Quadrant, and Armillary Sphere.

Table 1 includes the names of the Beijing Planetarium's on-chain collection, the hash values of the casting transaction, the NFT numbers, and the casting time of the NFT.

The digital collections created by the Beijing Museum of Natural History are: the fossil models of Mamenchissaurus, the skeletal models of Lufengosaurus, the fossil models of Psittacosaurus, the skeletal models of Yangchuanosaurus, and the skeletal models of Protoceratops. The collection hash values are shown in Table 2.

As exhibited in Table 2, the names of the on-chain collection of the Beijing Museum of Natural History, the hash values of the

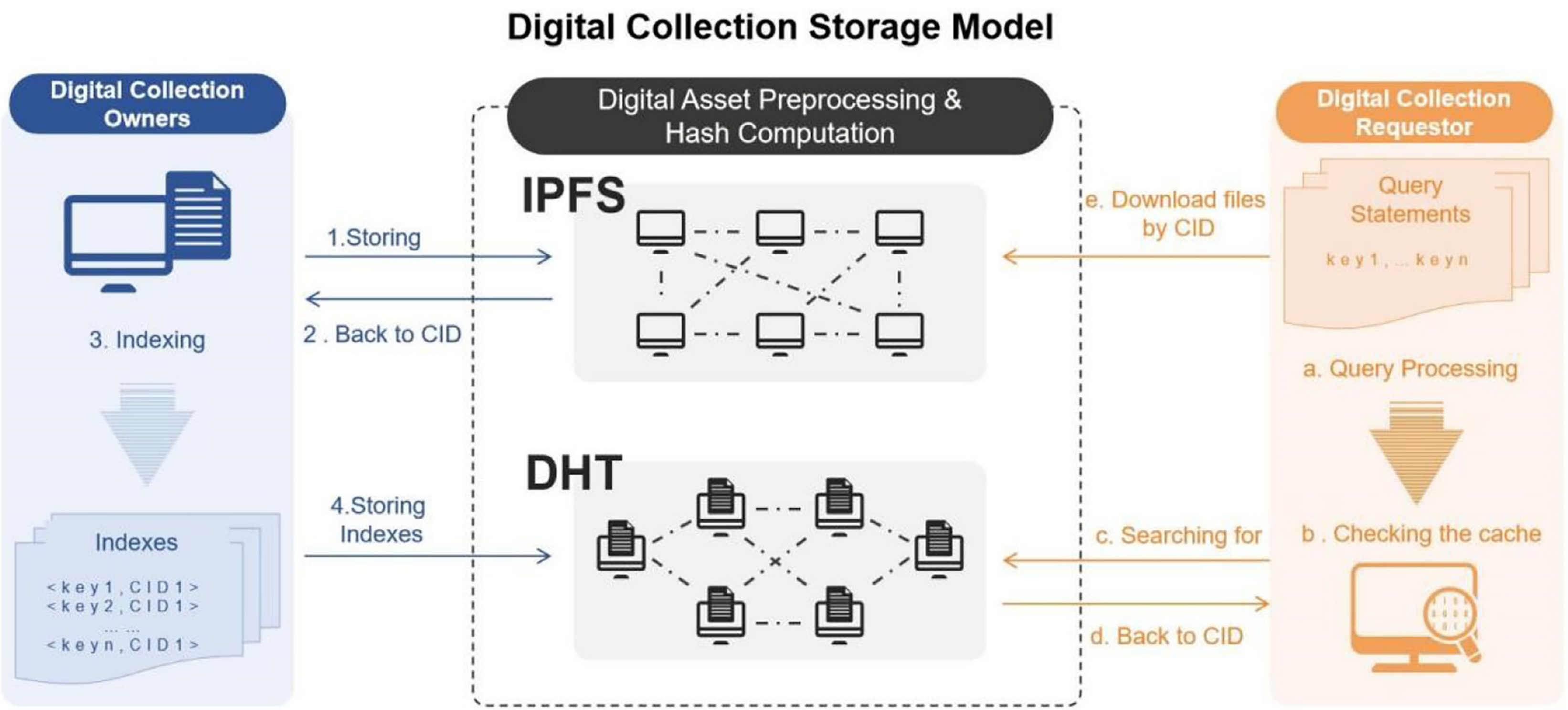
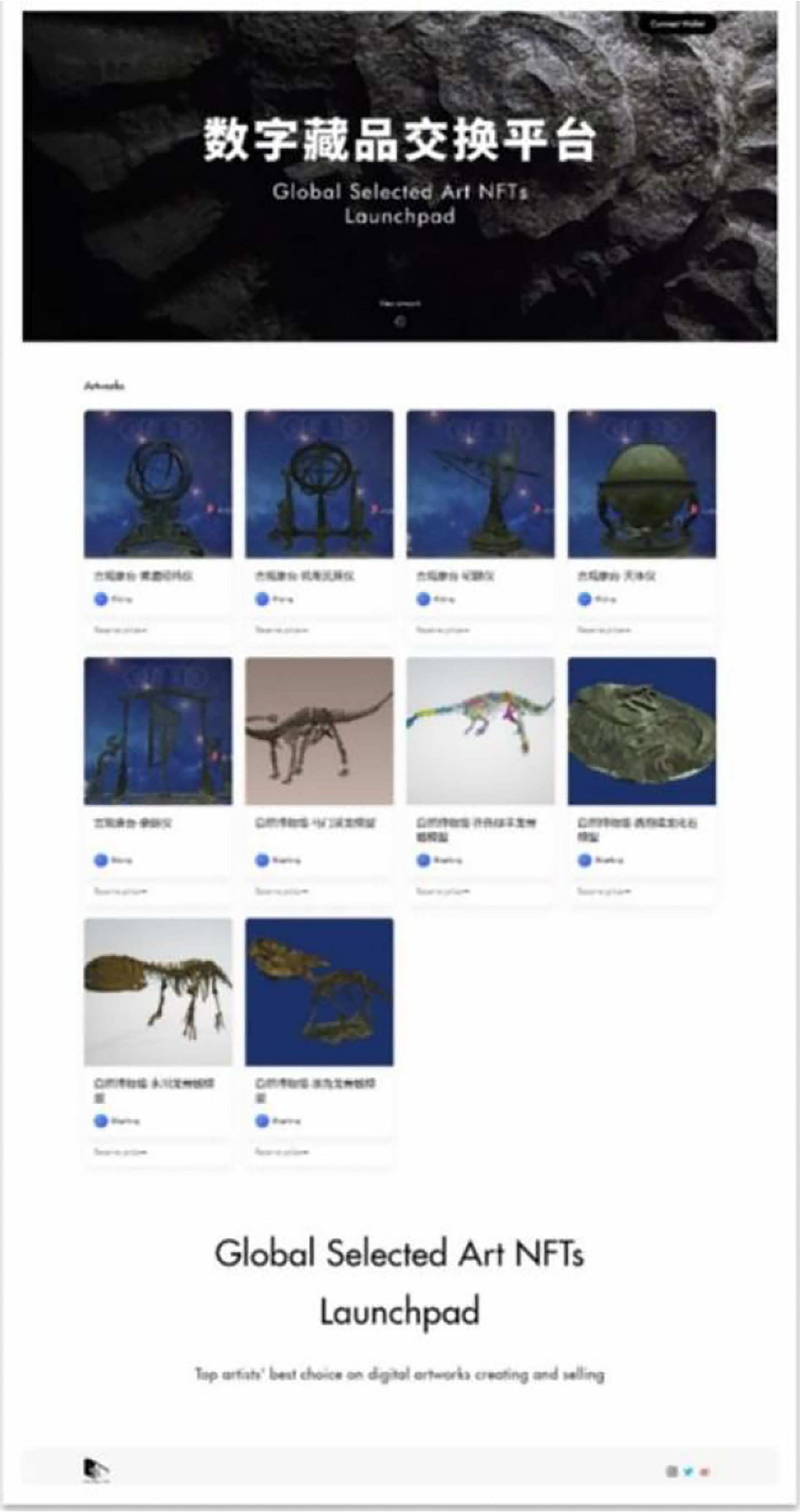


Fig. 5. The architecture of the Smart-MAXP contract.



数字藏品交换平台

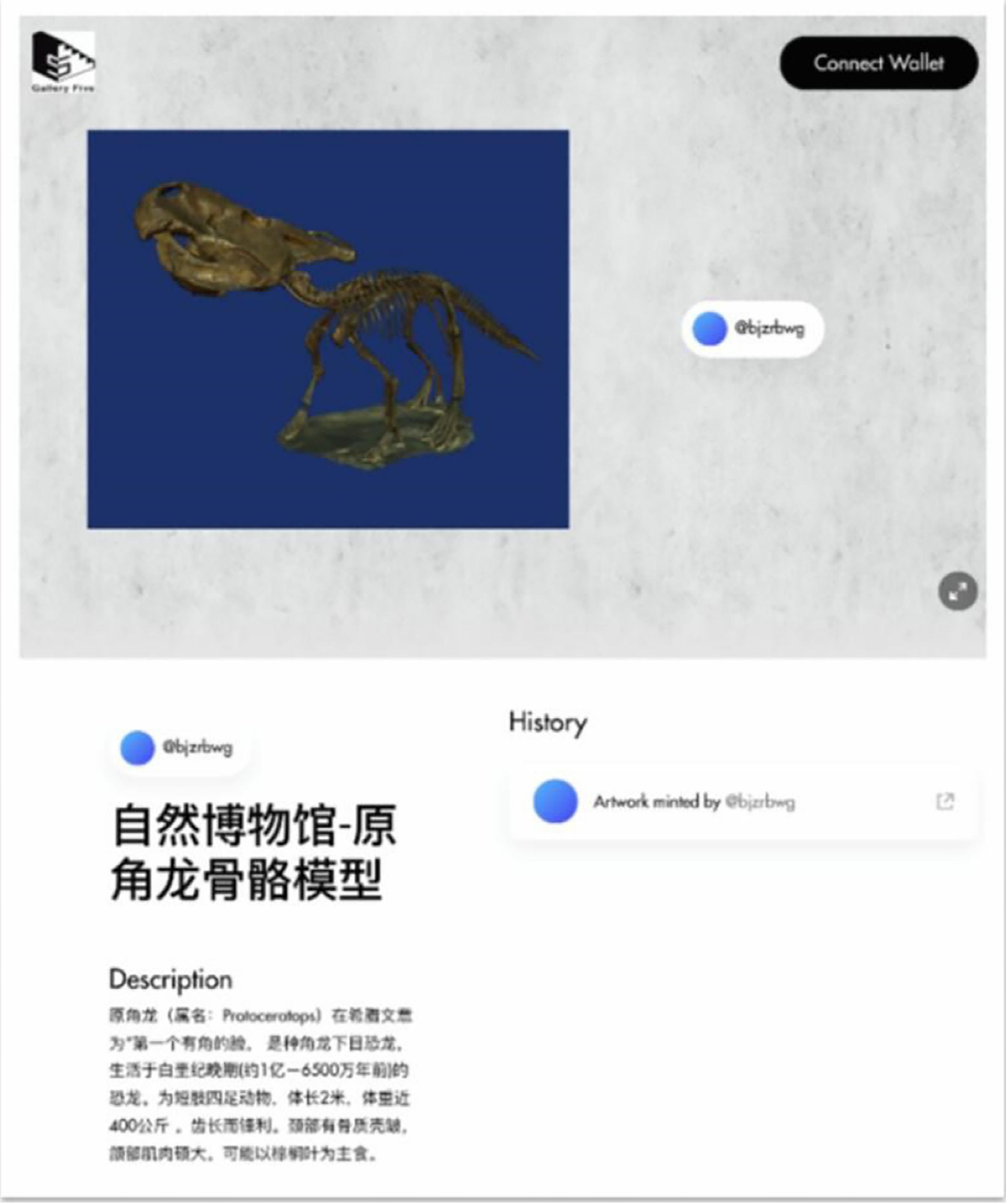
Global Selected Art NFTs
Launchpad

Artworks

Global Selected Art NFTs
Launchpad

Top artists' best choice on digital artworks creating and selling

Fig. 6. System main interface.



@bjzrbwg

自然博物馆-原
角龙骨骼模型

Description

原角龙（属名：Protoceratops）在希腊文意
为"第一个有角的脸。是种角龙下目恐龙，
生活于白垩纪晚期(约1亿－6500万年前)的
恐龙，为短肢四足动物，体长2米，体重近
400公斤 。齿长而锋利，颈部有骨质壳皱，
颌部肌肉顿大，可能以棕榈叶为主食。

History

Artwork minted by @bjzrbwg

Fig. 7. The NFT of the Protoceratops skeletal model.

casting transaction, the NFT numbers, and the casting time of the NFT.

The MAXP method is a technical standard for establishing a data path between two arbitrary museums on the blockchain. The systematic data interaction standards we constructed focuses on providing long-term, efficient exchange patterns for joint projects between museums, thereby meeting the developing demands of museums for the cross-museum collection information interchange in the context of the information age. System supports applications with NFT casting function. NFTs can be casted in the Ether-

Table 1
Hash values and casting information of the 5 sets of digital collections in Beijing Planetarium.

Name	Sketch map	Casting transaction hash value	NFT ID	Casting time
Elliptic Armilla		0x146dbac9fe1236dfabe859671d54l5a6 f0d5434315f919eafb2b2f1d9db078e7d	21	Dec-09-2021 08:09:00 PM +UTC
Celestial Globe		0x0c3799cc79e211e74e5cea8f3052e59 b80fb897a5191f1b1059d2a1bd7325c7d	24	Dec-09-2021 08:25:06 PM +UTC
New Sextant		0x14d493cfed1b8a21e2ab5ec3106b32e d62d263511cbd73b19ef5edfa37123ab2	23	Dec-09-2021 08:16:59 PM +UTC
Quadrant		0x83edf522dafef9f40150eb9d84e4a7aa 6337c81230b946c203bb92d0ee790e86	25	Dec-09-2021 08:30:38 PM +UTC
Armillary Sphere		0xab1f3a950dfc894fc1aa956a97c1ea6d bd0d0dce0c7ad134b4127dff256dbe16	22	Dec-09-2021 08:13:34 PM +UTC

Table 2
Hash values and casting information table of 5 sets of digital collections in Beijing Museum of Natural History.

Name	Sketch map	Casting transaction hash	NFT ID	Casting time
Mamenchissaurus		0xd8266c253f8f707df1edcf131f94c56f b60770a78f912c4f1910c8cda1115718	26	Dec-09-2021 08:35:51 PM +UTC
Lufengosaurus		0xceb1f5a9eaf563dd6190ed349eb7858 6ca9b9b38fd2e605d94f02c72dcddd237	27	Dec-09-2021 08:38:21 PM +UTC
Psittacosaurus		0x0220942ed774f9f1c0bbf810f2ed474 41f187929cc3d6e87c64c7f7fd0b4295e	28	Dec-09-2021 08:45:42 PM +UTC
Yangchuanosaurus		0x919351fc32a9c5a50e4949c70fb1a51 8d34870e0f9836fce5b1a847b5ddf339c	29	Dec-09-2021 08:49:51 PM +UTC
Protoceratops		0x1ef862841d74a95c7487b85e7b0f637 2f9c384f59d906f85eea9863f2832276b	30	Dec-09-2021 08:52:13 PM +UTC

net blockchain network to turn a museum's digital content artwork (e.g., a 3D model) into a limited-edition digital asset, generating higher scarcity of commercial value.

5. Results and discussion

5.1. Case study introduction

The traditional method of exchange with digital collections between the Beijing Planetarium and Beijing Museum of Natural History is that the two museums sign an agreement offline and copy the document through the physical storage media. The signed agreement offers the sharing time, exhibition venue, exhibition purpose, and so on. It then copies the corresponding data through a specific storage device and delivers it offline to the designated museum for exhibition. Upon expiry of the agreement, the relevant storage media will be shipped back to the contributing museum. The exhibitor guarantees that no copies will be retained and that the data will not be misused. The offline process is cumbersome and with potential risk at security, and efficiency and traceability need to be improved. Misuse the data may lead to data breaches or free dissemination, which can cause severe economic and social challenges. Through the MAXP system we have established, the two museums upload the encrypted data of the digital collections to the Ethernet blockchain and cast NFTs for the digital collections that must be interacted with. The relevant exchange protocols are drawn up and executed through smart contracts, and the exchange is confirmed online to complete the collection data exchange, improving efficiency and security significantly. The traditional centralized database data management model is vulnerable to systemic risks, such as malicious data modification or tampering, whereas the adoption of the MAXP system ensures data security. Our system features digital collection search-and-use, click subscribe-and-read, and download-and-copy after passing encryption authentication, preventing collection data from being copied and disseminated on a large scale, and enabling data traceability and control, and protecting digital copyright.

5.2. Discussion

Traditional digital museum collections management systems are similar to a "polycentric" data construction framework, making data sharing and enhancement difficult. Therefore, we have designed an open, transparent, and collaborative data exchange model for the digital museum collections. After choosing a type of digital collections, the museum can upload data files, begin casting NFTs upon uploading, and go through on-chain confirmation. After the completion of NFT casting, relevant permissions may be given for exchange following requirements for digital collection exchange. The system is characterized by traceability, transparency, and tamper proofing.

5.2.1. Traceability

The ownership and the token metadata stored on the blockchain of the digital collection NFT can be publicly identified. With CID, the IPFS can verify if the data have been tampered with and the storage and redundancy status of data.

5.2.2. Transparency

The whole process of digital collections, from casting to on-chaining to exchange, is transparent, whereas the storage of the NFT metadata and collection data is not, and the casting party chooses its method of storing. No possibility exists that the NFTs cannot be published and interacted with as long as they are casted

Table 3
Comparison between SM2 and our scheme.

		Enc(μs)	Dec1(μs)	Dec2 (μs)	Dec3 (μs)
32M bytes	SM2 encryption	155.4	104.9	-	-
32M bytes	Our scheme	270.6	104.9	222.4	225.2
64M bytes	SM2 encryption	156.2	105.1	-	-
64M bytes	Our scheme	274.7	105.1	222.9	232.4
1024M bytes	SM2 encryption	158.4	136.4	-	-
1024M bytes	Our scheme	307.9	136.4	256.7	258.7

given that the on-chain systems on which digital collections interact will not crash.

5.2.3. Tamper proof

Once validated, NFT's metadata and complete transaction records are stored permanently, allowing only new information to be added, with no past data can be modified. Tamper-proof due to the employing of the IPFS documentation system. The information seen in each museum is instantly updated, straightforward, and easy to circulate, eliminating the traditional information barriers between the data contributor-mediator-data acquirer.

5.2.4. Encryption and decryption efficiency analysis

We experimentally test the cryptogram scheme of MAXP with the SM2 scheme. Hardware configuration: Operation system Centos7.7, kernel 3.10.0–1062.el7.x86_64, CPU Intel(R) Xeon(R) Gold 5118 CPU 2.30GHz, and memory 192GB.

As shown in Table 3, the horizontal columns indicate the encryption time of sender, decryption time of the recipient, the decryption time of sender, and the decryption time of regulator, while the vertical columns represent the test results corresponding to the SM2 encryption solution and Our scheme.

The encrypted data capability is 32Mbytes, and the SM2 encryption time is 155.4μs respectively. The encryption time of Our scheme is 270.6μs respectively. When encrypting 64Mbytes of data, the encryption time of SM2 is 156.2μs, and the encryption time of Our scheme is 274.7μs. It takes 158.4μs to encrypt 1024Mbytes of data, and the encryption time of Our scheme is 307.9s respectively. As the scheme presented in Our paper additionally supports sender and regulator decryption, the encryption speed is relatively slow. However, the decryption time of the recipient in the SM2 and Our scheme are the same, both being 104.9μs 105.1μs 136.4μs. Finally, unlike the SM2 algorithm, Our scheme supports sender and regulator decryption with decryption times are 222.4μs 224.9μs 256.7μs and 225.2μs 232.4μs 258.7μs. Although the decryption time for the sender and receiver is slightly longer in Our scheme than in SM2, the decryption is fast. Moreover, the decryption speed of the sender and regulator does not affect the operation, while the decryption function of the sender and regulator has a great scope of application.

6. Conclusions

To address trust and security issues in the exchange of digital collections, we designed and completed a blockchainbased data exchange system of digital collections. The NFT mechanism and the process of data operating and accessing can be recorded in cryptographic signatures and an Ethereum distributed ledger, and data encryption can be implemented by means of the dual-receiver algorithm. The system has tamper-proof function, and the core of regulatory technology is key management, encryption algorithms, and smart contracts. The system we built has realized the casting of 10 sets of NFT digital collections of Beijing planetarium and Beijing Museum of Natural History. Two display methods exist, namely, physical and digital copyright. The museum staff can keep accurate records and preserve relevant data; the regulator can monitor overall data and transaction tokens, deal with any abnormal interactions in a timely manner, and achieve in-process monitoring. Practice has confirmed that the designed MAXP method is safe and reliable, which can realize the display and circulation of digital collections, and has an effective adjustment mechanism, which can be corrected for the transaction security control after the problem occurs. The evaluation on the encryption algorithm suggests that the scheme has fast decryption, as well as the security and expansibility of decentralized trust management. The system built by the MAXP method can effectively realize the interaction of digital collections, while regulating the content and tokens of digital collection transactions. Note: The authors declare no competing financial interest. Acknowledgements: We offer the great thanks to Beijing Computing Center Co., Ltd. for providing the experimental environment and to Dr. Zhong Lin and Mr. Liu Jidong for providing some application and algorithm suggestions. Our research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Note

The authors declare no competing financial interest.

Acknowledgements

We offer the great thanks to Beijing Computing Center Co., Ltd. for providing the experimental environment and to Dr. Zhong Lin and Mr. Liu Jidong for providing some application and algorithm suggestions. Our research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.culher.2022.11.001

References

[1] U. Art, Can the blockchain help secure museum collections?, 2021. https://www.uncopied.art/blog/blockchain-museum-collection-inventory/

[2] E. Bertacchini, F. Morando, The future of museums in the digital age: New models of access and use of digital collections (2011).

[3] Virtual equivalents of real objects (VEROs): a type of non-fungible token (NFT) that can help fund the 3d digitization of natural history collections, Megataxa 6 (2) (2021) 9395. BOLTONS J, C.J.R.

[4] M. Charr, Legal case concerning a 3d scan of a museum artefact may impact on all institutions. https://www.museumnext.com/article/legal-case-concerning-a-3d-scan-of-a-museum-artefact-may-impact-on-all-institutions/, 2019.

[5] D.D.F. Maesa, A. Marino, L. Ricci, Data-driven analysis of bitcoin properties: exploiting the users graph, Int. J. Data Sci. Anal. (6) (2017) 1–18.

[6] E. Daniel, F. Tschorsch, Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks (2021).

[7] D. Das, P. Bose, N. Ruaro, C. Kruegel, G. Vigna, Understanding security issues in the NFT ecosystem(2021).

[8] T. Diament, H.K. Lee, A.D. Keromytis, M. Yung, The dual receiver cryptosystem and its applications, Int. J. Netw. Secur. 13 (3) (2011).

[9] N.K. Dumpeti, R. Kavuri, A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain, Mater. Today:. Proc. (3) (2021).

[10] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms 31 (4) (1985) 469–472.

[11] F. Valeonti, Crypto collectibles, museum funding and openGLAM: challenges, opportunities and the potential of non-fungible tokens (NFTs), Appl. Sci. 11 (2021).

[12] I. Damgård, On protocols, Lecture Notes (2002).

[13] P. Ivan, Pdd defence: deanonymisation techniques for tor and bitcoin.

[14] L. W, et al., New constructions of traceable range proofs: towards multiple regulation and joint regulation, Cryptol. ePrint Arch. (2020).

[15] F. Liddell, Building shared guardianship through blockchain technology and digital museum objects (2021).

[16] Z. Ma, W. Huang, W. Bi, H. Gao, Z. Wang, A master-slave blockchain paradigm and application in digital rights management, Commun. China 15 (8) (2018) 174–188.

[17] S. Muralidharan, H. Ko, An interplanetary file system (IPFS) based iot framework, in: 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1–2, doi:10.1109/ICCE.2019.8662002.

[18] M. Patel, M. White, N. Mourkoussis, K. Walczak, R. Wojciechowski, J. Chmielewski, Metadata requirements for digital museum environments, Int. J. Digit. Librar. (2005).

[19] A. Qureshi, D.M. Jiménez, Blockchain-based multimedia content protection: review and open challenges, Appl. Sci. 11 (1) (2020) 1.

[20] A. VisWa, F.K. Hussain, A blockchain based approach for multimedia privacy protection and provenance, 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 2018.

[21] Y.C. Wang, C.L. Chen, Y.Y. Deng, Museum-authorization of digital rights: a sustainable and traceable cultural relics exhibition mechanism, Sustainability 13 (2021).

[22] B. Zheng, L. Zhu, M. Shen, D.U. Xiaojiang, M. Guizani, Identifying the vulnerabilities of bitcoin anonymous mechanism based on address clustering (2020).

[23] M. Zhaofeng, H. Weihua, G. Hongmin, A new blockchain-based trusted DRM scheme for built-in content protection, EURASIP J. Image Video Process. 2018 (1) (2018).

[24] J. Zhang, M. Guo, B. Li, R. Lu, A transport monitoring system for cultural relics protection based on blockchain and internet of things, J. Cult. Herit. (5) (2021).

[25] P. Zhu, J. Hu, X. Li, Q. Zhu, Using blockchain technology to enhance the traceability of original achievements, IEEE Trans. Eng. Manage. (2021) 1–15, doi:10.1109/TEM.2021.3066090.