Research on Constructing a Digital Management System Model for Ancient Books Using Blockchain Technology (Postprint)

Authors: Gao Li, Wang Chunyan, Gao Xindan

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] From the perspective of blockchain technology, this study proposes a blockchain-based system model for digital ancient books management as a solution to existing problems in the field of ancient books preservation and utilization, thereby realizing an innovative paradigm for ancient books governance. [Method/Process] First, a decentralized P2P architecture based on blockchain is designed from both structural and implementation dimensions. Network-wide consensus is achieved through node-initiated transactions, block construction, and legitimacy verification to link blocks across the network. Second, an information storage mechanism and smart contract protocol algorithms are established, with automated execution ensuring the efficiency and transparency of the model, thereby realizing immutable and traceable digital ancient books copyright registration and circulation utilization information. Finally, the consensus mechanism and IPFS protocol-based distributed storage system address ancient books data storage and security concerns, while a reasonable incentive mechanism is established to achieve effective management of ancient books data. [Result/Conclusion] Through the establishment of this model, the traditional centralized management paradigm of ancient books databases is abandoned, and the entire process of ancient books preservation and utilization is rendered traceable and immutable in the form of block+chain, thereby achieving technological innovation in ancient books preservation.

Full Text

Preamble

Vol. 63 No. 3 February 2019 ChinaXiv Cooperative Journal

Research on Constructing a Digital Ancient Book Management System Model Using Blockchain Technology

Gao Li[1], Wang Chunyan[1], Gao Xindan[2]
[1]Northeast Forestry University Library, Harbin 150040
[2]College of Information and Computer Engineering, Northeast Forestry University, Harbin 150040

Abstract

[**Purpose/Significance**] From the perspective of blockchain technology, this paper proposes a blockchain-based system model for digital ancient book management to address existing problems in the protection and utilization of ancient books, thereby implementing an innovative management model. [**Method/Process**] First, a decentralized P2P architecture based on blockchain is designed from both construction and implementation perspectives. Network-wide consensus linking of blocks is achieved through node-initiated transactions, block construction, and legitimacy verification. Second, an information storage mechanism and smart contract protocol algorithm are established to automatically execute and ensure the efficiency and transparency of the model, enabling tamper-proof and traceable copyright registration and circulation utilization information for digital ancient books. Finally, the consensus mechanism and IPFS protocol system's distributed storage mechanism solve ancient book data storage and security issues while establishing reasonable incentive mechanisms to achieve effective management of ancient book data. [**Result/Conclusion**] Through this model, the traditional centralized management mode of ancient book databases is abandoned, and the entire process of ancient book protection and utilization is made traceable and tamper-proof through the block+chain format, thereby achieving technological innovation in ancient book protection.

Classification Number: G250
Keywords: blockchain, digital ancient books, smart contract, IPFS
DOI: 10.13266/j.issn.0252-3116.2019.03.011

In November 2017, when President Xi Jinping met with U.S. President Trump and visited the Forbidden City, he introduced: "China has a history of more than 5,000 years. Although Egypt's history is longer, China is the only civilization whose culture has never been interrupted and has been continuously passed down." The inheritance of Chinese culture relies on the vast sea of ancient books and documents. As Qian Zhendong wrote in *Shu E Shu Yao*: "Culture is to a nation what spirit is to a body, and ancient books are what culture relies on for transmission" [1]. Ancient Chinese books record and testify to the continuous history of Chinese civilization, inheriting the humanistic spirit and moral norms contained in excellent traditional Chinese culture. As generations pass and time goes by, ancient books have experienced catastrophic hardships, making the surviving rare editions increasingly valuable, treasured by all collecting institutions [2]. Digitalization of ancient books aims to protect and utilize these precious resources, representing a new method for organizing Chinese classics, a new pathway for disseminating traditional culture, and a new symbol of spir-

itual civilization construction [3]. Since the "Eleventh Five-Year Plan," China has proposed launching major national publication projects such as the digitalization of *Zhonghua Da Dian*. In recent years, with strong support from relevant national departments for digital transformation and upgrading, digital ancient book resources have gained new vitality [4]. However, while developing rapidly, digital ancient books also face urgent issues regarding ownership, circulation and utilization, and data security that demand attention.

2. Applicability and Research Significance of Blockchain-Based Digital Ancient Book Management System

2.1 Applicability of Blockchain for Digital Ancient Book Management

2.1.1 Subject Applicability Digitalization is an effective means for protecting and utilizing ancient books. The digital ancient book management system requires numerous participating entities for coordination and support, including libraries, museums, collecting institutions or individuals, digitalization vendors, and database companies. These participants exhibit diversified characteristics, forming multiple decentralized and autonomous ancient book data centers. Blockchain systems typically adopt peer-to-peer P2P networks for decentralized, distributed organizations. All nodes have equal status and provide proof of work through encryption algorithms for block verification. They interconnect through a flat topological structure without centralized special nodes or hierarchical structures. Therefore, the subject characteristics of digital ancient book management systems highly align with blockchain's decentralization and distributed storage features.

2.1.2 Object Applicability The core of blockchain technology utilizes encrypted block structures to verify and store data blocks. All user nodes generate and update data with timestamps through consensus algorithms. In the blockchain, data is permanently stored in blocks. The blockchain acts as a state machine that confirms and records each state change in the network, generating blocks and linking them chronologically into a chain. Each block records all transaction information occurring during its creation period [13]. The current blockchain application fields can be summarized as digital currency, financial transactions, product traceability, data storage, data authentication, and digital asset management, enabling registration, rights confirmation, authorization, and real-time monitoring of intangible assets such as intellectual property rights for various digital works. The objects of ancient book management are digital ancient books, whose entire circulation process from collection and organization, digital processing, indexing and classification, sharing and circulation to authorized use can typically be abstracted as the formation and transaction process of data assets. Therefore, the object composition of digital ancient book management highly matches blockchain's digital asset management application scenarios.

2.1.3 Functional Applicability While current digital ancient book management brings convenience to researchers and readers, it also faces several problems: (1) Increasing infringement cases, with frequent plagiarism and piracy among peers; (2) Lack of content control, where digital ancient book content is arbitrarily added, deleted, or modified to meet market needs; (3) Absence of incentive mechanisms, as public libraries, museums, or individual collectors with ancient book collections are not enthusiastic about digital ancient books, making digitalization of some traditional ancient books more difficult; (4) Digital ancient books appear in centralized database management forms, where full-text image databases and text-image comparison databases are more conducive to protection and utilization but increase storage requirements and pose data security issues. These problems mainly arise from weak trust foundations among participating entities, centralized management of ancient book databases, and lack of effective incentive measures. Blockchain's characteristics of all-node participation in verification, immutability, traceability, and consensus-based incentive mechanisms align perfectly with the functional requirements for building a digital ancient book management system to enhance ancient book protection and utilization.

2.2 Significance of This Study

This paper introduces blockchain technology into the field of digital ancient book management and designs a blockchain-based digital ancient book management model. Through blockchain's inherent characteristics of immutability, timestamps, traceability, and distributed storage [12], it provides full on-chain services for digital ancient book management in copyright protection, circulation and sharing, and data security storage. Ancient book data as blocks is constructed, verified, and linked by participants. Every transaction (operation) occurring in the network is permanently preserved in the blockchain and cannot be altered. This enables users to register copyrights for digital ancient books with network-wide consensus confirmation, while all processes such as downloading, copying, and browsing are recorded and traceable, ensuring the authority and traceability of digital ancient book copyrights.

3. Technical Foundation for Model Construction

3.1 Basic Principles of Blockchain

Blockchain technology (BT), also known as distributed ledger technology, is characterized by decentralization, immutability, traceability, and transparency, allowing everyone to participate in database recording. The main concepts include: (1) Transaction: Each operation changes the ledger state once and adds a record; (2) Block: Records transactions and state results occurring within a period, representing a consensus on the current ledger state; (3) Chain: Blocks are 串联 in chronological order, forming the entire log record of state changes. Block data structures are generally divided into block headers and block bodies [14]. The block header records information H including: Version, previous

block Hash value, Merkle root, Timestamp, Target_{bits} (difficulty value), and Nonce (fixed size of 80 bytes). The block body records corresponding transaction information T and other information U. The formal definition of block B is shown in Equation (1):

$$B = (BH, BT, BU)$$

The block body records all transaction information during block generation, with variable size. Although the block header is much smaller than the block body, most functions are implemented by the block header.

3.2 Smart Contracts

Smart contracts are sets of preset condition computer codes proposed by scholar Nick Szabo in 1995. As triggers on the blockchain, smart contracts execute accurately and automatically without human intervention [15]. In the digital ancient book management blockchain network, smart contracts include transaction processing and preservation mechanisms, as well as a complete state machine for accepting and processing various smart contracts. Both transaction preservation and state processing are completed on the blockchain. This process encapsulates preset rules in code within blocks, sets trigger conditions based on event description information, and after verification and linking by digital ancient book management blockchain network nodes, the blockchain network monitors deployed contracts in real-time, triggering smart contracts for state machine judgment. If trigger conditions for one or more actions in the automatic state machine are met, the state machine selects contract actions to execute automatically according to preset information.

4. Model Architecture Design Scheme

Establishing a digital ancient book management network based on blockchain technology can achieve decentralized consensus trust mechanisms and distributed storage, changing the relationships among parties in traditional digital ancient book protection and utilization activities. By constructing a P2P architecture with blockchain as the core storage mechanism, the management model for digital ancient book copyright registration, circulation, and data security is realized through creating transactions, constructing blocks, verifying block legitimacy, and linking blocks. The specific model design for the digital ancient book management blockchain network architecture is shown in Figure 1 [Figure 1: see original paper].

4.1 User Node Block Construction and On-Chain Mechanism

4.1.1 Transaction Initiation User nodes are client terminals connected to the blockchain network. Each operation request performed by a user node on

the client side can be viewed as initiating a transaction that generates transaction data. Blockchain nodes submit transaction data to smart contract state machines deployed in the blockchain, triggering Remote Procedure Call (RPC) interface to execute preset smart contract algorithms, thereby implementing functions such as digital ancient book copyright registration, verification, and transaction.

In the designed model, smart contract algorithm automatic execution requests include three types: (1) Digital ancient book copyright registration request, denoted as Tα; (2) Digital ancient book usage authorization request, denoted as Tβ; (3) Digital ancient book copyright verification request, denoted as Tγ. For example, the specific execution process for copyright registration is: In the digital ancient book management blockchain network, when a copyright user registers copyright for their digital ancient book, the node sends a Tα request to the blockchain. The smart contract algorithm deployed in the blockchain network automatically executes a Tγ request, traversing the blockchain network. If Tα is true, the newly initiated transaction is broadcast across the network, and the smart contract algorithm writes the digital ancient book copyright information into a new block. The new block's header records this transaction information with a timestamp, making this ancient book copyright information data on the blockchain immutable. Moreover, every operation information and flow data of this data is recorded in the block body in chronological order as added records. The transaction initiation processes for Tβ and Tγ follow the same principle, providing authoritative proof for digital ancient book copyright ownership.

4.1.2 Transaction Processing The transaction processing process in the blockchain network is also the process of generating new blocks. Whether transaction processing can be completed and new blocks generated is jointly determined by nodes and the consensus mechanism in the blockchain network. Nodes determine who has block generation qualification, while the consensus mechanism determines which of these qualified nodes can ultimately generate a block.

Blockchain consensus mechanisms involve all nodes calculating Hash to achieve Proof of Work (POW). Suppose there are sequentially generated data blocks A, B, and C. The formal definition of Hash header calculation is shown in Equation (2):

$$\begin{aligned} H_0 &= Hash(A \| Nonce_0) \\ H_1 &= Hash(B \| H_0 \| Nonce_1) \\ H_2 &= Hash(C \| H_1 \| Nonce_2) \end{aligned}$$

In Equation (2), due to the one-way nature of the cryptographic Hash() function: Hash(x) = y, it is difficult to find x through y; $\|$ represents concatenation; Nonce is a random number. When a node receives a transaction request initiated

by a user, the digital ancient book management blockchain network forms a consensus mechanism that performs mathematical operations on local nodes to obtain bookkeeping rights, then calculates the latest Hash header. When a node successfully calculates a Hash that meets requirements, a new digital ancient book copyright block is generated. The new block is broadcast among all network nodes. Each consensus requires participation from the entire network in calculations. When over 50% of nodes confirm the block is valid, the copyright information is written into the blockchain for storage [16]. The entire blockchain transaction processing process is automatically executed by smart contracts through code without intervention, ensuring the fairness and transparency of the entire process.

4.2 Blockchain P2P Network Implementation Mechanism

4.2.1 Optimization of Transaction Information Storage Consensus Mechanism Current blockchain consensus mechanisms mainly adopt the Proof of Work (POW) mechanism. While processing transaction data, nodes use the SHA256 algorithm to continuously perform Hash calculations to compute the random number Nonce. When one node in the network calculates the Nonce, it publishes its packaged block. Other nodes verify it, and after verification, they consistently agree to link this block to the blockchain, then continue constructing and calculating the next block [17]. During this process, fork blocks are generated and require multiple confirmations. This simple brute-force method ensures the legitimacy of the entire blockchain system. However, this consensus mechanism has obvious deficiencies when applied to transaction information storage systems in digital ancient book management.

Therefore, in the digital ancient book management blockchain network, to maximize the benefits of consensus block computation itself and ensure the relationship between transaction information data storage security and effectiveness, this paper adopts a consensus mechanism combining node verification sets and POW benefit sets to achieve network-wide consensus [18]. In the Hash calculation process for constructing new blocks, when all nodes have pending verification information, nodes for their own benefit will not change their verification results for other blocks [19]. The mathematical description in the transaction information storage system is: B = {B_1, B_2, …, B }, representing a set of nodes. Suppose: After node B 's computation and construction of an information block, it receives verification from other nodes and POW benefits, which can be represented by set G = {V $_1$, …, V : u }. Then in the verification combination (V $_1$, …, V , …, V) formed by nodes for the information block constructed by node B , any participating verification node B submits verification result V to node B , satisfying Equations (3) to (5):

$$V_{ij} = \begin{cases} 1, & \text{if node } B_j \text{ verifies that the block submitted by node } B_i \text{ is true} \\ -1, & \text{if node } B_j \text{ verifies that the block submitted by node } B_i \text{ is false} \end{cases}$$

$$B_i : u_i = u_i + 1$$

$$B_i : u_i = u_i - 1$$

The bookkeeping right for this round of transaction information blocks can be divided into three cases: (1) If the Hash operation for this round of transaction information blocks has not ended, when B B first appears and u (V $_1$, …, V , …, V) = n, then B is the best block for this round of Hash operation, i.e., the block that can pass verification by all nodes in the blockchain network. (2) If the Hash operation for this round of transaction information blocks has ended, when B , B B, and n > u (V $_1$, …, V , …, V) > u (V $_1$, …, V , …, V), then B is the best block for this round of Hash operation. (3) If the Hash operation for this round of transaction information blocks has ended, when B , B , B B, and n > u (V $_1$, …, V , …, V) = u (V $_1$, …, V , …, V) > u (V $_1$, …, V , …, V), then the block that first reaches the current value of u among B and B is selected as the best block for this round of Hash operation.

4.2.2 Consensus Mechanism Execution for Block Construction and Linking Any node in the digital ancient book management blockchain network that wants to produce a new transaction information block and write it to the blockchain requires three elements: block, difficulty value, and proof-of-work function. During new block construction, bookkeeping rights for the next block are obtained by synchronizing the latest blockchain. Unconfirmed transactions in the network during this period are collected as T = {T$_1$, T$_2$, …, T }. The difficulty value of digital ancient book transaction blocks determines the amount of Hash operations needed to generate new blocks. The difficulty value H_d in the new block header sets the next mining target Target. During transaction execution and verification, transactions undergo SHA256(SHA256()) calculation to compute the transaction information Hash value, recorded in the block header's Merkle root. Additionally, important information contained in digital ancient book blocks is calculated and collected to form a transaction information data list recorded in the block body's TransactionInfo. Digital ancient book block information is shown in Figure 2 [Figure 2: see original paper].

After constructing transaction information block B without the random number Nonce, the consensus algorithm POW is executed to build digital ancient book block B. According to difficulty value H_d in block B 's header, this block's difficulty coefficient is defined as Target, where Target = 2^{256} / H_d, generating a corresponding random number Nonce. Through POW function operation, the FinalHash value is obtained. If FinalHash < Target, the digital ancient book management block B is successfully constructed. This block construction process is formally represented by Equation (6):

$$F \leq 2^{256}/H_d \| F = PoW(H_i, Tx, nonce, datatorrent)$$

Where F represents the qualified FinalHash value, POW represents the proof-of-work consensus algorithm function, H is block B 's header, Tx is the Hash value of confirmed transactions in digital ancient book management block B, Nonce is a random number, and Datatorrent is the dataset generated from this block's pseudo-random seed.

The specific block construction process is shown in Figure 3 [Figure 3: see original paper]. After constructing a new digital ancient book block, it is broadcast across the network. Other nodes verify the block, and if valid, synchronize the new block to the digital ancient book management blockchain. The blockchain state transition is formally represented by Equation (7):

$$C_{t+1} = S(... \eta(\eta(C_t, T_0), T_1) ...)$$

Where block B generated at time t+1 has n confirmed transactions (T_1, T_2, ..., T); S is the digital ancient book management blockchain state transition function for block B linking; is the blockchain state transition function for single transaction generation. After passing network-wide verification and linking, the transaction is confirmed and permanently recorded in the digital ancient book management blockchain, never to be altered.

The transaction information storage algorithm is shown in Algorithm 1:

Algorithm 1: Transaction Information Data Block Storage Algorithm
Input: AsetNoofNodes, newblock B, blockchain C
Input: Tend, the end of create block stop
1) procedure store(N, B, C, Tend)
2) P = {T_1, T_2, ..., T }
3) create Blockhead H()
4) if time < T_{end} then
5) foreach nonce do
6) if nonce <= 2^{256}/Hd && mixhash = H(mixhash)
7) if (nonce, mixhash) = PoW() then
8) foreach n N do
9) verify(B)
10) if B = true then
11) C = addBlock(C, B)
12) foreach n N do
13) distributeBlockchain(C^', n)
14) else updateTime()
15) end procedure

4.2.3 Dynamic Transaction Information Block Storage Architecture for Digital Ancient Books The storage architecture of the digital ancient book management blockchain network adopts a multi-level access control mode. The entire process from node-initiated transactions, creation of genesis blocks,

construction of new blocks through transaction processing, to block on-chain verification constitutes the complete flow from copyright registration to query and then to requests from other nodes to use digital ancient books, fulfilling the circulation process of digital ancient books. This entire process is completed on the blockchain, representing a dynamic transaction data on-chain storage process. Due to blockchain's immutability characteristic, inter-block information data is added dynamically. Dynamic data corresponds to the transfer of digital ancient book copyrights and usage rights. The communication interaction between adjacent blocks is shown in Figure 4 [Figure 4: see original paper].

The foundation of blockchain is cryptography, with encryption and decryption implemented through keys. The digital ancient book management blockchain network generates key pairs (PK , SK) for each node on the chain. The key pairs enable information data communication between adjacent blocks, allowing only adjacent blocks to communicate. For two adjacent blocks B and B $_1$ on the blockchain, assuming block B is the sender and block B $_1$ is the receiver, the dynamic transaction information data generated by block B is encoded as S . To reduce storage space and improve computational speed, adjacent blocks use a secondary hash iteration method for communication, using both the sender's public key PK and information encoding S as variables for the Hash function to obtain a Hash-based Message Authentication Code (HMac) as a characteristic value. The mathematical calculation formula is shown in Equation (8):

$$HMac(PK_i, S_i) = H(PK_i \oplus odata \| H(PK_i \oplus idata \| S_i))$$

Where PK is the sender's public key, S is the information to be sent, H is the hash function, represents XOR, ‖ represents concatenation, and odata and idata represent pre-specified strings.

The sender signs the message authentication code HMac obtained from Equation (8) with its private key. Block B transmits the signed HMac and message body to block B $_1$. Each node's account on the blockchain is its public key, and node accounts use their private keys to sign verified information. The new transaction creation and block construction process has been described previously. When a node broadcasts the transaction across the network through the P2P network, each node block verifies the transaction and selects the block achieving consensus in each round according to the consensus mechanism proposed in Section 4.2.2, then broadcasts it again through the P2P network. Finally, the transaction information block is linked to the blockchain through Hash methods while synchronizing the chain to all blockchain nodes for updates, completing dynamic transaction information storage and distributed accounting of transaction data.

For example, in the digital ancient book management blockchain, a newly generated block B can be represented by a quadruple array (s, t, l, c), where s is the block sequence number, t is the transaction information type for different blocks in the blockchain, l is the length of this transaction information in the

new block, and c is the dynamic transaction information data encoding format established according to blockchain standards. Assuming a digital ancient book management blockchain node initiates a transaction generating a genesis block and the new block is non-empty, the block validity verification algorithm is shown in Algorithm 2:

Algorithm 2: New Block Validity Verification Algorithm
Input: newblock B, blockchain C
1) procedure validate_{block}(B, C)
2) B ← (x, c)
3) if B (C) then
4) (s, t, l, c) ←
5) HMac(S , PK)
6) HMac ← M(S , PK)
7) if validblock(s, t, l, c) (HMac == HMac)
8) then
9) blockchain C ← l ‖ h(tail(C))
10) else
11) B = false
12) endif
13) endif
14) return(B)
15) end procedure

4.3 Smart Contract Protocol for Digital Ancient Book Management Model

The digital ancient book management model based on blockchain automatically executes digital ancient book copyright registration and usage transactions through establishing smart contracts.

4.3.1 Digital Ancient Book Copyright Registration Smart Contract

Ancient books are works left by ancestors whose original authors have been deceased for hundreds or thousands of years; their copyrights are not exclusive to any individual. However, the inheritance and protection of ancient books rely on collecting units, individuals, and organizations, scholars, and publishers who organize and publish them, all of whom have corresponding rights and interests. The resulting full-text image data, text-image comparison data, and text data of digital ancient books enjoy corresponding copyrights.

The copyright registration smart contract (CopyrightRegistrationContract, CRC) established by the digital ancient book management blockchain model follows the principle of "whoever creates first, applies first, owns the copyright." When user nodes install the client for registration, they simultaneously deploy a CRC on the blockchain, constructing the contract owner through an initialization registration function. When a node calls the CRC, the contract first detects the transaction initiator's information. If the contract caller is

not the contract owner, the ancient book copyright cannot be written into the blockchain. If digital ancient book copyright registration is successful, the smart contract CRC returns a Hash value extracted from the data's characteristic value as the identifier for this digital ancient book copyright [20]. The smart contract CRC algorithm is shown in Algorithm 3:

Algorithm 3: Digital Ancient Book Copyright Registration Contract
Input: newblock B, blockchain C, Tx), transaction object
Output: if error, registration failure else return ID
1) procedure register(Tx)
2) if msg.sender = owner then
3) Tx = newTransaction();
4) Tx.name = Tx.name;
5) Tx.time = now;
6) Tx.content = Tx.content;
7) hash = createID()
8) blockchain C ← l
9) return hash

4.3.2 Digital Ancient Book Copyright Authorization Smart Contract

The digital ancient book management blockchain enables flexible management of ancient book copyrights by owners. According to the Copyright License Contract (CLC), when a user sends a usage authorization request to the copyright owner, the copyright owner calls the ancient book copyright usage authorization protocol in the smart contract CLC upon receiving the request, triggering this transaction. If the copyright owner agrees to the transaction, the smart contract CLC calls the transfer function to execute the authorization transaction. If the copyright owner does not agree to the user using their data, the transaction is stopped from the transaction queue. The smart contract CLC algorithm is shown in Algorithm 4:

Algorithm 4: Digital Ancient Book Copyright Usage Authorization Contract
Input: Tx, transaction object
1) procedure receiveTx(tx)
2) if msg.sender = owner then
3) if tx.operation == true then
4) transaction(tx.to, tx.from)
5) digitalWork = getCIC(tx, hash);
6) removeFrom(owner, digitalWork);
7) linkTo(tx.requester, digitalWork);
8) endif
9) stop(tx)
10) endif
11) end procedure

5. Distributed Storage and Incentive Mechanisms for Digital Ancient Books

While deploying blockchain smart contract protocols can solve digital ancient book management problems from copyright protection and circulation perspectives, blockchain's distributed storage and consensus mechanisms can address issues of digital ancient book storage and the lack of incentives in traditional ancient book databases.

5.1 Distributed Storage of Digital Ancient Books

Currently, digital ancient book data uses centralized database storage, requiring massive storage space as data volume increases. Distributing this data from central databases using HTTP protocols leads to high dependence on Internet backbone networks when content becomes overly centralized, reducing efficiency or causing routing table control issues, creating data security problems.

As known from Section 4.2, blocks on the blockchain only record transaction information data, smart contracts, some summary notes, and files smaller than 256K, determined by the defined block structure to avoid storage explosion from storing large data directly on the blockchain. Blockchain technology addresses large data storage through IPFS (The InterPlanetary File System), a P2P distributed data distribution protocol that connects all computing devices with the same file management mode. Therefore, constructing a digital ancient book management blockchain model fundamentally changes the storage, search, and download methods for digital ancient books [21].

IPFS is universal for storing various files without size limitations. For ancient book data such as full images and text-image comparisons, individual data files are large. The IPFS system automatically splits large data files into multiple small data blocks and distributes them for storage across numerous node computers. To ensure data security and reliability, the blockchain IPFS distributed storage protocol replicates each digital ancient book dataset more than three times for dispersed storage. Blockchain user nodes can be divided into two types: light nodes, which are ordinary consumer users capable of constructing blocks, completing smart contracts, verifying blocks, and performing digital ancient book blockchain maintenance, copyright registration, querying, and downloading; and full nodes or IPFS nodes, which can perform all light node operations while also contributing storage space for data storage, realizing the sharing concept of "all for one, one for all." The incentive mechanism under the blockchain consensus mechanism also tends to favor full node users.

When digital ancient books are uploaded to IPFS nodes, a new name is generated, which is actually an encrypted Hash value calculated from the data content. Encryption ensures that the Hash value always represents only this data content—modifying even a single bit in the data completely changes the Hash value. Simultaneously, the IPFS system calculates the number of IPFS

nodes across the network and divides the digital ancient books and their copies into multiple data blocks stored across various IPFS nodes.

IPFS fundamentally changes node user search and download methods. When nodes send search requests through smart contracts, IPFS uses a distributed Hash table to find corresponding Hash values, enabling rapid retrieval (requiring only 20 hops in a network with 10,000,000 nodes) of nodes possessing the ancient book data and using Hash verification to ensure data correctness, allowing users to quickly find desired content. Downloads use authorized smart contracts to provide P2P download protocols similar to BitTorrent. After authorization, download users receive a seed file containing calculated addresses of nodes with the ancient book data blocks, enabling fast downloads.

5.2 Incentive Mechanisms for Digital Ancient Book Management Blockchain Network

Consensus mechanisms are the cornerstone of blockchain, equivalent to laws maintaining normal blockchain network operation and proof of participants' contributions and rights acquisition in the blockchain network. The digital ancient book blockchain network establishes a Trustless accounting institution through smart contracts and network-wide node consensus, ensuring consistency across all accounting nodes for every operation such as uploading, downloading, retrieving, and browsing digital ancient books. Participants who contribute more receive more incentives.

Blockchain economic models use tokens to activate internal ecosystems through "consensus mechanisms" and "decentralization," establishing a decentralized self-organizing digital ancient book management system. Tokens are accounting units attached to and used within the blockchain network, forming the basis of incentive mechanisms. Tokens are strictly executed according to blockchain code upon issuance, 不受个人或机构控制.

Assuming the constructed digital ancient book management blockchain network develops well and forms a harmonious blockchain ecosystem for ancient book management, protection, development, and utilization, the total token issuance can be set based on future growth expectations with no additional issuance, establishing a deflationary token system. This study draws on incentive mechanisms from foreign blockchain-based content communities like Steem and domestic blockchain knowledge content communities, exploring corresponding incentive mechanisms for the digital ancient book management blockchain network. For example: (1) Digital ancient book resource construction pool (50% of total tokens) releases 10% of its balance annually to reward copyright users providing digital ancient books, with more work yielding more rewards; (2) Digital ancient book value reward pool (30%) releases 10% of its balance annually to reward copyright owners based on digital ancient book utilization rates; (3) Data storage security maintenance pool (15%) releases 10% of its balance annually to reward IPFS node users providing storage space; (4) Digital ancient book

blockchain network operation and promotion pool (5%) is allocated to standard setters, managers, and central operation promoters, distributed proportionally year by year.

Token value should be multifaceted: On one hand, the value of ancient books themselves is unquestionable as carriers of cultural heritage. The amount of tokens reflects the contribution to ancient book literature protection and can serve as a standard for national reward mechanisms. On the other hand, there is market value—holding tokens is equivalent to owning equity in the digital ancient book management network system, which appreciates as the ancient book industry value increases.

References

[1] Cao Tianxiao. Research on classification and significance of ancient book digitalization under new technology [J]. Library Research and Work, 2017(9): 37-41.
[2] Nie Can. Millennium ancient books tell civilization on paper [N]. Shenzhen Business Daily, 2018-05-24(B5).
[3] Huang Shuiqing, Wang Dongbo. Current status and trends of ancient Chinese information processing research [J]. Library and Information Service, 2017, 61(12): 43-49.
[4] Yu Li, Guan Jiawa. Analysis and development research on current status of ancient book digitalization construction in China [J]. Digital Library Forum, 2017(11): 41-47.
[5] Shen Tu Xiaoming. Analysis of blockchain application models and technical solutions in media industry [J]. Media Review, 2018(4): 27-31.
[6] Jia Yinshi. Research on network copyright transaction issues based on blockchain technology [J]. Science-Technology & Publication, 2018(7): 90-98.
[7] Zheng Yang, Du Rong. Application of blockchain technology in digital knowledge asset management [J]. Publishing Science, 2018(3): 97-104.
[8] Li Yue, Huang Junqin, Wang Ruijin. DCI management model for digital works based on blockchain [J]. Computer Applications, 2017, 37(11): 3281-3287.
[9] Hao Kun, Xin Junchang, Huang Da, et al. Decentralized distributed storage model [J]. Computer Engineering and Applications, 2017, 53(24): 1-7, 22.
[10] Wu Zhenquan, Liang Yuhui, Kang Jiawen, et al. Smart grid data security storage and sharing system based on consortium blockchain [J]. Computer Applications, 2017, 37(10): 2742-2747.
[11] Wang Jiye, Gao Lingchao, Dong Aiqiang, et al. Research on blockchain-based data security sharing network system [J]. Journal of Computer Research and Development, 2017, 54(4): 742-749.
[12] GRINBERG R. Bitcoin: an innovative alternative digital currency [EB/OL]. [2017-03-01]. https://www.researchgate.net/publication/228199328_{{{Bitcoin}}{{An}}}{{{Innova
[13] Meng Qixun, Wu Yijie. Technical approach to network copyright transaction from blockchain perspective [J]. Publishing Science, 2017, 25(6): 25-31.
[14] Yuan Yong, Zhou Tao, Zhou Aoying, et al. Blockchain technology: from

data intelligence to knowledge automation [J]. Acta Automatica Sinica, 2017, 43(9): 1485-1490.
[15] SZABO N. Formalizing and securing relationships on public networks [EB/OL]. [2016-11-20]. http://journals.uic.edu/ojS/index.php/fm/article/view/548/469.
[16] Wang Shuaiyu, Li Chen. A big data rights confirmation method and system based on blockchain technology: China, CN106815728A [P]. 2017-06-09. http://nvsM.cnki.net/kns/detail/detail.aspx?QueryID=5&CurRec=1&dbcode=SCPD&dbname=SCPD2017&
[17] ZHAO J L, FAN S, YAN J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue [J]. Financial innovation, 2016, 2(28): 2-7.
[18] Qiao Rui, Dong Shi, Wei Qiang, et al. Research on dynamic data storage security mechanism based on blockchain technology [J]. Computer Science, 2018, 45(2): 57-62.
[19] GRAMOLI V. From blockchain consensus back to Byzantine consensus [J]. Future generation computer systems, 2017, 9(23): 1-5.
[20] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts [C]//Proceedings of the 2016 IEEE symposium on security and privacy. Piscataway: IEEE, 2016: 839-858.
[21] Yin Long, Wang Hongwei. Research on distributed data sharing system based on IPFS [J]. Internet of Things Technologies, 2016, 6(6): 60-62.

Author Contributions

Gao Li: Proposed research ideas and wrote the paper;
Wang Chunyan: Provided revision suggestions;
Gao Xindan: Guided research ideas and designed paper framework.

English Abstract

[Purpose/significance] From the perspective of blockchain technology, this paper proposes a solution to the problems of the protection and use of ancient books, and proposes a solution to the digital block management system model for ancient books, and implements an ancient management innovation model. **[Method/process]** First of all, a blockchain decentralized P2P architecture is designed from the aspects of construction and implementation. The entire network consensus link block is realized by the node initiating the transaction, the construction block, and the validity verification. Secondly, an information storage mechanism and smart contract protocol algorithm is established to automatically implement the guarantee model in an efficient and transparent manner, and the digitized ancient books copyright registration and circulation utilization information cannot be tampered with and traceable. Finally, the consensus mechanism and the distributed storage mechanism of the IPFS protocol system solves the scientific data storage and security, and at the same time establishes a reasonable incentive mechanism to achieve effective management of scientific data. **[Result/conclusion]** Through the establishment of

this model, the traditional centralized management system of ancient books database is abolished, and the entire process of protection and utilization of ancient books can be traced and cannot be tampered with the form of block + chain to achieve the technological innovation of protection of ancient books.

Keywords: blockchain, digital classics, smart contract, IPFS

Note: Figure translations are in progress. See original paper for figures.