ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

A model for sinking digital resources in rural preschool education: blockchain-enabled resource sharing and copyright protection

Guiyun Li[1] *and Chenhui Ru*[1,*]

[1] Hebei Institute of International Business and Economic, Qinhuangdao, Hebei, 000315, China

SUMMARY: *At a time when urban and rural educational resources are dependent on each other, promoting the sinking of digital educational resources to the countryside is an important path to bridge the education gap, and the study proposes a blockchain-enabled solution to this end. First, we build a "federation chain + IPFS" architecture to jointly maintain metadata such as resource ownership and access policies. Resource files are stored in an efficient distributed file system (IPFS). Next, an attribute-based access control (ABAC) model is constructed. The system realizes permission determination by comprehensively evaluating their identity attributes, resource labels and environments. Finally design a fine-grained secure sharing algorithm that incorporates attribute-based encryption. The access policy is transformed into an encryption policy tree and integrated into the resource ciphertext. Only users with exactly matching attributes can decrypt the ciphertext, and key update and policy adjustment are supported. The study compares it with two methods GT-DEMATEL and Asmuth-Bloom in multiple dimensions. This paper's method is able to handle over 900 concurrent resource requests per second in resource sharing efficiency, and the system transaction latency is extremely low, with a transaction taking only 93ms to be confirmed in a network of 36 nodes even in the presence of Byzantine nodes. At the same time, the internal communication cost of the system is extremely low. In a network of 36 nodes, the communication overhead for reaching consensus is only 187, less than 1/6 of the comparison scheme.*

KEYWORDS: *rural preschool education; digital resources; blockchain; resource sharing; IPFS; ABAC*

1 Introduction

The rational allocation of preschool education teaching resources in rural areas determines the quality of rural preschool education, directly affects the development of rural early childhood education, and even relates to the harmonious development of the entire urban and rural society [1, 2]. However, due to the imbalance of China's economic and social development, there are obvious differences in the allocation of preschool education resources in urban and rural areas, threatening the healthy development of preschool education in rural areas [3].

With the development of information technology, digital teaching resources provide support for enriching rural preschool education resources and bridging the gap between urban and rural preschool teaching due to their reproducibility, diversity, and efficient dissemination [4, 5]. However, this kind of ponderous and unidirectional resource circulation faces the problem of structural contradiction. Rural preschool education frequently encounters the phenomenon of

*china.ruchenhui@163.com
https://doi.org/10.65102/is2026332
Published: 30 April, 2026

resource silos in cross-regional collaboration, data barriers between different platforms lead to the inability to efficiently share high-quality content, and a large number of original resources are idle or duplicated development [6]. What's more, the lack of copyright protection mechanism makes the piracy rate of resources remain high, and the rights and interests of originators are seriously infringed [7]. This situation not only frustrates the enthusiasm of educational content creators, but also directly leads to the uneven quality of education, rural preschool education is difficult to obtain high-quality teaching materials, further aggravating the phenomenon of educational inequity.

Analyzing the root causes of the problem in depth, there are fundamental flaws in the resource confirmation link, and the existing system lacks a tamper-proof ownership record mechanism, so when teachers develop micro-lesson videos or write e-teaching plans, their intellectual property rights are often difficult to get timely and effective legal confirmation [8, 9]. And blockchain technology as is a distributed, tamper-proof database technology, which realizes decentralized, safe, reliable, and tamper-proof data storage and transmission by using cryptographic algorithms, provides technical support for solving the above problems [10-12]. By constructing a blockchain-based digital resource sinking model, the characteristics of blockchain technology can be used to realize the sharing of educational and teaching assets and intellectual achievements while achieving copyright protection and solving the problem of intellectual property disputes [13, 14].

Rural preschool education is the cornerstone of national development, and it is vital to the realization of education for all and the promotion of educational equity. However, due to historical, geographic and economic factors, educational resources in rural areas are relatively insufficient, which brings a series of challenges to the development of rural preschool education. Literature [15] examined the imbalance in the allocation of resources for rural preschool education, pointed out that differences in regional economic development are the main reason for the unequal distribution of resources, and emphasized the key responsibility of the government in promoting the equitable distribution of resources and establishing a per capita financial subsidy system. Literature [16] studied the efficiency of resource allocation for rural preschool education in China from 2012 to 2020 through a three-stage data envelopment model, analyzed the impact of external factors such as the level of urbanization, pointed out that the overall efficiency has improved but there are regional differences, and put forward suggestions to optimize human, financial and material resources. Literature [17] predicted the demand for urban and rural preschool education through the Leslie matrix, analyzed the resource gap, and pointed out that in order to cope with the demographic changes, it is necessary to dynamically adjust the resource allocation, through scientific planning and construction, supplementing teachers and guaranteeing the financial investment, in order to solve the problem of rural preschool education resource allocation. Literature [18] constructed a three-party evolutionary game model to analyze the resource allocation problem of rural preschool education in China, and examined the key roles of government subsidies, regulation and supervision in enhancing the quality and fairness of education, and emphasized the significance of optimizing the incentive and punishment mechanism and adjusting the policies to promote the effective use of resources and guarantee the sustainable development of rural preschool education. Literature [19] analyzed the spatial and temporal differences in the allocation of resources for rural preschool education in China from 2003 to 2019 based on the data of the Three-Year Action Plan for Preschool Education, pointing out that the allocation of resources has improved in general, but is still unbalanced and on the low side, examining the impact of differences in financial and human resources between regions, and putting forward relevant recommendations to reduce the regional differences in the allocation of resources for preschool education. The impact of inter-regional differences in financial and human resources is examined, and relevant

suggestions for reducing regional differences in preschool education resource allocation are put forward. Literature [20] studied the problem of rural preschool education resource allocation, and by analyzing the gap between urban and rural productivity, teacher quality and family background, it pointed out that these factors are the important reasons leading to the uneven development of urban and rural preschool education, and emphasized the key role of government scientific inputs and upgrading the level of rural teachers' team in narrowing the gap. Literature [21] analyzes the three major structural dilemmas facing the allocation of physical education resources in rural preschool education, pointing out the problems of urban-rural resource imbalance, lack of professional teachers and insufficient protection, and emphasizes the importance of building a sustainable and localized resource supply model to promote educational equity by proposing optimization paths such as hierarchical protection and three-tier training system. Literature [22] takes Luochuan County as an example and analyzes the problem of rural preschool education resource allocation, pointing out that there is an oversupply of services in rural areas and an unmet demand in urban areas, and at the same time emphasizing the phenomena of reduced subsidies from local governments and inefficiency of urban and rural services.

The application of digital teaching resources brings opportunities for the development of education, while blockchain technology guarantees the security of these digital teaching resources and promotes resource sharing. Literature [23] analyzed the application of blockchain in the copyright protection of digital teaching resources by proposing the BC-DERCP mechanism, examined its advantages in secure storage and collaborative verification, pointed out that the technology can effectively protect copyright and privacy, and emphasized that it can help stimulate the enthusiasm of resource creation. Literature [24] proposes the EduCopyRight-Chain framework based on Ethernet blockchain and NFT, analyzes its application in protecting the copyright of digital teaching resources, examines its performance advantages through simulation experiments, and emphasizes the significance of this technology in solving the problem of resource authentication and piracy. Literature [25] investigated the application of blockchain technology in online education platforms, analyzed its potential in solving the problems of digital copyright infringement, certificate security and resource openness by proposing a network architecture combining public and private chains and a smart contract scheme, and emphasized its feasibility as a multimedia data protection scheme. Literature [26] examines the application of blockchain technology in protecting the copyright of digital teaching resources, analyzes its importance in maintaining the quality of content and the rights of educators by constructing a conceptual model, and emphasizes its potential in promoting trust and security in digital education. Literature [27] analyzed the application of blockchain technology in digital teaching resource sharing, pointed out its advantages in protecting resource copyrights, enhancing transparency and simplifying transactions through questionnaires, and emphasized its important role in building a trustworthy education ecology and promoting resource sharing and integration. Literature [28] studied the application of blockchain in digital teaching resources authentication, analyzed how its decentralization and tamper-resistant features protect the rights and interests of resource owners, and emphasized the important role of the system in ensuring the safe circulation of resources. Literature [29] explores the application of blockchain technology in digital teaching resources and management in education, analyzes its potential in improving administrative efficiency, securing secure data sharing and supporting micro-authentication, while pointing out challenges such as data privacy, standardization and implementation costs, and emphasizes its importance in promoting innovation and change in the education system. Literature [30] proposes a blockchain-based open service platform solution for digital educational resources in universities, and through the use of distributed ledgers and smart contracts, analyzes its

application in guaranteeing resource security and simplifying copyright authentication, and emphasizes the significance of this technology in solving the problems of openness and quality.

The research focuses on blockchain empowerment as the underlying trust infrastructure, which is deeply integrated with access control policies, encryption algorithms, distributed storage, and other technologies. The study designs a distributed network involving multiple preschools, resource centers, and management nodes. Resource uploading, authorization and other operations are automatically executed through smart contracts, and consistency is ensured by a consensus mechanism. The Interplanetary File System (IPFS) is also introduced to store the resource files themselves in a distributed manner, and only key information such as the hash fingerprints and access policies of the resources are uplinked. An attribute-based access control model is constructed on this basis. Label users, resources and access environments with attributes, and resource owners can define policies accordingly. When a user initiates a request, access is allowed only if the attributes match. Further, in this regard, design a fine-grained access control security sharing algorithm for digital educational resources. From system initialization and generation of user keys, to transforming the access policy into a policy tree and embedding the ciphertext, and then introducing third-party pre-decryption to alleviate the computational pressure on the user's end and achieve secure decryption. The final algorithm is landed through the resource management function on mainstream blockchain platforms. Based on the Hyperledger Fabric platform, the whole process of nodes such as administrators, subject teachers, students, etc., from endorsement, sorting to bookkeeping is realized by configuring nodes, creating subject organizations, establishing transaction channels and deploying smart contracts.

2 Blockchain-enabled educational resource sharing: model construction, access control and system implementation

2.1 Blockchain-based cross-domain data security sharing model

2.1.1 Distributed multi-domain network design

The cross-domain access control model for preschool teaching resources proposed in the study is based on a federated chain design [31], which prevents malicious nodes from entering the network to some extent. The model organization consists of multiple security domains and regulatory agencies, all of which participate directly in the blockchain network as nodes and jointly manage the distributed ledger. Each institution or enterprise acts as a participating node in data sharing executing transactions and invoking smart contracts for data authorization and interaction. The roles in the model include:

(1) Certification Authority (CA): the CA is responsible for issuing certificates to users with identities and attribute sets authenticated by the administrator, providing users with certificates to verify their identities and encrypted private keys to prove that the users are legitimate;

(2) Administrator (Admin): the Admin belongs to the CA and is responsible for verifying the consistency between the actual identity in the local database and the attribute set provided by the user to ensure the correctness of the user information;

(3) Data Owner (DO): a DO is an entity that shares data and sets policies, which are defined by valid attribute sets. They can invoke smart contracts to upload resources to IPFS, encrypt hashes by invoking smart contracts, and create appropriate access control policies for shared resources;

(4) Data Requestor (DR): a DR is an entity that requests data by invoking a smart contract. It also has the set of attributes that are authenticated by the access control policy, and only users

who meet the authentication are authorized to access the data;

(5) Interplanetary File System (IPFS): an IPFS cluster provides distributed storage for shared data, connected to the blockchain network to reduce the pressure on blockchain storage and improve the efficiency of resource sharing.

Each transaction in the network is supervised by regulatory nodes, which provide auditing capabilities and warning services for abnormal events. Users of each security domain must complete registration in the blockchain network to obtain a CA certificate. Only when they have a valid certificate can they join the network through authentication at the application layer interface and invoke contracts to share resources or request data from other domains. In this model, most of the system functions are performed automatically by smart contracts and consistency between nodes is guaranteed by the Raft consensus algorithm.

2.1.2 Attribute-based access control model construction

This model assigns the roles of resource owner (DO) and resource requester (DR) to each user for different scenarios based on the ABAC model [32]. In the initial phase of the system, each security domain negotiates to define a unified set of user attributes $Attr(u)=UA_1,UA_2,\cdots,UA_k$, a set of resource attributes $Attr(r)=RA_1,RA_2,\cdots,RA_k$ and the set of environmental attributes $Attr(e)=EA_1,EA_2,\cdots,EA_k$. These attribute sets represent each entity, e.g., users and resources, and are used to validate the requester's privileges, but the attribute sets will not include the user's private information.

This model is a set of resource-defined policies $P=p_1,p_2,\cdots,p_n$, restricting the range of the user attribute $Attr(u)$ and the environment attribute $Attr(e)$. p_i is one of the sub-policies of P and is defined as $p_i=\{UP_1,\cdots,UP_s,EP_1,\cdots,EP_t\}$, where $UP_1,\cdots,UP_s$ and $EP_1,\cdots,EP_t$ are respectively define the policies corresponding to user attributes and resource attributes. The name of each policy attribute is consistent with the user and environment attribute names to facilitate the validation of the attribute values. When UA_i and EA_i are the same as UP_j and EP_j attribute names, respectively, the corresponding attribute values are verified. If the user attribute and the environment attribute satisfy: $UA_i \in UP_j\ (0<j<s, 0<i<n, s\le n)$, and $EA_i \in EP_j\ (0<j<t, 0<i<m, t\le m)$, then the user is then verified as having privileges and access to it is allowed. For example: $UP_j=\{company:\{"DomainA","DomainB"\}\}$, $UA_i=\{company:\{"DomainA"\}\}$

When the attribute names of UP_j and UA_i are the same and $UA_i \in UP_j$, it also means that the user attribute UA_i satisfies the attribute UP_j of the policy. The policy set P determines whether the data requestor (DR) can access the resource r under certain environmental conditions e when satisfied:

$$\begin{aligned} &checkAccess\left(Attr(DR), Attr(e), p_i\right) \\ &=\left(Attr(DR)\in p_i\right)\wedge\left(Attr(e)\in p_i\right) \end{aligned} \tag{1}$$

and each sub-policy is satisfied, the permission validation passes:

$$\begin{pmatrix} checkAccess\left(Attr(DR), Attr(e), p_1\right) \vee \cdots \\ \vee checkAccess\left(Attr(DR), Attr(e), p_n\right) \end{pmatrix} = true \tag{2}$$

The access control model architecture is shown in Fig. 1, in which the environment attributes are automatically set by the system, and these attributes record the environment in which the requester is located, such as the time when the request is initiated, the IP address, and the device. User attributes are managed by the admin user of each domain to avoid tampering of user attribute information. Resource attributes and policy attributes are collections managed by the resource owner. When the blockchain system receives a data request initiated by a user, it will call the smart contract to obtain the user information $Attr(u)$ of the DR and the environment information $Attr(e)$ of the requester, and validate the requester's privileges according to the policy p_i to which the resource belongs. If the requestor's attributes satisfy the corresponding access control policy, he will receive the re-encrypted ciphertext of the corresponding resource; on the contrary, the blockchain will reject the request. The blockchain ledger records each resource request, so the flow of all data is traceable.

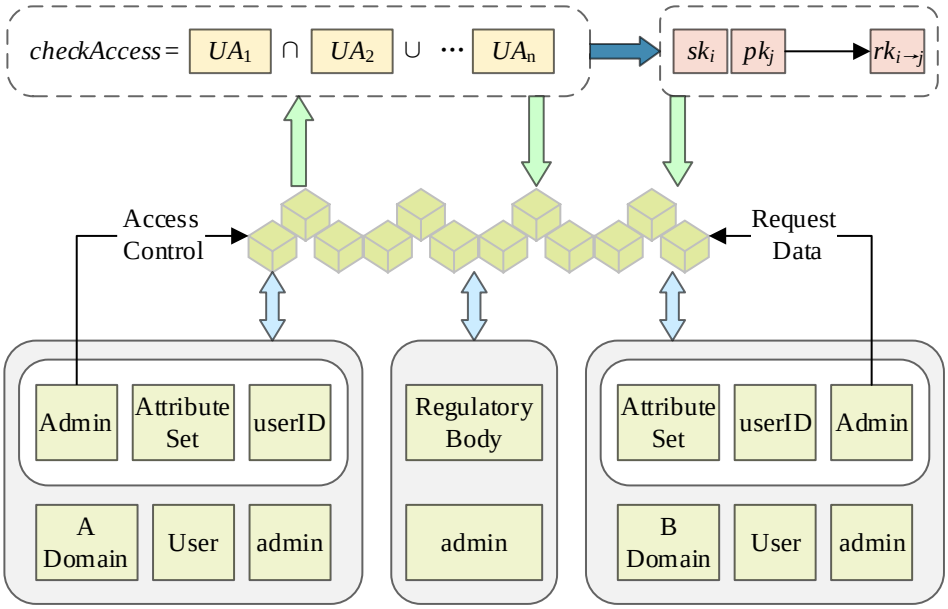

Figure 1: Access control model

2.2 Specific Algorithms for Secure Sharing of Digital Educational Resources with Fine-Grained Access Controls

Specific encryption and key management algorithms are also required to land the above attribute-based access control model as an executable secure sharing mechanism. For this reason, this section proposes a set of fine-grained access control secure sharing algorithms, from system initialization, key generation, policy embedding to data decryption and updating, to guarantee the confidentiality of educational resources in the sharing process.

(1) System Initialization

The input parameter of System Set Up algorithm is λ. Choose two multiplicative cyclic groups G_1 and G_T generated by the element g of order prime p, the algebraic operation from $G_1 \times G_1$ to G_T is defined as $e: G_1 \times G_1 \to G_T$, and call this mapping a bilinear mapping.

Two random numbers β and α are chosen, $\alpha \in Z_p$, $\beta \in Z_p$, followed by exponential operations to generate h and f, the system public key PK is generated according to Equation (3) and the system master key MSK is generated according to Equation (4). Using the unified hash algorithm $H:\{0,1\}^* \to G_1$, the hash algorithm will be subsequently used to map the virtual attributes to the elements on G_1, which is easier and faster than customizing the correspondence table between user attributes and elements on G_1.

$$PK = \left(G_1, g, h = g^{\beta}, f = g^{\frac{1}{\beta}}, e(g,g)^{\alpha} \right) \tag{3}$$

$$MSK = \left(\beta, g^{\alpha} \right) \tag{4}$$

In addition to generating PK and MSK, public keys, private keys, certificates, and global attribute mapping tables for peer nodes in the Hyperledger Fabric network need to be generated. The global attribute mapping table is used for the subsequent generation of attribute keys and access policy tree process to ensure that the user privacy is not exposed to the third party, avoiding the distributed ledger to directly store the actual user information.

(2) Generation of user key and third-party pre-decryption key

The Attr Prv Key Gen key generation algorithm will receive a set of user attributes Attrs as input [33], and then transform the actual attributes into a virtual attribute set Vir_Attrs according to the global attribute mapping table. Then select a random $r \in Z_p$, traverse the virtual attribute set Vir_Attrs, and for each virtual attribute vir_ attr selects the random number $r_j \in Z_p$. Run the algorithm to obtain the user attribute key component, which is shown in Equation (5). Select the random number $TSK \in Z_p$ to generate the third party pre-decryption key as shown in Equation (6).

$$SK = \left(D = g^{\frac{\alpha + r}{\beta}}, TSK = z \right) \tag{5}$$

$$MidSK = \begin{pmatrix} \forall\, vir\_attrs[j] \in Vir\_Attrs: \\ MD_j = g^r \cdot H(vir\_attrs[j])^{r_j TSK}, MD'_j = g^{r_j TSK} \end{pmatrix} \tag{6}$$

(3) Access Policy Embedding Ciphertext Data

Encrypt algorithm implementation requires three steps:

(1) Firstly, according to the access control policy uploaded by the creator of educational resources is transformed into the form of a specific access control tree. The user access control policy representation is in the form of a string and the content is information containing attributes and thresholds. Assuming that the global attribute set is Attrs=(Attr1, Attr2, Attr3, Attr4, Attr5, Attr6, Attr7, Attr8, Attr9), the attributes in the policy need to be selected from the global attribute set, and in order to better understand it using the mid-range expression way to give an example of the user access control policy string, str= “((Attr1orAttr2orAttr3))or(Attr4andAttr5and(Attr6orAttr7))”, which is transformed into the corresponding access policy tree structure shown in Figure 2. Instead of the traditional and or

gate tree structure expression, a threshold expression is used, $(n:k)$, when $n=k$ represents the "and" gate, when $n>k$ represents the "or" gate, and k is called the node threshold. The leaf node attribute values inside the access structure tree are converted into virtual attribute values to ensure that the real user attributes are not disclosed. The access structure tree with virtual attributes is named Policy_Tree, and Policy_Tree participates in the encryption algorithm in the second step.

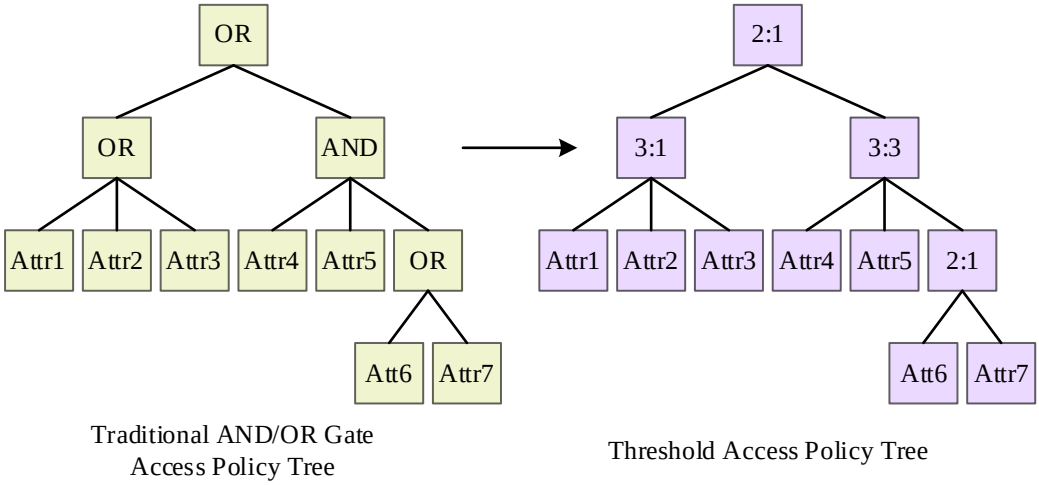

Figure 2: Access policy tree

2) Calculate the secret value slice of leaf nodes. The algorithm traverses each node starting from the root node root of Policy_Tree. The polynomial generation method for each node is as follows, the highest ordinal term of the polynomial for each node is the node threshold $k-1$, and the rest of the polynomial coefficients except the constant term are chosen randomly. If x is the root node, the constant term is randomly chosen. If x is not the root node, the constant term is the value of the parent polynomial at this node index, i.e., $p_x(0)=p_{parent}\left(index_x\right)$. Execute the above method until the leaf node y completes the generation of polynomials, and finally obtain the secret value slice data $p_y(0)$ for the generation of the ciphertext component. Firstly, a secret value $s\in Z_p$ is randomly selected for node root, then the polynomial $p_{\text{root}}(x)$ is constructed, and the number of the highest subterm of $p_{root}(x)$ is one less than the root node threshold value k, i.e., the highest subterm of $p_{root}(x)$ is 0, and s is used as $p_{root}(x)$ as a constant term, which finally yields $p_{root}(x)=s$. Assign index values to the child nodes in increasing order, $(3:1)$ node has index $index_{3:1}=1$, and $(3:3)$ node has index $index_{3:3}=2$. The generated node $(3:3)$ corresponds to the polynomial $p_{3:3}(x)$ with the highest number of subterms 1 less than its own threshold, i.e., the highest subterm of $p_{3:3}(x)$ is 2. Then the polynomial coefficients a_2 and b_2 are randomly chosen for the 2nd and 1st terms, and the constant term of $p_{3:3}(x)$ is $p_{root}\left(index_{3:3}\right)=s$, and finally $p_{3:3}(x)=a_2x^2+b_2x+s$.

3) Generate ciphertext data. Generate the ciphertext component according to Eq. (7), Y is the set of leaf nodes in Policy_Tree, m is the set of data related to the encrypted digital educational resources, s is the secret value of the root node, and $p_y(0)$ represents the value

of the polynomial of the leaf node at $x=0$, i.e., the secret slice value.

$$\begin{aligned} Ct = \Big(& Policy\_Tree, C' = me(g,g)^{\alpha s}, C = g^{\beta s}, \\ & \forall y \in Y : C_y = g^{p_y(0)} C'_y = H\left(vir\_attr(y)\right)^{p_y(0)} \Big) \end{aligned} \tag{7}$$

All AA nodes execute the above encryption algorithm and if the consensus is successful, Ct is deposited into the state of the world with Course_Id as the primary key, and this transaction is permanently recorded on the blockchain ledger and cannot be changed.

(4) Third party pre-decryption algorithm

The third party receives the pre-decryption request from the application platform and performs the following two-step pre-decryption PreEecrypt operation based on the ciphertext data in the request body, the access policy, and the set of virtual attributes of the requesting visitor.

1) Traversing the access policy tree. For the leaf node, find out the attributes that are consistent with the attributes of this node in the attribute set of the data visitor, use MD_j in the conversion key and C_y in the ciphertext, and do the bilinear mapping between MD'_j in the conversion key and C'_y in the ciphertext, respectively, and decode the leaf node's mixed-sliced secret value according to Eq. (8), and label This leaf node satisfies the condition.

$$\begin{aligned} & DecryptNode\left(Ct, MidSK, y\right) = \frac{e\left(MD_j, C_y\right)}{e\left(MD'_j, C'_y\right)} \\ & = \frac{e\left(g^{TSK \cdot r} \cdot H(vir\_attrs[j])^{r_j}, g^{p_y(0)}\right)}{e\left(g^{TSK \cdot r_j}, H(vir\_attrs[j])^{p_y(0)}\right)} \\ & = e(g,g)^{TSK \cdot r \cdot p_y(0)} \end{aligned} \tag{8}$$

2) For non-leaf nodes, when the number of leaf nodes that satisfy the condition is equal to the threshold of the parent node, the Lagrange interpolation algorithm is done on the number of children to derive the polynomial of the parent node. Let the threshold value of the parent node z be n, and there are n child nodes labeled to satisfy the condition, noting that these n child nodes are y_i, $i \in [1,n]$ and i is an integer. The hybrid partition secret value of non-leaf node z can be deduced by bringing Eq. (9), Eq. (10) and Eq. (11) into Eq. (12).

$$F_{y_i} = e(g,g)^{TSK \cdot r \cdot p_{y_i}(0)} = e(g,g)^{TSK \cdot r \cdot p_z(\mathrm{index}_{y_i})} \tag{9}$$

$$l_i(0) = \prod_{j=1, j \neq i}^{n} \frac{0 - \mathrm{index}_{y_j}}{\mathrm{index}_{y_i} - \mathrm{index}_{y_j}} \tag{10}$$

$$f_i = p_z(\mathrm{index}_{y_i}) \tag{11}$$

$$\begin{aligned} F_z &= \prod_{i=1}^{n} F_{y_i}^{l_i(0)} = \prod_{i=1}^{n} \left(e(g,g)^{TSK \cdot r \cdot p_z\left(index_{y_i}\right)} \right)^{l_i(0)} \\ &= \prod_{i=1}^{n} e(g,g)^{TSK \cdot r \cdot p_z(index_{y_i}) \cdot l_i(0)} \\ &= e(g,g)^{TSK \cdot r \cdot \sum_{i=1}^{n} f_i \cdot l_i(0)} = e(g,g)^{TSK \cdot r \cdot p_z(0)} \end{aligned} \tag{12}$$

The mixed secret value can be decrypted in the above manner for all non-leaf nodes up to the root node. The final value of the intermediate secret MidCt of Eq. (13) is derived.

$$MidCt = F_{root} = e(g,g)^{TSK \cdot r \cdot s} \tag{13}$$

(5) Final decryption

Finally the final decryption step is performed by the user according to equation (14)

$$Mt = m = \frac{C' \cdot MidCt^{\frac{1}{TSK}}}{e(C,D)} \tag{14}$$

(6) Data Update

1) Attribute update

The user applies for attribute update to the authorization center, and after the authorization center verifies the user's identity, all authorization centers AA regenerate the attribute key and third-party intermediate key for the user as shown in equations (15) and (16), and the versions of the user's attribute key and the third-party key generated by all authorization centers after consensus are consistent. If the user still uses the previous attribute key for decryption operation, it will not be decrypted.

$$SK_1 = \left(D_1 = g^{\frac{\alpha + r_1}{\beta}}, TSK_1 = z_1 \right) \tag{15}$$

$$\begin{aligned} MidSK_1 = \big(& \forall\, vir\_attrs[j] \in Vir\_Attrs : MD_{j_1} \\ & = g^{r_1} \cdot H\left(vir\_attrs[j]\right)^{r_{j_1} TSK_1}, MD'_{j_1} = g^{r_{j_1} TSK_1} \big) \end{aligned} \tag{16}$$

2) Policy update

After the user submits a new policy, the encryption algorithm is executed again and the new ciphertext is updated to the blockchain distributed ledger as shown in Eq. (17) to update the state-of-the-world database.

$$\begin{aligned} Ct_1 = \big(& Policy\_Tree_1, C'_1 = me(g,g)^{\alpha s_1}, C_1 = g^{\beta s_1}, \forall y \in Y : \\ & C_{y_1} = g^{p_{y_1}(0)}, C'_{y_1} = H\left(vir\_attr(y)\right)^{p_{y_1}(0)} \big) \end{aligned} \tag{17}$$

3) Update data

When the information of the digital educational resources source file is modified, the digital educational resources file needs to be re-symmetrically encrypted and uploaded to IPFS, and the data set related to the educational resources is re-processed through AA encryption, updating

the state-of-the-world database, and recording this transaction on the zone chain.

2.3 Implementation of blockchain resource management functions

After constructing the blockchain network, to specifically implement the resource management function in the digital education resource management system designed earlier, it is necessary to further improve the blockchain architecture, based on the content involved in the detailed design of the main functions earlier, configure several key nodes, organizations and channels required by the system. For the digital educational resource management system, users must include administrators, subject administrators, and ordinary user nodes, and administrators are determined at the beginning of the creation of the system, and there is one and only one within the channel formed by the same transaction transaction. Discipline administrator is the authority determined by the administrator when the user node joins the network based on the responsibilities assumed by the members of the node in a realistic scenario. Ordinary user nodes are the vast majority of users that make up the system, taking on functions such as bookkeeping and endorsement within the system. The relevant operations in the Fabric blockchain platform are shown below.

2.3.1 Node Configuration in IBM

In blockchain nodes depend on smart contracts to exist and store the general ledger, they allow transactions to take place on the organizational network. In IBP, nodes can be added to the console by creating a new node or importing a deployed node. Click on “Nodes” on the left to view or create, and you can see that the page contains three sections: Add Sibling Node, Authentication Center, and Sort Services.

Adding a node to IBM requires a total of seven steps:

(1) Select the node location;

(2) Set the node name;

(3) Add an authentication center to the node and select the organization to which the node belongs;

(4) Add the CA registration mark;

(5) Determine the resource allocation for the node;

(6) Associate the node identity;

(7) Node configuration is successful.

In this system contains administrator, resource user and resource provider. The administrator joins the network as an admin node, and when other nodes apply to join, the admin node classifies the nodes according to their type and then authorizes them. When there is no transaction, each user node exists in the system only as a bookkeeping node, and when a transaction occurs, some of the nodes become endorsement nodes to endorse the transaction. Take uploading language resources as an example, when the user uploads information, the nodes in the network will receive a request from the system, and the node whose resource type belongs to the system is language will act as an endorsement node to endorse the transaction, and after sorting nodes, a new block will be formed in the end.

2.3.2 Creating organizations

Organizations are clusters of user nodes, in this system we can set up different organizations according to the disciplines, and users join in different organizations according to the discipline classification at the time of registration. While creating organization we need to perform this operation from CA node, we need to create MSP definition and import MSP definition.

2.3.3 Creating channels

After creating the organization, we need to join the organizations of the same transaction within the channel. In this study, each user of digital educational resources for rural preschool education maintains the security of the ledger together based on the resource transactions, so the organization members are added into one channel.

2.3.4 Smart Contract Deployment

Before you can get started, you need to install the VS Code extension on the IBM Blockchain Platform. Click Extensions in the sidebar on the left side of the screen, and at the top, search the IBM Blockchain Platform Extensions Marketplace. Click Install, and then click Reload to install the VS smart contract extension code. When creating a new smart contract project, click “Smart Contracts” on the left to view or create.

The following is a concrete example to illustrate how the above parts work. Assuming that there are a total of 55 teachers and students in the course of data analysis and statistics in a rural preschool education program, this group of people are the users of the system, and these users register and log in to the system, and the administrator of the blockchain system will set up different permissions for the users according to their registration information, and the users who have successfully registered become the nodes of the system and join the same organization according to the course attributes. Successfully registered users become nodes of the system and join the same organization according to their course attributes. The teacher of the course is the subject administrator, who supervises and audits the uploading of course resources by students. When a student user uploads resources related to the course, the student nodes and teacher nodes related to this business will join the same channel to call and execute the smart contract for this function. First, the system administrator will audit the identity and authority and the relevance of the resources, and after the audit is passed, the request will enter the blockchain endorsement link. The system will send the request to the teacher and other 54 users according to the pre-defined endorsement strategy, the teacher as the subject administrator will endorse the resources, and other student users will also endorse the resources, and only with the valid signatures of the teacher and the 10 students, the resources will be uploaded to the blockchain system, and then broadcasted to the network, completing the entire resource upload and storage process.

3 Analysis of blockchain-based storage and sharing of educational resources in preschool education

In order to meet the comparative needs of the experiment, GT-DEMATEL-based educational resource data sharing method and Asmuth-Bloom algorithm-based educational resource data sharing method are introduced to share the preschool education resource data of IoT environment with the method of this paper. Taking a regional rural pilot university as an example, the kind of methods are applied for data sharing respectively, in which the user operates the computer terminal for access control of educational resource data in IoT environment. At the same time, this paper introduces blockchain technology to verify the identity of the logged-in users of the teaching resources database, and finally, the application of this paper's method in the test environment is completed through the design of encryption and decryption and sharing transmission of the educational resources data of the IoT environment.

3.1 Analysis of blockchain-based educational resource sharing

3.1.1 Shared efficiencies

First of all, the resource sharing efficiency of the three methods is compared and examined, and the number of front-end concurrent requests for resource data that can be processed per second under each method is used as the examination index.The number of front-end concurrent requests for resource data that can be processed per second for the first 20 seconds of the sharing of the three methods is shown in Fig. 3 (the experiments of each method are repeated for 10 times, and the results shown are the average value of the 10 experiments).

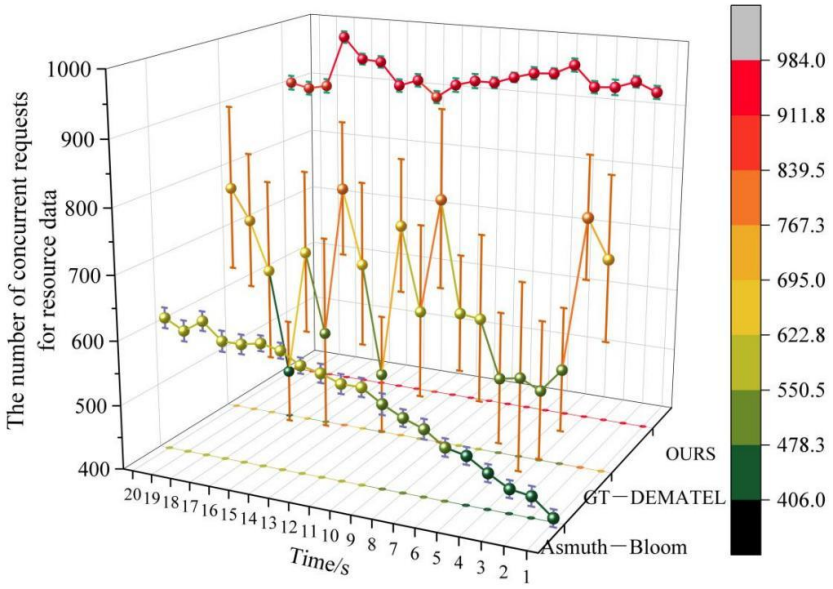

Figure 3: The efficiency of resource sharing for the three methods

In the test lasting 20 seconds, when this paper's method carries out educational resource data sharing processing, it has the highest number of resource data that can be processed per second, which is always maintained at more than 900 items, and the highest number of items can be processed per second is 983 items.The number of concurrent requests for resource data from the front-end that can be processed per second by GT-DEMATEL is also relatively high, but it varies erratically, and the number of concurrently processed data jumps sharply between GT-DEMATEL also has a relatively high number of concurrent requests per second, but the variation is unstable, with the number of concurrently processed data fluctuating between 495-786, which is prone to problems such as data interruption and data loss in the shared transmission.Asmuth-Bloom's resource data sharing and transmission process is more stable, but compared with the method of this paper, the number of concurrently processed front-end requests for resource data per second in the method is low, with an average value of only about 500. Thanks to the “federation chain + IPFS” architecture adopted in this paper, the heavy pressure of storing and distributing resource files is stripped from the main chain of the blockchain and handed over to the highly efficient distributed file system, and the blockchain is only responsible for lightweight verification of ownership and access logic. This enables the system to avoid the performance bottleneck caused by data expansion on the chain when facing highly concurrent requests for rural preschool education resources, thus realizing the high throughput capacity shown in Figure 3.

3.1.2 Transaction delays

Transaction latency is the time difference between when the client sends a transaction request and when the client receives feedback from all the nodes. The study of the algorithm transaction delay test for the existence of node evil on the three algorithms in the case of different number of nodes. Each node setup under each method were conducted 10 experiments, show the data to take the average of the 10 experiments, the experimental results are shown in Fig. 4 and Fig. 5, respectively.

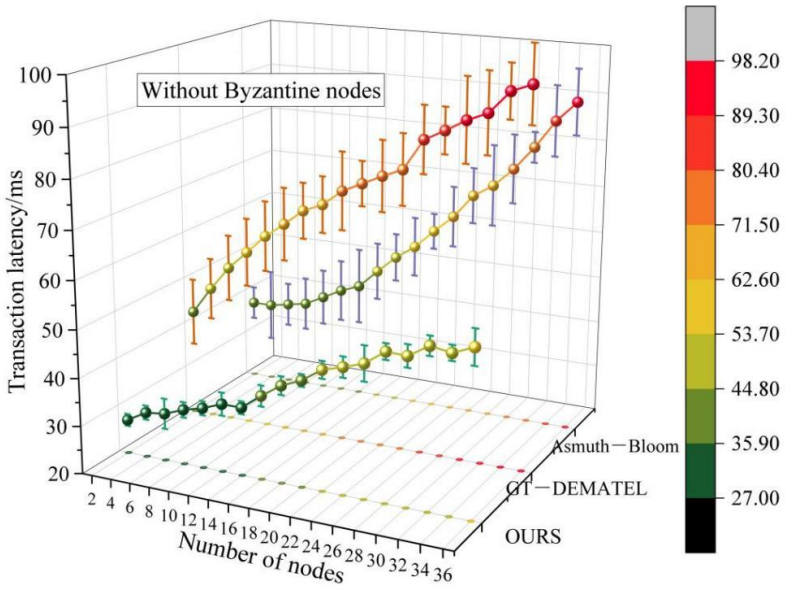

Figure 4: Transaction latency without Byzantine nodes

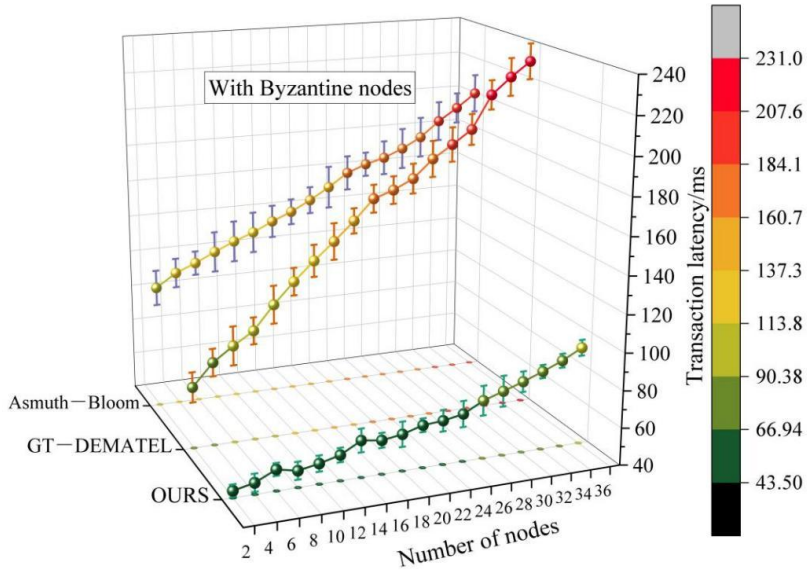

Figure 5: Transaction latency with Byzantine nodes

The transaction latency test results further confirm the reliability of this paper's system in complex network environments. Both in the ideal network without Byzantine nodes and in the simulated attack environment with the presence of malicious nodes, the latency of this paper's method is the lowest, and the latency growth curve is in the lower flat path with the increase of the number of network nodes, whereas the growth curve of the transaction latency of the two

traditional methods, GT-DEMATEL and Asmuth-Bloom, is much steeper. Taking the case of the presence of Byzantine nodes (36 nodes number) in Fig. 5, the latency of this paper's method is 92.64ms, while GT-DEMATEL and Asmuth-Bloom soar to 230.59ms and 201.73ms, which is more than twice of this paper's method. The increase in members (nodes) increases some negotiation costs, but relying on the Raft consensus mechanism deployed in Chapter 2 and the clear smart contract rules, agreement can still be reached quickly without redundant transaction latency. Especially in the presence of Byzantine nodes, the Attribute-Based Access Control (ABAC) authentication system and the tamper-proof records on the chain in this paper can quickly identify and exclude invalid or malicious requests, preventing them from slowing down the consensus process of the whole network, and thus the latency control remains excellent.

3.1.3 Communication overhead

The communication overhead refers to the total amount of communication generated by all nodes in order to reach consensus when the client sends a request. Same as the above experimental environment for testing the sharing efficiency and transaction delay, the communication of this paper's algorithm, GT-DEMATEL and Asmuth-Bloom algorithms are tested for different number of nodes, and each method is also tested for 10 experiments respectively, and the experimental results are shown in Fig. 6.

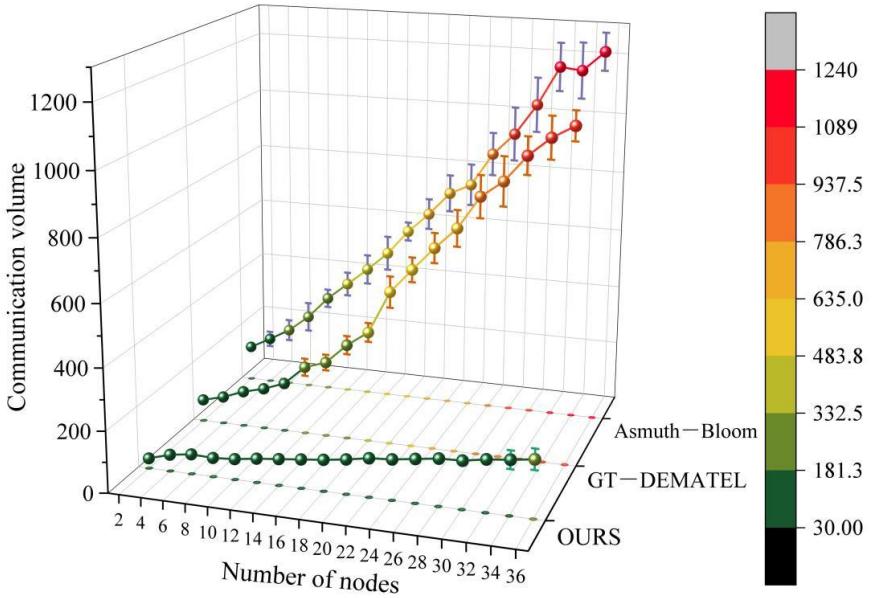

Figure 6: Communication overhead of three methods with different numbers of nodes

The communication overhead of this paper's method is significantly lower than that of the other two schemes, and the communication volume always stays around 200 times during the increase of the number of nodes from 2 to 36, which has the smoothest growth curve and is also located at the lower end of the picture. Under the large-scale network of 36 nodes, the average communication volume of this paper's method is only 187.77±11.27 times under 10 experiments, while GT-DEMATEL and Asmuth-Bloom are as high as 1086.22±78.59 and 1239.29±90.12, respectively, which are 5.8 and 6.6 times higher than that of this paper's method and the error is much larger, i.e., the results are volatile and unstable. This advantage reaffirms the article's statement that “the results are more volatile and unstable”. This advantage reaffirms the superior design concept of the article “Alliance chain + customized consensus”. Instead of using the mining mechanism, which has extremely high energy and communication costs, the study chose the efficient Raft consensus algorithm for the scenario of education resource

alliance, and stored the complex resource files in the IPFS under the chain. This allows the blockchain main chain to handle only light transaction verification and state synchronization, radically reducing the amount of data that needs to be repeatedly broadcast and verified between nodes.

3.2 Analysis of blockchain-based secure storage of educational resources

3.2.1 Detectability

The next focuses on the security analysis of the efficient blockchain-based secure storage method for digital educational resources proposed in this paper, which is mainly analyzed and verified in terms of the detectability of digital educational resources.

Assume that the resource is divided into n data blocks, in which b data are corrupted and a data blocks are challenged, and the probability of corrupted data blocks is $P_b = \frac{b}{n}$. Let X be exactly the number of selected corrupted data blocks and P_X be the probability that at least one corrupted data block is detectable.

The probability of detecting a corrupted data block P_X and its corresponding challenged block when the probability of corrupted data block P_b is chosen to be 1%, 2%, 3%, 4%, and 5%, respectively, are shown in Figure 7.

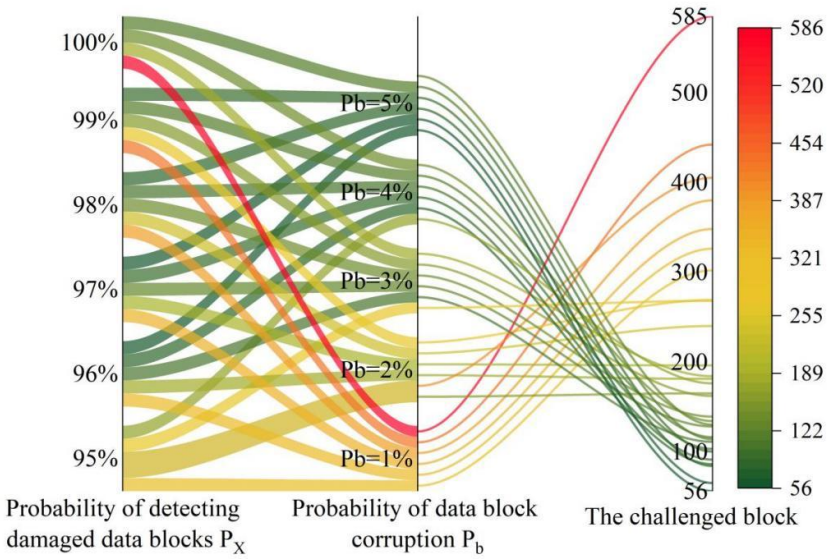

Figure 7: Probability of detecting damaged data blocks and the challenged blocks

When P_b = 1%, at least 585 data blocks must be required to achieve 100% detectability. To achieve 95% detectability, a minimum of 302 data blocks must be required. When P_b = 2%, at least 405 data blocks must be required to achieve 100% detectability. To achieve 95% detectability, a minimum of 165 data blocks must be required. When P_b = 3%, at least 268 data blocks are required to achieve 100% detectability. A minimum of 111 data blocks must be required to achieve 95% detectability. When P_b = 5%, at least 130 data blocks are required to achieve 100% detectability. To achieve 95% detectability, at least 56 data blocks must be required.

In summary, even with a very low probability of corruption, the method in this paper

requires only a few hundred blocks to be sampled to detect the problem with a very high probability. As the probability of corruption rises, the number of spot checks required is greatly reduced. This efficient detectability is also due to the research of "hash fingerprint on the chain + IPFS distributed storage" two-tier security system. Each educational resource generates a unique encrypted hash value when it is stored in IPFS, which is recorded on the tamper-proof blockchain. When conducting integrity audit, the system does not need to pull the entire file, but only need to randomly request part of the data block, recalculate its hash and compare it with the records on the chain. This makes the detection operation very lightweight and targeted, thus realizing the high detection efficiency and low verification overhead shown in Figure 7.

3.2.2 Computational overhead

Continuing to expand the research object to the comparative performance analysis with GT-DEMATEL and Asmuth-Bloom methods, the secure storage scheme contains three main phases, the initialization phase, the challenge phase and the verification phase. In the initialization phase, the time overhead it requires mainly comes from homing the resource definitions; in the challenge phase, the main time overhead comes from sampling some of the data blocks for integrity verification; in the validation phase, the time overhead mainly comes from verifying whether it complies with the predefined access policy.

In order to calculate the time for integrity verification, the file size selected in the experiment is 5M, the number of resource blocks is 100-1000 (incremented by 100), and the challenged data block is 100 to carry out the experiment, and all the results shown in Fig. 8 are the average time of 10 repetitions of the experiment.

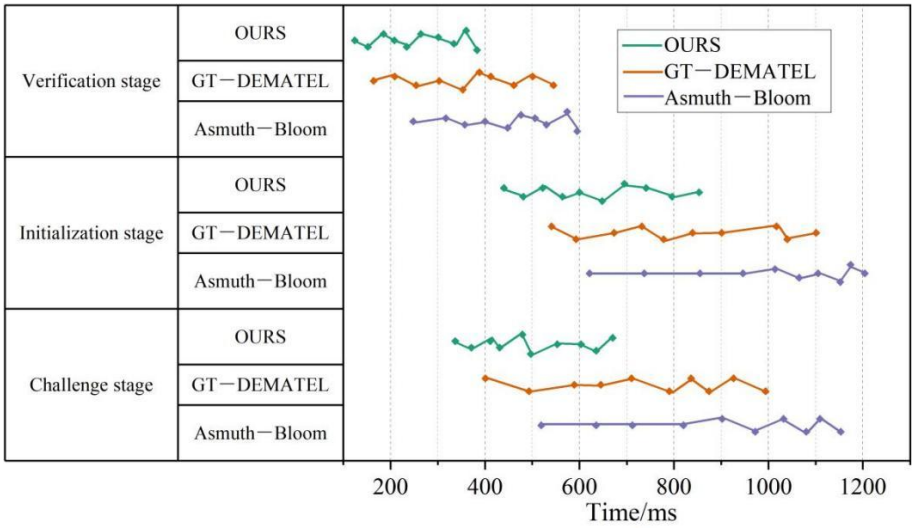

Figure 8: Time taken for integrity verification

It is known that as the number of data blocks goes from 100→1000, the time consumption of the three methods at each stage tends to increase as expected, so the data points shown in the figure from left to right are the computational overheads corresponding to the number of databases=100/200/300/400/500/600/700/800/900/ 1000, respectively. As shown in Fig. 8, the green data point corresponding to this method is the most to the left and has the shortest span, i.e., it has the smoothest growth and is always at the lowest time consumption level. In the initialization phase, this paper's method takes only 853ms to process 1000 data blocks, which is 22.52% and 29.15% less than GT-DEMATEL's 1101ms and Asmuth-Bloom's 1204ms, thanks to the lightweight metadata processing flow designed in the study. The method in this paper saves preparation time by automatically generating and registering the hash fingerprints and

attribute policies of resources through smart contracts, which avoids complex global negotiation and multiple signatures. This paper's method also performs optimally in the challenge phase of random sampling, which is only 670ms (GT-DEMATEL and Asmuth-Bloom take 994 and 1153ms) at 1000 blocks, and its efficiency stems from the on-chain hash deposit mechanism. The auditor does not need to carry or parse the whole file, but only needs to pinpoint and request a sampling of specific data blocks based on on-chain fingerprints, which greatly reduces the data transmission and processing burden. The verification phase of this paper's method is 383ms at 1000 blocks, which is also better than the other two algorithms' more than 500 milliseconds. It is because the verification logic is highly integrated into the smart contract, and combined with the pre-set access control policy, the system can quickly perform comparison and adjudication without manual or cross-system review.

3.2.3 Throughput and Latency of Blockchain Smart Contracts

The number of transactions per second is set to 50 to 500 with an interval of 50, and the throughput and latency of storing smart contracts, challenging smart contracts, and verifying smart contracts under the three methods continue to be analyzed. Fig. 9 and Fig. 10 show the throughput and latency of the three phases of the three methods, respectively.

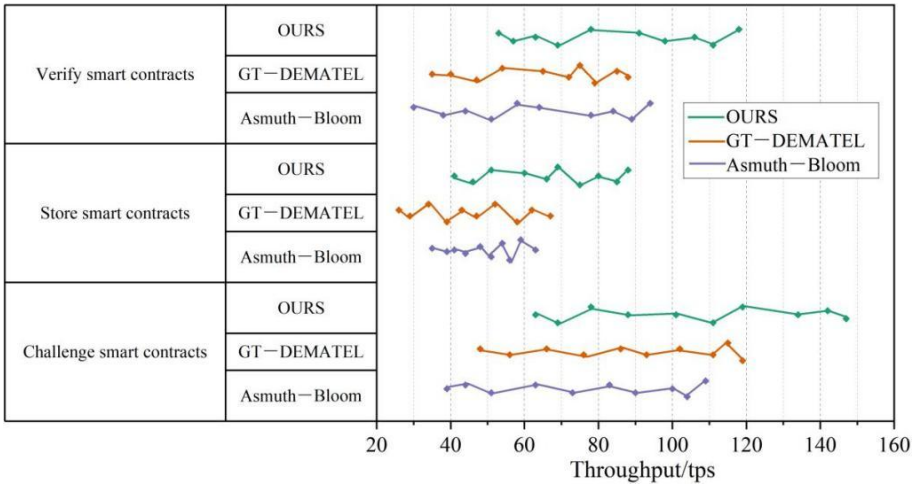

Figure 9: Throughput of Three methods and three stages

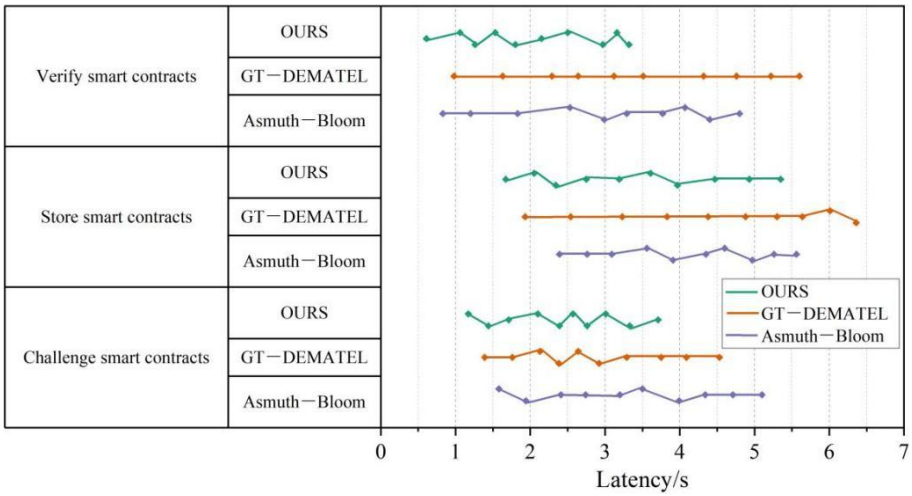

Figure 10: Latency of Three methods and three stages

This paper's side also leads across the board in terms of overall throughput capacity and response agility under constant, highly concurrent system pressure. Regardless of storage, challenge, or verification tasks, under external request pressures ranging from 50 to 500 TPS, the corresponding smart contract throughput of this paper's method is always higher than the other two methods, and the advantage tends to be more obvious as the pressure increases. Especially in the challenge phase, when the pressure reaches 500 TPS, the throughput of this paper's method is as high as 147tps, which is significantly higher than GT-DEMATEL's 119 and Asmuth-Bloom's 109tps. i.e., this paper's system, when facing a large number of concurrent resource storage requests, has a wider business processing channel and stronger digestion ability, and is less likely to experience request backlog.

Focusing again on Fig. 10 corresponding to the latency, under the same request pressure, the method in this paper maintains the lowest latency at all stages throughout. In the final validation phase when the pressure is 500 TPS, the latency of this paper's method is 3.32s, while the comparison method reaches 5.60s and 4.80s, respectively.The lower latency means that the user can get a clear feedback faster after initiating a request, which makes the experience smoother.

4 Conclusion

The blockchain-enabled solution proposed in this study has significant advantages in sharing efficiency, system response, operational overhead and security performance. It provides both prospective and feasible technical paths for solving the challenges of security, trustworthiness, and fine control in the sinking of rural preschool education resources.

(1) In terms of efficiency and response, this paper's method can handle up to 983 concurrent resource requests per second in terms of resource sharing efficiency, which is 27%-52% ahead of GT-DEMATEL and Asmuth-Bloom methods.

(2) The system transaction latency is extremely low, even in the simulated presence of malicious nodes environment, the response time of the system to reach consensus is still controlled at a very low level, with a latency within 43-92ms, demonstrating a strong anti-interference and fast consensus capability.

(3) In terms of operation overhead and scalability, the internal communication cost of the system is extremely low. The communication overhead for reaching consensus at 12 nodes reaches only 78 units, and only 187 units in a 36-node network, implying that the burden of the system in this paper grows gently when the network scale is expanded, with good scalability, suitable for rural pre-school education multi-institutional collaboration.

(4) The resource damage detection capability is excellent, only sampling 114 data blocks, it can detect 5% damage with 99% probability, realizing efficient security audit.

(5) The scheme in this paper has the shortest computation time consumption in all three phases of initialization, challenge, and verification. It takes only 383ms to verify 1000 data blocks.Meanwhile, the underlying smart contract demonstrates high throughput capability, processing 147 transactions per second in the challenge phase with the lowest latency.

About the Author

Guiyun Li was born in Hengshui, Hebei, P.R. China, in 1982. She received the master's degree from Shaanxi Normal University, P.R. China. Now, She is employed at Hebei Institute of International Business and Economic. Her research focuses on digitalization in preschool education.

Chenhui Ru was born in Qinhuangdao City, Hebei Province, China, in 1990. She graduated from Shenyang Normal University with a master's degree in Preschool Education. She is currently employed at Hebei institute of International Business and economics. Her research interests include preschool teacher education and the digital development of preschool education.

References

[1] Zhang, L., & Liu, Q. (2017). Early childhood education in economically disadvantaged rural areas of China. Early childhood education in Chinese societies, 111-130.

[2] Zhu, W., & Chang, D. F. (2020). Detecting the equality of resource allocation for pre-school education based on Gini coefficients of China's provinces. ICIC Express Letters, 14(1), 53-65.

[3] Hu, B. Y., Roberts, S. K., Leng Ieong, S. S., & Guo, H. (2016). Challenges to early childhood education in rural China: Lessons from the Hebei province. Early child development and care, 186(5), 815-831.

[4] Vidal-Esteve, M. I., & Martín-Gómez, S. (2023). Digitalization of Classrooms: A Comparative Study on Teachers' Perceptions about the Use of Digital Teaching Materials in Early Childhood and Primary Education. Education Sciences, 13(11), 1156.

[5] Aditya, B. R., Ismiatun, A. N., Atika, A. R., & Permadi, A. (2022). Digital disruption in early childhood education: a qualitative research from teachers' perspective. Procedia Computer Science, 197, 521-528.

[6] Madida, M., Rugbeer, H., & Naidoo, G. M. (2019). Barriers to effective digital teaching in rural schools. Gender and Behaviour, 17(4), 14101-14115.

[7] Suryavanshi, A. (2024). Exploring the Copyright Challenges and Compliance in Digital Education: Navigating Intellectual Property in Distance Learning Platforms. Journal of Law and Intellectual Property Rights, 1(1), 64-72.

[8] Lazariuc, C. (2021). Digital education as a strategy for the protection of intellectual property rights. Eastern European Journal for Regional Studies (EEJRS), 7(1), 132-155.

[9] Shen, T. (2024). Right to learn in the digital age: Challenges and protection in China. Computer Law & Security Review, 53, 105989.

[10] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[11] Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705.

[12] Xie, R., & Tang, M. (2024). A digital resource copyright protection scheme based on blockchain cross-chain technology. Heliyon, 10(17).

[13] Savelyeva, T., & Park, J. (2022). Blockchain technology for sustainable education. British

Journal of Educational Technology, 53(6), 1591-1604.

[14] Li, J., Lan, M., Tang, Y., Chen, S., Wang, F. Y., & Wei, W. (2020). A blockchain-based educational digital assets management system. IFAC-PapersOnLine, 53(5), 47-52.

[15] Yue, H. (2018). Balanced allocation method of preschool education resources based on coordinated development of urban and rural areas. Kuram ve Uygulamada Egitim Bilimleri, 18(6), 3599-3609.

[16] Tang, M. M., Zeng, Z., & Lan, Q. (2024). How to evaluate the efficiency of rural preschool education resources and its regional differences in China. Scientific Reports, 14(1), 22705.

[17] Huang, C., & Li, L. (2023). Research on the resource allocation of preschool education in urban and rural areas of China from 2021 to 2050 under the three-child policy. Journal of East China Normal University (Educational Sciences), 41(12), 113.

[18] Zhan, Z., & Fan, A. (2022). How to promote quality and equity of early childhood education for sustainable development in undeveloped rural areas of China: An evolutionary game study. Sustainability, 14(24), 16438.

[19] Sun, J., Wu, H., & Shi, S. (2023). A research of the evaluation of preschool education resource allocation level and spatio-temporal differences: Based on repeated indicators method and Theil index. Heliyon, 9(6).

[20] Chen, W. (2024). An analysis of the inequality between urban and rural preschool education in China. In Addressing Global Challenges-Exploring Socio-Cultural Dynamics and Sustainable Solutions in a Changing World (pp. 204-210). Routledge.

[21] Li, G., & Zhang, G. (2025). Rural Kindergarten Sports Resource Supply Dilemmas and Solutions Under Rural Revitalization. Journal of Sport for All and Recreation, 7(2), 177-186.

[22] Yang, W., & Jiang, Q. (2024). Inefficient urban-rural resource allocation and reduced tuition benefits for preschool education: an example from a Chinese county. Asian Education and Development Studies, 13(5), 432-443.

[23] Zhao, G., He, H., Di, B., & Guo, Q. (2024). BC-DERCP: Blockchain-based copyright protection mechanism for digital educational resources. Education and Information Technologies, 29(15), 19679-19709.

[24] Rani, P., Sachan, R. K., & Kukreja, S. (2024). Educopyright-chain: an educational resources copyright protection system utilizing permissionless blockchain and non-fungible tokens. Peer-to-Peer Networking and Applications, 17(6), 3583-3602.

[25] Guo, J., Li, C., Zhang, G., Sun, Y., & Bie, R. (2020). Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, 79(15), 9735-9755.

[26] Silaghi, D. L. (2025, May). Blockchain-Based Solution for Protecting Teachers' Copyrights on Educational Resources. In 2025 18th International Conference on

Engineering of Modern Electric Systems (EMES) (pp. 1-6). IEEE.

[27] Hao, Z., Yahya, M. Y. B., & Lu, J. (2023). Influence of Blockchain Technology Application in Education on Online Teaching Resources Sharing. Int. J. Emerg. Technol. Learn., 18(11), 25-37.

[28] Wahyuningsih, T., Oganda, F. P., & Anggraeni, M. (2021). Design and implementation of digital education resources blockchain-based authentication system. Blockchain Frontier Technology, 1(01), 74-86.

[29] Al Samarai, B., & Morato, J. (2023). Use of blockchain technology in educational field. IJTPE J, 15(4), 140-151.

[30] Chen, Y. (2024, August). Design of Blockchain-Based Digital Education Resource Platform. In International Conference on Knowledge Innovation and Invention (pp. 127-134). Singapore: Springer Nature Singapore.

[31] Tang, S., Wang, Z., Jiang, J., Ge, S., & Tan, G. (2022). Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain. Scientific Reports, 12(1), 4426.

[32] Nguyen, D. H., Sei, Y., Tahara, Y., & Ohsuga, A. (2025). A model-based approach for designing and validating ABAC policies. In Software Engineering and Management: Theory and Applications (pp. 19-36). Springer, Cham.

[33] Liu, C., Xiang, F., & Sun, Z. (2022). Multiauthority Attribute‐Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks, 2022(1), 8497628.