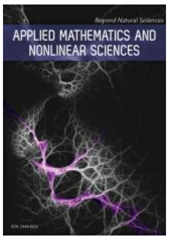

Applied Mathematics and Nonlinear Sciences

https://www.sciendo.com

Data Owner Rights Protection and Digital Identity Management Enabled by Blockchain

Dong Liang[1,†], Jun Wang[1], Zhixin Wang[2], Cuizhi Tong[2], Hui Zhang[2]

1. State Grid Jibei Electric Power Company Limited, Beijing, 100054, China.
2. Smart Distribution Network Center, State Grid Jibei Electric Power Company Limited, Qinhuangdao, Hebei, 066100, China.

Submission Info

Communicated by Z. Sabir
Received September 7, 2024
Accepted December 26, 2024
Available online February 5, 2025

Abstract

With the rapid development of blockchain technology, it shows great potential in data owner rights protection and digital identity management. In this study, a shared rights protection system for data owners and a digital identity management system were constructed using the blockchain architecture system, combined with cryptography technology. Additionally, the functional module design is implemented for both groups of systems, and the performance of the data owner rights protection system and digital identity management system is verified through simulation experiments. The throughput of the PBFT consensus algorithm used in this paper's entitlement protection system is 1281, 1319, 1205, 1348, and 1346 in order when the number of nodes is 10, 20, 30, 40, and 50.The entitlement protection system proposed in this paper is tested on trusted preprocessing, audit file encryption, audit cipher uploading, audit cipher downloading, audit file decrypting, and trusted root verification. 150 times with an average time consumption (ms) of 6.50, 460.43, 28.99, 37.43, 240.09, and 6.47, respectively. In addition, the proposed digital identity management system has a less average time consumption for individual credential issuance. The time consumption of this system in the authentication phase is 0~163.71ms faster than the comparison system and it can improve the security of the management system by using multi-signature technique.

Keywords: Blockchain; Cryptography Technology; Shared Rights Protection; Digital Identity Management; PBFT Consensus Algorithm.
AMS 2010 codes: 68T05

†Corresponding author.
Email address: gpaorl90@163.com

ISSN 2444-8656
https://doi.org/10.2478/amns-2025-0046

1 Introduction

The rapid development of the digital economy has created more value for the society, and at the same time, it has also generated a large amount of data, and how these data can be better protected has become a key issue that must be considered in the era of digital economy. Especially in the virtual network environment, a series of infringement events caused by data are more and more, and the expectation of data owner rights protection is also higher and higher, only by clarifying the huge impact on the protection of the rights and interests of the data owner in the era of digital economy, can we find a better way to solve these problems [1-4]. Identity authentication is the first barrier to protect user data resources in the network, and there are some deficiencies in the existing identity management system. For example, the standard of identity management mechanism is not uniform, the lack of strong trust relationship between organizations, different application services are not easy to integrate, identity management relies on third-party authoritative central institutions, identity information is easy to be leaked, abused, user data access control mechanism is not perfect, the user lacks autonomy over their own data, user data is easy to be stolen. Therefore, how to manage the identities of different systems and corresponding user data resources has become a challenging problem [5-8].

Blockchain creates a new computing paradigm and collaboration model to establish trust at low cost in an untrustworthy competitive environment, which can realize penetrating regulation and trust cascading by virtue of its unique trust establishment mechanism. Originating from crypto-digital currencies, blockchain is now being extended to vertical fields, contains huge potential for change, is expected to become an important component of the information infrastructure of the digital economy, and is changing the development picture of many industries. Among them, blockchain-based data owner rights and interests protection and digital identity management are two of its important directions [9-11]. As the current digital identity still exists problems such as information fragmentation, easy data leakage, and difficult self-control of users, blockchain technology, with its decentralized, encrypted, and difficult-to-tamper features, provides a direction worth exploring for credible authentication, autonomous authorization, and privacy protection of digital identities, which has attracted much attention from the government and industry. If the decentralized blockchain technology is combined with the existing centralized system, it may be possible to make the protection of the rights and interests of data owners and the management of digital identities more effective, so that the blockchain-based digital identity management system is expected to become a basic architectural component of the future Internet [12-15].

In the context of digital transformation, the digital economy on the one hand increasingly highlights the economic value of personal data, on the other hand, it also makes the data subject in the protection of the rights and interests of personal data face greater risks. Literature [16] points out that the use of blockchain may interfere with the privacy rights of individuals, from the perspective of privacy to the problem of identifiers on the blockchain, the distribution of responsibilities of participants, and the contradiction with the rights of data subjects, and puts forward the proposal of applying the principle of privacy design to the application of the blockchain to harmonize the protection of the rights and interests of data owners. Literature [17] proposes a decentralized data management framework that can ensure the privacy and control of user data, and in which a protocol for controlling user data using blockchain technology is proposed in order to reduce the occurrence of incidents related to multimedia copyrights and security breaches, and to safeguard the rights of users. Literature [18] proposes a personal data privacy protection scheme based on federated blockchain and experimentally verifies the effectiveness and feasibility of the scheme, which enables the implementation of data ownership and fine-grained access control of users to solve the problem of lack of transparency and auditability of data. Literature [19], in order to enable data owners to perceive whether service providers comply with the General Data Protection Regulation (GDPR) and effectively protect their personal data, proposes the design concept of developing a GDPR-compliant personal data management platform using emerging blockchain and smart contract technologies, and verifies the effectiveness and feasibility of the design concept through empirical analysis.

With the arrival of digital society, digital identity management has become an important content concerning the national Internet development strategy, digital economic security, and users' digital rights. Literature [20] reviews the existing literature on blockchain-based identity management solutions, identifies potential research gaps and opportunities in this literature, and provides reference data for subsequent researchers to study data identity management methods. Literature [21] points out the importance of digital identity for digital transformation, tries to apply the governance principle of self-sovereign identity to a blockchain-enabled privacy-preserving identity management system, and illustrates its effectiveness and limitations through experiments. Literature [22] explores how to apply the user-controlled resilient identity management system (SSI) framework to a blockchain-based decentralized identity management system, and proposes a proof-of-concept based on the case of public transportation, which provides a high-level of security and transparency to all parties involved in the public transportation ecosystem. Literature [23] focuses on investigating the development of blockchain-based concepts and products in the context of validating claims and self-sovereign identities, demonstrating the highlights and shortcomings of various data identity management solutions, and facilitating the sustainable development of zonal chain-based data identity management technologies.

The purpose of this paper is to explore how blockchain empowers the protection of data owners' rights and interests, and how to optimize digital identity management. Using the data storage, consensus mechanism, and smart contract in the blockchain system, and combining several cryptographic techniques, we have designed a blockchain-enabled data owner rights protection and digital identity management system. The PBFT consensus algorithm throughput and audit item indicators are used to evaluate the performance of the rights protection system. The performance of the digital identity management system constructed in this paper is also evaluated by measuring the time overheads of different identity credential issuance and verification phases.

2 Key technologies for blockchain-based rights protection and identity management

2.1 Blockchain system architecture

The blockchain system architecture is shown in Figure 1. The data layer is the lowest layer in the blockchain system architecture, encapsulating a series of data structures. The network layer is composed of a P2P network, a data dissemination mechanism, and a data validation mechanism that safeguards the communication between the nodes in the blockchain. The consensus layer contains a variety of consensus algorithms to reach an agreed state through consensus among the nodes in the blockchain network. The incentive layer encapsulates a reward mechanism to motivate nodes in the network to actively participate in data verification and consensus, ensuring the safe and stable operation of the blockchain system. The Hop smart contract enables the programmable features of the blockchain system. The application layer encompasses various application scenarios for the blockchain system, which include both digital currency and non-digital currency applications.

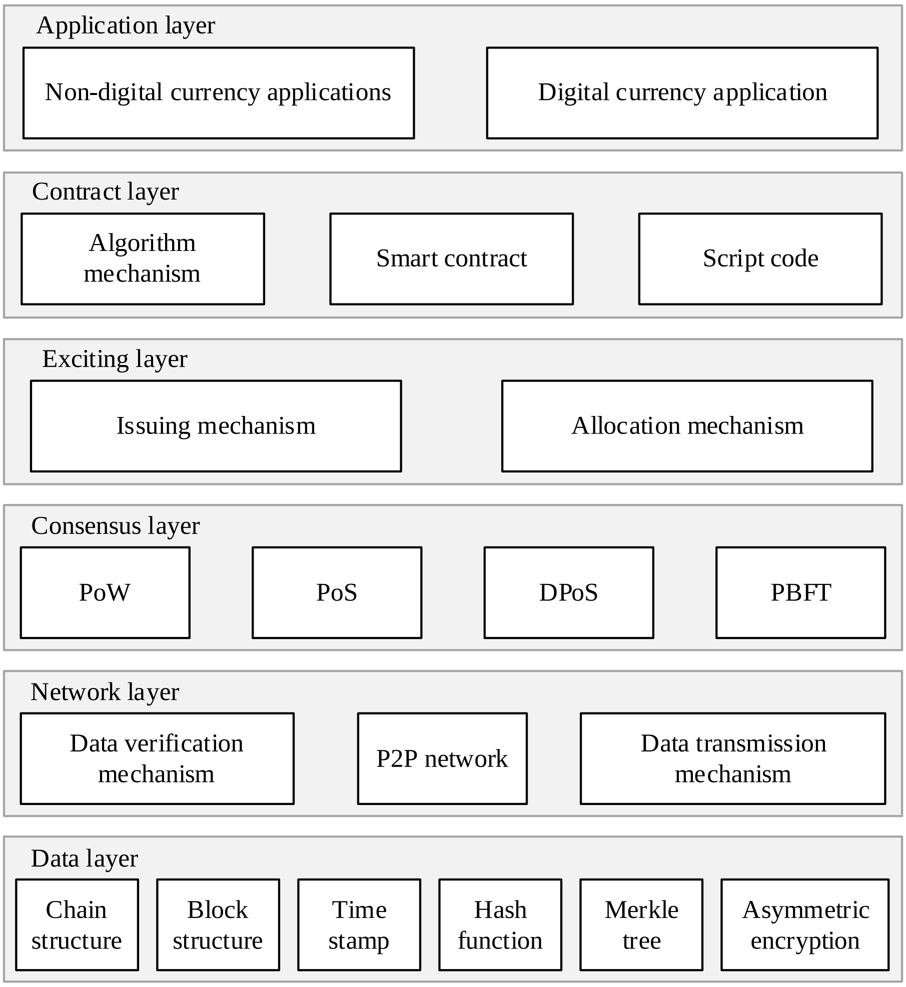

Figure 1. Blockchain system architecture

2.1.1 Data storage structure

Blockchain is a decentralised network public ledger, from the perspective of data structure, the ledger consists of blocks, nodes collect and validate transactions in the network and organise the transactions into blocks in the form of a Mekle tree, and any change in the transaction will result in a change in the root value of the Mekle tree.The root value of the Mekle tree, together with the hash value of the previous block, the one-time count, and the timestamp make up the block header, and blocks are connected to each other using the hash pointer of the block header to form a chain structure. The blocks are connected to each other using the hash pointer of the block header to form a chain structure.

2.1.2 Consensus mechanisms

The consensus algorithm used in this paper is Practical Byzantine Fault Tolerant Consensus (PBFT). In PBFT, up to 1/3 of the malicious nodes in the system can be tolerated [24]. In a PBFT-based blockchain network, the blockchain nodes are divided into master and sub nodes. There is only one master node, while the rest are sub nodes. The master node receives the consensus request message from the client and sends it to the vice node, the vice node receives the message and performs the legitimacy verification and sends the verification result to the other nodes, when the number of passed verifications is greater than 2f+1 (f is the number of malicious nodes), then it confirms the message and replies to the client with the result of execution.

2.1.3 Smart Contracts

A smart contract is a set of state response rules that are securely stored on the blockchain. Smart contracts enable users to control their digital assets, express business logic, and formulate their rights and obligations. When two or more participants agree on every rule in a smart contract, it is then cryptographically signed and sent to the blockchain network for verification. The smart contract will be executed independently and automatically according to the rules formulated once the predefined conditions are triggered.

2.2 Cryptographic techniques

2.2.1 Multiple signatures

The implementation process of digital signature can be expressed as follows: the sender uses the hash function H to generate a digest d for the message M, and uses his own private key SK to sign d; then sends the message M together with the signature s to the receiver B; the receiver B verifies s using A's public key PK, and if the signature is valid, it means that the message came from the sender A; the receiver B uses the hash function H to generate a digest d' for the message M, and compares it with d sent by A. If the signatures are the same, the message will not be tampered with or corrupted. And compares it with the one sent by A. The message hasn't been tampered with or corrupted if the digests are identical.

2.2.2 Hash functions

The representation of a general hash function is in the form of Equation $H:\{0,1\}^* \rightarrow \{0,1\}^n$. where H is the hash function; $\{0,1\}^*$ is the set of inputs; and $\{0,1\}^n$ is the set of outputs. The hash function is a mapping function, which is centred on mapping an input value to an output value through an input value, and different input values should be mapped to different output values, but of the same length [25].

2.2.3 State secret algorithms

State secret algorithm (SM algorithm) refers to the standard of cryptographic algorithms independently developed by the Chinese cryptographic community, of which SM2 and SM3 algorithms are mainly applied in this paper [26-27].

The SM2 algorithm uses a fixed elliptic curve parameter set, which is selected as a secure parameter set that satisfies certain mathematical conditions, and is called the "SM2 recommended curve". The specific parameters include the finite domain p, the elliptic curve equation parameters a and b, the order n of the points on the elliptic curve, and the coordinates of the base point G (Gx, Gy). These parameters are obtained through a series of calculations and verifications to satisfy the security requirements.

In the SM2 signature algorithm, the signature value is calculated as:

$$R=(e+x_1)modn \tag{1}$$

$$s=((1+d)^{-1}*(k-x_1*r))modn \tag{2}$$

where e is the hash of the message, x_I and r are random numbers on the curve, k is a random number, d is the private key and n is the order of the curve. The bilinear pair operation is used to compute the value of $I+d$. In SM2 encryption algorithm, the ciphertext is computed as:

$$C_1=[k]G \tag{3}$$

$$C_2=M\oplus KDF(H,k_{len}) \tag{4}$$

$$C_3=Hash(x_2\square M\square y_2) \tag{5}$$

$$C=C_1\square C_2\square C_3 \tag{6}$$

Where, G is the base point, k is a random number, M is the plaintext message, H is the hash value of the message, k_{len} is the key length, KDF is the key derivation function, x_2 and y_2 are the coordinates of the public key and Hash is the hash function. The bilinear pair operation is used to compute C_I, where $[k]G$ denotes the base G multiplied by k.

The SM3 algorithm can convert a message of arbitrary length into a 256-bit hash value for security applications such as data integrity checking, digital signatures, identity authentication, etc. The design idea of the SM3 algorithm is mainly borrowed from the SHA-256 algorithm, but it is different in the algorithmic structure, the message extension, the initial value setting, the nonlinear function, and the compression function.

3 Blockchain-enabled data-sharing rights protection design

3.1 Design of the general framework for rights and interests protection

The overall framework and core processes of the system are designed from three perspectives: system architecture, application architecture, and technical architecture. The first step is to build the overall architecture of the system, based on the online auditing platform, to build a framework for the protection of data sharing rights and interests, and then to go deeper into the application architecture of the system layer by layer, designing the application services from the data source layer to the data visualisation layer, and finally completing the design of the technical architecture of the system.

3.1.1 System architecture

The data sharing and interest protection system's architecture is depicted in Figure 2. The auditing blockchain deploys smart contracts for the controlled flow of auditing data to achieve the functions of smart contract execution, uploading of deposited data to the chain, and querying and verification of information on the chain. Uploading audit behavior to the chain for certification is the basic guarantee for security review, and the realization of the blockchain's certification of data operations, access records, etc. facilitates the tracing of responsibility and auditing after the fact. Internal and external network isolation technology is used by the data source end to ensure data security within each business department and create a secure and trustworthy data transmission channel. The data encryption component ensures that the audit data is transmitted in the form of cipher text to the external world. At the same time, it uses trusted root verification technology to ensure the chained credibility of data and prevent data from being tampered with during transmission. The data middle station summarizes the power data transmitted by each business department and stores the ciphertext of the audit data processed by the encryption component. It provides data upload, download, and storage services for internal personnel. The trusted execution environment is a secure development environment protected by hardware mechanisms with built-in API interfaces for key management, cryptographic algorithms, and so on. Auditors can conduct black-box audits in the trusted execution environment to protect the confidentiality of audit data.

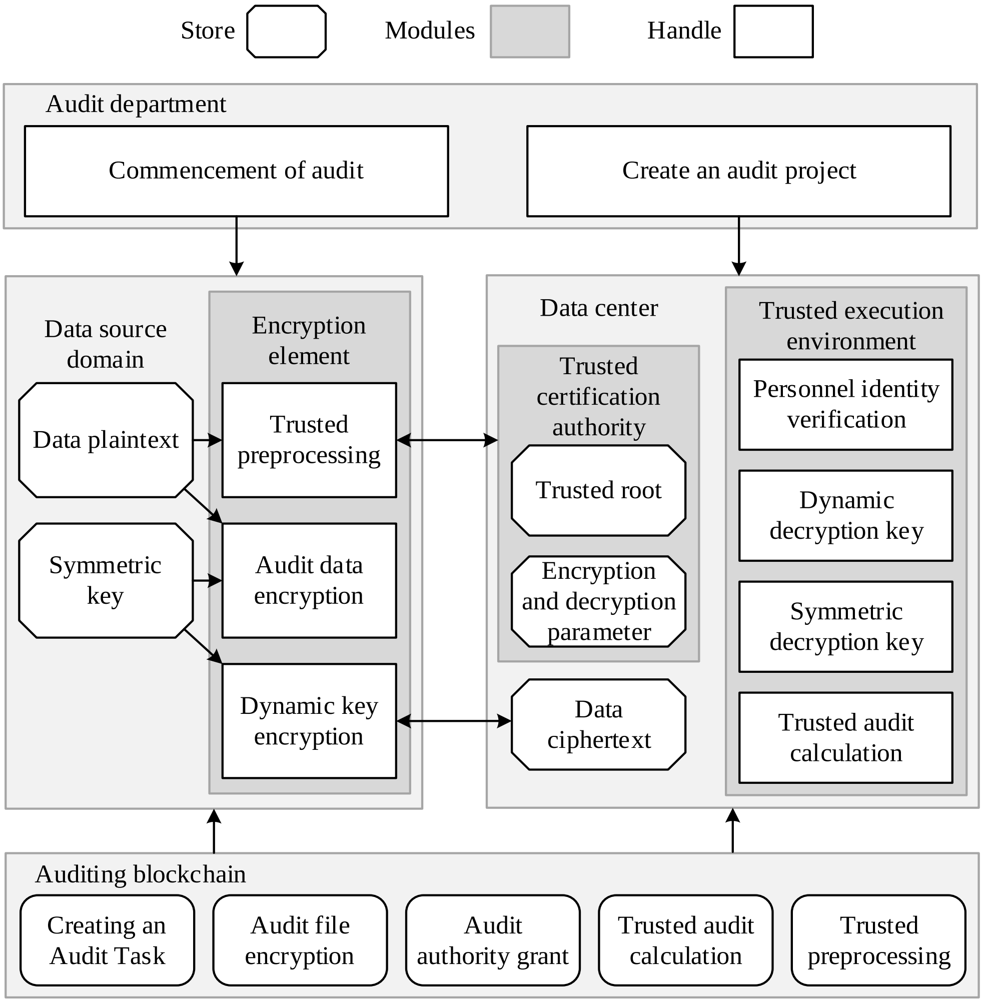

Figure 2. Architecture design of data sharing rights protection system

3.1.2 Operational architecture

Relying on the architecture of the data sharing rights protection system, a five-layer system business architecture is designed, including the data source layer, data processing layer, data sharing layer, data analysis and mining layer, and data visualisation layer. The whole application service process adopts smart contract management, encrypts the underlying data source, relies on the data sharing platform for ciphertext delivery management, implants the user requirement model for auditing calculation, and obtains and transmits the auditing result report through the data visualisation layer to ultimately realise the security protection of auditing data that is “available but not visible”. The architecture of the system for protecting shared rights is shown in Figure 3.

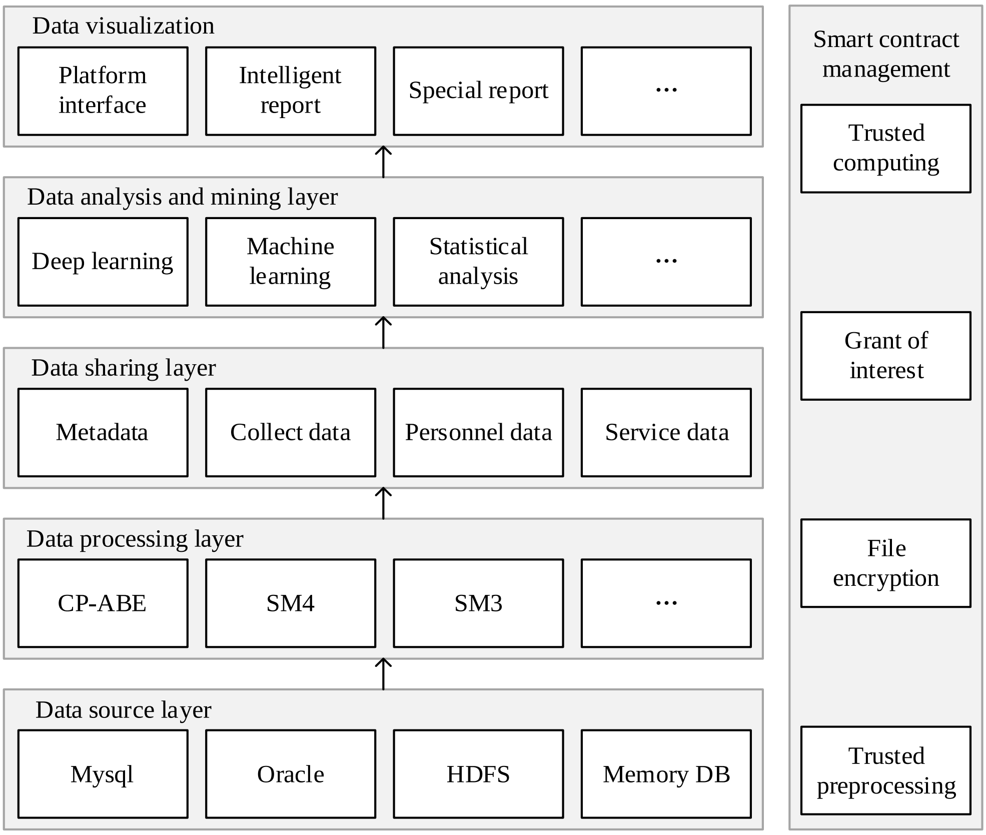

Figure 3. Application architecture design of data sharing rights protection

3.2 System core function realisation

The audit team leader formulates the access control strategy of audit operations, opens different ranges of audit data for auditors with different permissions, and with the help of encryption components, conducts mixed encryption of audit data, and the audit data is stored and transmitted in the form of cipher text, so as to realise the reliable transmission of audit data and the safe management of audit permissions.

1) Trusted Preprocessing

Whenever a batch of new business data is generated at the data source, it needs to be encrypted and uploaded to the data source for safe storage on a regular basis. Firstly, trusted preprocessing of business data is carried out to generate the secondary trusted root of the business data, which is used for subsequent verification of the consistency and integrity of the business data.

2) Audit file encryption

The audit team leader creates an online audit task, specifies the auditor, audit file, audit time and other information, generates the access control policy for the audit file according to the audit task requirements, and encrypts the audit file by combining cryptography technology.

The shared file encryption process is shown in Figure 4. The business department encrypts the audit file using the symmetric key Kdata to get the audit file ciphertext DE; constructs the access control structure tree T with time restriction, encrypts the symmetric key Kdata using the permission structure tree T and the public parameter PK attribute to get the access control ciphertext uploads the audit file ciphertext KE and the access control ciphertext KE to the data middle station for storage.

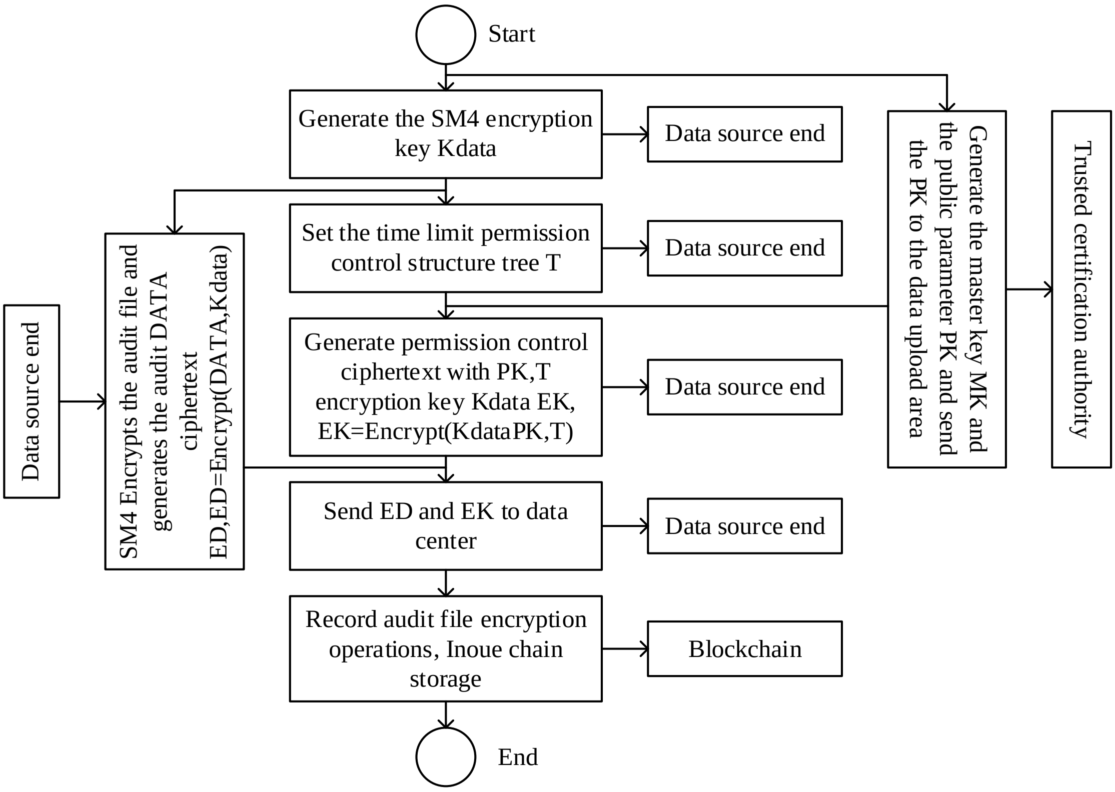
Start
Generate the SM4 encryption key Kdata
Data source end
Set the time limit permission control structure tree T
Data source end
Generate permission control ciphertext with PK,T encryption key Kdata EK, EK=Encrypt(KdataPK,T)
Data source end
Send ED and EK to data center
Data source end
Record audit file encryption operations, Inoue chain storage
Blockchain
End
Data source end
SM4 Encrypts the audit file and generates the audit DATA ciphertext ED,ED=Encrypt(DATA,Kdata)
Generate the master key MK and the public parameter PK and send the PK to the data upload area
Trusted certification authority

Figure 4. Flowchart for encrypting shared files

3) Granting of Auditing Privileges

The online auditing platform grants online auditing privileges to designated personnel, and only auditors whose user attributes satisfy the access control structure tree r within the auditing timeframe can decrypt the ciphertext of the auditing file and obtain online auditing privileges for the data.

4) Trusted Audit Determination

The auditor verifies the correctness of the received data using the second-level validation root, and performs black-box calculations in the trusted execution environment, uses the built-in audit determination model, performs statistical analysis and processing of the audit data, and exports a report of the audit results.

3.3 Performance Analysis of the Data Sharing Rights Protection System

3.3.1 Audit of time consumption assessment of project evaluation indicators

Experimental environment: Windows system with Intel(R) Core(TM) i7-3687U CPU @2.10GHz 8GB RAM.

This section analyzes the performance test of the data owner's rights protection system under blockchain mentioned above. The test includes the time consumption of six indicators: trusted preprocessing, audit file encryption, audit ciphertext upload, audit ciphertext download, audit file decryption, and trusted root verification.

Figure 5 demonstrates the results of the performance test of the entitlement protection system. This section records the time consumed results of testing each test element 150 times. As can be seen from the figure, the time consumption of the proposed interest protection system can be maintained in a small time consumption interval for 150 times of testing on trusted preprocessing, audit file encryption, audit ciphertext uploading, audit ciphertext downloading, audit file decryption, and trusted root authentication, e.g., the time consumption on trusted preprocessing is 6-7ms, which indicates that the system in this paper has a better stability of the interest protection. In addition, the average time consumption (ms) of 150 times tested on the six indicators is 6.50, 460.43, 28.99, 37.43, 240.09, and 6.47, respectively, which shows the feasibility of this paper's interest protection system.

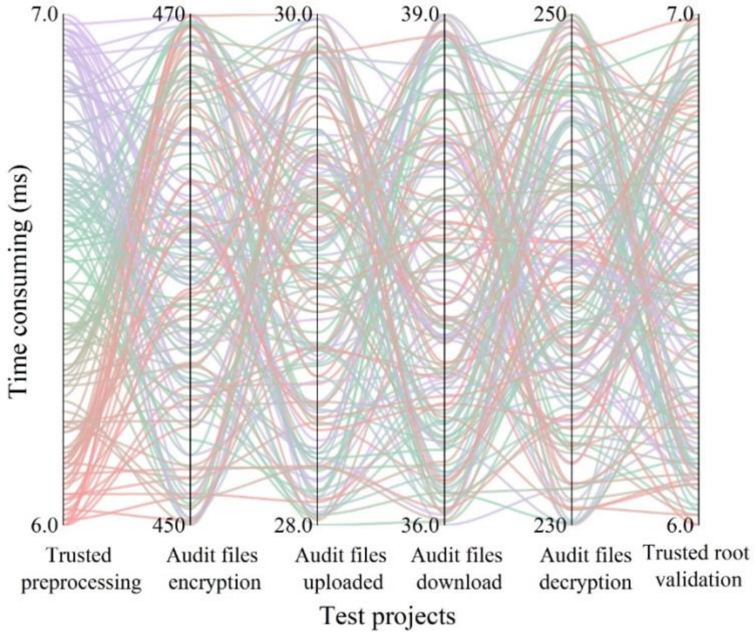

Figure 5. The protection of rights and interests can test the results

3.3.2 Throughput Measurement of PBFT-based Consensus Algorithm

In order to analyse the performance of the consensus algorithm in this paper, the following is a comparative analysis of this algorithm with other algorithms in terms of throughput. In testing the throughput performance, the experimental environment is kept the same, and the number of nodes is set to increase from 10 to 50. The comparison algorithms are PoW, PoS, and DPoS.

The performance and efficiency of a system can be determined by its throughput (TPS). The larger the system transaction throughput, the better the performance and efficiency of the algorithm. The calculation formula is as follows:

$$TPS_{\Delta t} = T\_Transactions_{\Delta t} / \Delta t \tag{7}$$

where $T\_Transactions\Delta t$ denotes the total transaction volume per unit of time t, and Δt denotes the time between the initiation of the creation of the transaction and the time interval between the block being confirmed.

The throughput comparison results of the four consensus algorithms are shown in Fig. 6. The throughput of all four consensus algorithms in the figure fluctuates, and the PoW algorithm has the lowest throughput between 150 and 196. Secondly, under different numbers of consensus nodes, the throughput of the proposed algorithm PBFT is always higher than that of the comparison algorithms, and when the number of nodes is 50, it improves by 1188, 362 and 245 compared with PoW, PoS and DPoS, respectively. It can be seen that PBFT is more stable in throughput under the condition of increasing the number of consensus nodes. In addition, the throughput averages of the four consensus algorithms are, in descending order, 169 (PoW), 945 (PoS), 1208 (DPoS), and 1300 (PBFT). To sum up, the throughput of the algorithm presented in this paper is the best performance among these algorithms.

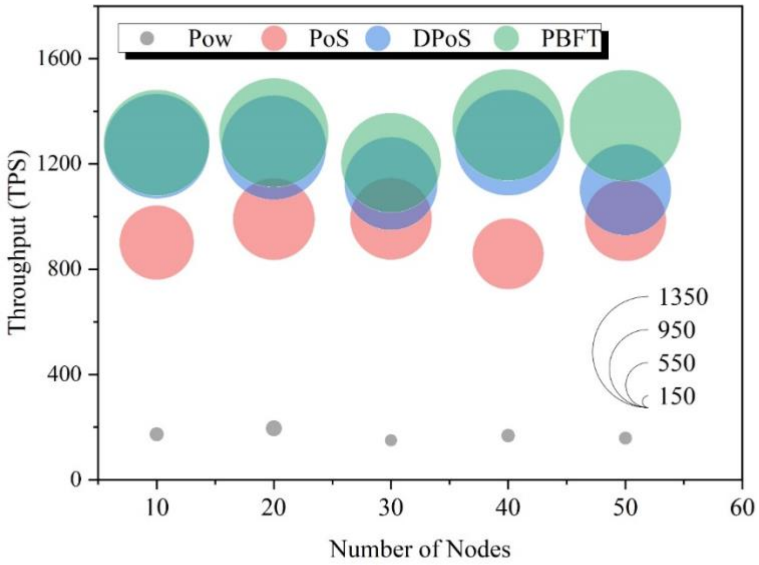

Figure 6. The throughput comparison results of the four consensus algorithms

4 Blockchain-based digital identity management system implementation and testing

4.1 Overall design of the identity management system

This section proposes and systematically implements a blockchain-based identity management mechanism, and Fig. 7 shows the overall architecture of the identity management system. It is divided into the following four layers:

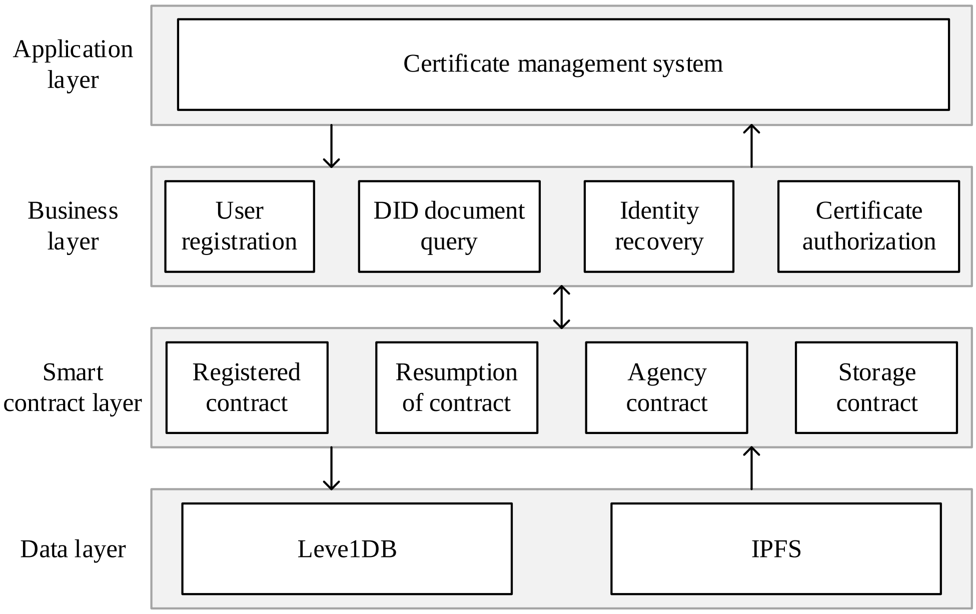

Figure 7. Hierarchy of the digital identity management system

The application layer: Users send corresponding requests to the back-end interface using HTTP and TCP protocols by filling in data, clicking buttons, and other operations. The back-end subsystems include the user system, blockchain system, and IPFS system. The user system receives service requests from users and acts as a middleware to invoke contracts with the blockchain system, submit identity information to the IPFS system, or extract identity information.

Business Layer: It is the service end of each sub-system, which handles legitimate requests submitted by the application layer, such as digital user registration, identity credential issuance, identity credential verification, identity restoration and other business logics, and executes commands within the layer to make calls or additions, deletions, changes and checks to the lower layer.

Smart Contract Layer: It is mainly responsible for the registration of digital identity, storage of identity credential declaration, verification, identity recovery and other functions. A smart contract is a contract that can be executed automatically, and it consists of a set of code and data that can be run on the blockchain.

Data layer: usually implemented by a database, which can be relational or distributed. The design of the data layer needs to consider factors such as data security, reliability, and consistency to ensure data integrity and accuracy.

4.2 Functional design of the identity management system

The distributed identity management system that is based on blockchain allows for on-chain and off-chain collaboration to safeguard the security of identity credentials. It uses certificate-less encryption algorithms to encrypt and store the original identity data in IPFS, ensuring the security and trustworthiness of the data. By creating DID identifiers for data users to register their identities, uploading the identity credentials statement to the blockchain, the identity credentials are locally stored by the data owner, and the data owner can use one identity credentials to authenticate their identities with different service providers, which improves the system usability and user experience.

4.2.1 Identity Registration and Login Module

The data user enters an account number, selects a login role, and clicks the Register button. The front-end sends the account name and role type to the back-end, which verifies that the digital user has been registered, and the system calls the Register interface function in the registration smart contract to store the DID document, didDocument, that records the data user's public key, PK, with the distributed identifier, DID, to complete the identity registration.

4.2.2 Identity credential issuance module

The Identity Center is accessed by the identity owner to add certificate information and complete the identity data form. The identity owner chooses the data provider as the authentication organization for their identity credentials and then inputs the original identity data into the text box to apply for the identity credentials.

The data provider logs into the "Pending Credentials Center" of the system to view the list of identity credential applications of the data owner. The provider looks up the corresponding identity data cipher text, decrypts the original identity data information using the private key, verifies the authenticity of the original identity data, and issues the identity credentials to the data owner after the verification is successful.

4.2.3 Identity credential validation module

The service provider requests identity credentials from the data owner, who encrypts the identity credentials VC and returns them. The service provider calls queryDIDDocument interface function to find the DID document according to the data provider identifier dpDID in the VC, and obtains its public key value to verify the signature value of the identity credential. If the verification passes, it proves that the identity credential is genuine and legitimate. If the verification passes, the service provider calls the queryUserIdentityClaim interface function in the smart contract to query the hash value of the identity credential declaration VCHash, calculate the hash value of the identity credential credential's credentialSubject, and then compare the VCHash of the identity credential declaration with the HASH of the identity credential, and then, if it is the same, prove that the identity credential provided by the data owner is real and legitimate. If the identity credential provided by the data owner is credible, authentication will pass; otherwise, authentication will fail.

4.3 Performance validation of blockchain-based identity management system

4.3.1 Identification credential issuance time overhead measurement

In order to further assess the feasibility of the identity management system, this section conducts a performance test on the proposed system simulation implementation by measuring the performance overhead of the key interaction operations during the authentication process in order to assess the overall performance of the system, the selected interaction operation is credential issuance.

The issuer node issues 100, 500, 700, 1000, and 1500 credentials to the holder node, respectively, and network system 1 (Hyrax) and network system 2 (Bulletproofs) are chosen as the comparison systems to observe their completion time. The comparison results of the total time (s) for issuing credentials with different throughputs are shown in Fig. 8. Table 1 shows the average time consumed (ms) for individual credentials with different throughputs.

As can be seen from the chart, the total time consumed for issuing credentials of this system is lower than that of the comparison system under different credential issuing volume, e.g., when the credential issuing volume is 1500, the time consumed (s) of this system is lower than that of the network systems 1 and 2 by 46.88 and 24.56, respectively.In addition, the average time consumed for issuing single credentials of the present system, the network system 1, and the network system 2 is found to be 64.474, 94.596, and 86.764, it can be seen that in the operation of approaching credentials from the issuer node to the holder node, when the number of credentials reaches the order of hundreds, the average time consuming of issuing a single credential does not show a significant increase in time consuming with the rise in the amount of credentials. Meanwhile, the average time consumed for issuing a single credential in this paper can meet the system’s requirements for the performance overhead of the key operations of identity management.

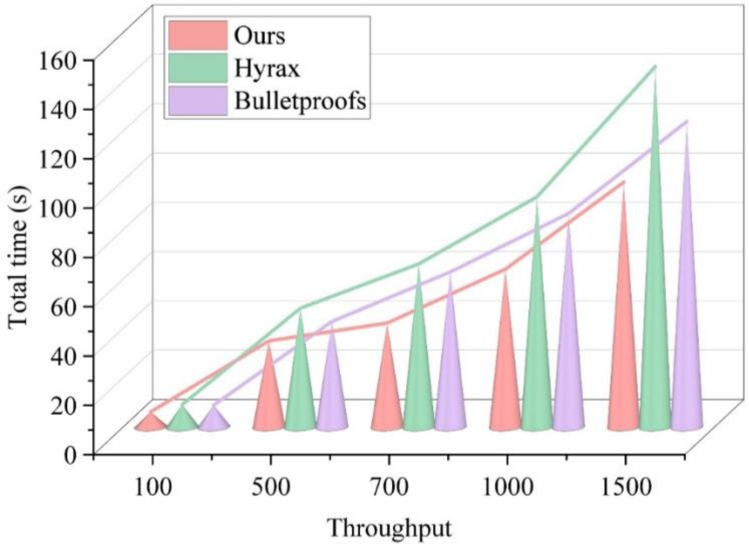

Figure 8 The total time of issuing certificates under different throughput

Table 1. The average time of a single voucher is time-consuming

Certificate quantity	Mean time (ms)		
	Ours	Hyrax	Bulletproofs
100	61.95	91.17	89.03
500	69.91	96.45	85.7
700	60.27	94.53	89.87
1000	64.03	93.37	86.64
1500	66.21	97.46	82.58
Average (ms)	64.474	94.596	86.764

4.3.2 Multi-signature based authentication time overheads

In order to evaluate and test the time overhead performance of this system, this section compares the system in this paper with the two reference systems in the previous section, in an experimental setting consistent with the above. Fig. 9 depicts the variation of time cost with the number of signatures for the aggregation phase and the aggregation verification phase.

As can be seen from the figure, when the number of nodes increases linearly, the sum of time costs for both the aggregation and aggregation verification phases of the three groups of systems shows an upward trend, but with the increase in the number of nodes, the sum of time costs of this paper's system is always lower than that of the control system, and when the number of nodes is 150, the system of this paper reduces its time consumption (ms) by 141.80 and 103.76 compared to the network systems 1 and 2, respectively.

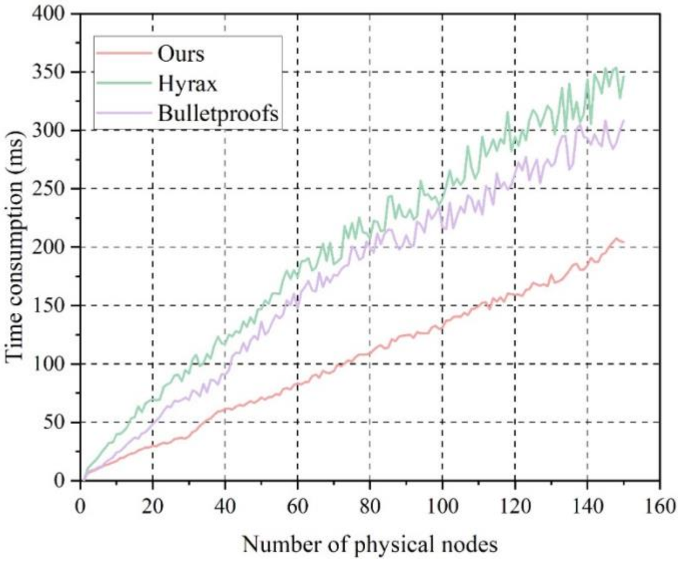

Figure 9. Time cost varies with the number of signatures

In order to further test the performance of the identity management systems proposed in this paper, this section also compares the computational overheads on the user side and server side. Table 2 shows the time (ms) overhead of the three sets of systems on the user and server sides during the cross-domain authentication phase. From the table, it is clear that the time overhead of this paper's system is slightly higher than the other two systems at the user side and server side and it requires more overhead at the server side which is 13.65 ms. This is because the system used in this paper uses multi-signature, which is more costly. But the system in this paper completes the authentication of bulk users instead of one-to-one authentication in the comparative system, the user side does not need to add too many operations and the multi-signature is calculated by the server.

Table 2. Authentication of the calculation overhead of the client and server

Time overhead (ms)	Ours	Hyrax	Bulletproofs
User	6.09	3.89	3.31
Server	13.65	5.38	4.17

5 Conclusion

In this paper, we design the data owner's rights and interests protection as well as the digital identity management system empowered by blockchain and cryptography key technology. Through several simulation experiments, the effectiveness of the two groups of systems in application is evaluated using experimental results. The following experimental results have been obtained.

For the rights and interests protection system, the PBFT consensus algorithm used in this paper always has a higher throughput than the comparison algorithm as the number of nodes increases and has better stability as the number of nodes increases. The system is stable in a small time-consuming interval for 150 tests on trusted preprocessing, audit file encryption, audit ciphertext uploading, audit ciphertext downloading, audit file decryption, and trusted root verification; e.g., the time consumption on trusted root verification is 6–7 ms.

For the digital identity management system, when the number of identity credentials issued is 1500, the system in this paper consumes less time (s) than Hyrax and Bulletproofs systems by 46.88 and 24.56, respectively, and its single credentials issuance time is 64.474ms.In addition, in the authentication phase, when the number of signatures is 150, its time consumed is 204.39ms.The time overheads in the user-side and server side time overheads are higher than the comparison system, and the overhead time in the server segment is 13.65ms.

References

[1] Wang, B., Jiawei, S., Wang, W., & Zhao, P. (2022). Image copyright protection based on blockchain and zero-watermark. IEEE Transactions on Network Science and Engineering, 9(4), 2188-2199.

[2] Sahoo, S., & Halder, R. (2021). Traceability and ownership claim of data on big data marketplace using blockchain technology. Journal of Information and Telecommunication, 5(1), 35-61.

[3] Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2019). Blockchain-enabled decentralized trust management and secure usage control of IoT big data. IEEE Internet of Things Journal, 7(5), 4000-4015.

[4] Ibáñez, L. D., O'Hara, K., & Simperl, E. (2018, July). On blockchains and the general data protection regulation. EU Blockchain Forum and Observatory.

[5] Shaik, M. (2022). Rethinking Federated Identity Management: A Blockchain-Enabled Framework for Enhanced Security, Interoperability, and User Sovereignty. Blockchain Technology and Distributed Systems, 2(1), 21-45.

[6] Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). Bidm: a blockchain-enabled cross-domain identity management system. Journal of Communications and Information Networks, 6(1), 44-58.

[7] Das, D., Dasgupta, K., & Biswas, U. (2023). A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems. Computers and Electrical Engineering, 105, 108535.

[8] Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the "Self-Sovereign" individual. Frontiers in Blockchain, 3, 26.

[9] Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: privacy-preserving protection of sensor data. Journal of the Association for Information Systems, 20(9), 1274-1309.

[10] Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem. Security and Communication Networks, 2019(1), 1431578.

[11] Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). BPDIMS: A blockchain-based personal data and identity management system. In The 52nd Hawaii International Conference on System Sciences. HISS 2019: HISS 2019 (pp. 6855-6864). Hawaii International Conference on System Sciences (HICSS).

[12] Fan, K., Ren, Y., Wang, Y., Li, H., & Yang, Y. (2018). Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET communications, 12(5), 527-532.

[13] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653.

[14] Sadhu, A. K. R. (2021). Reimagining Digital Identity Management: A Critical Review of Blockchain-Based Identity and Access Management (IAM) Systems-Architectures, Security Mechanisms, and Industry-Specific Applications. Advances in Deep Learning Techniques, 1(2), 1-22.

[15] Kikitamara, S., van Eekelen, M. C. J. D., & Doomernik, D. I. J. P. (2017). Digital identity management on blockchain for open model energy system. Unpublished Masters thesis–Information Science.

[16] Jiménez-Gómez, B. S. (2019). Risks of blockchain for data protection: a European approach. Santa Clara High Tech. LJ, 36, 281.

[17] Vishwa, A., & Hussain, F. K. (2018, November). A blockchain based approach for multimedia privacy protection and provenance. In 2018 IEEE symposium series on computational intelligence (SSCI) (pp. 1941-1945). IEEE.

[18] Liang, W., Yang, Y., Yang, C., Hu, Y., Xie, S., Li, K. C., & Cao, J. (2022). PDPChain: A consortium blockchain-based privacy protection scheme for personal data. IEEE Transactions on Reliability, 72(2), 586-598.

[19] Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. IEEE Transactions on Information Forensics and Security, 15, 1746-1761.

[20] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of network and computer applications, 166, 102731.

[21] Naik, N., & Jenkins, P. (2020, October). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In 2020 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-6). IEEE.

[22] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications, 2(2), 100014.

[23] Kuperberg, M. (2019). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. IEEE Transactions on Engineering Management, 67(4), 1008-1027.

[24] Xiaohua Wu,Zirui Wang,Xiaoyu Li & Lei Chen. (2025). DBPBFT: A hierarchical PBFT consensus algorithm with dual blockchain for IoT. Future Generation Computer Systems107429-107429.

[25] Mujtaba Hassan,Arish Sateesan,Jo Vliegen,Stjepan Picek & Nele Mentens. (2024). A Genetic Programming approach for hardware-oriented hash functions for network security applications. Applied Soft Computing112078-112078.

[26] Yichuan Wang,Yiliang Yan,Yaling Zhang,Mengjie Tian & Xiaoxue Liu. (2024). Ensuring Cross-Chain Transmission Technique Utilizing TPM and Establishing Cross-Trusted Root Security via SM Algorithm. Electronics(15),2978-2978.

[27] Yichuan Wang,Yiliang Yan,Yaling Zhang,Mengjie Tian & Xiaoxue Liu. (2024). Ensuring Cross-Chain Transmission Technique Utilizing TPM and Establishing Cross-Trusted Root Security via SM Algorithm.Electronics(15),2978-2978.

About the Author

Dong Liang (1969-), male (Han Nationality), born in Tangshan, Hebei province, master, senior engineer, main research direction: power grid digitalization.

Jun Wang (1975-), male (Han Nationality), Langfang, Hebei province, master, senior engineer, main research direction: power grid digitalization.

Zhixin Wang (1990-), female (Han Nationality), born in Qinhuangdao, Hebei province, undergraduate, engineer, research direction: data management support, big data analysis and application, blockchain technology research.

Cuizhi Tong (1994.09.19-), female (Han Nationality), born in Jincheng, Shanxi Province, master, engineer, research direction: business distribution and adjustment data management support, big data analysis and application, blockchain technology research.

Hui Zhang (1988.06.08-), female (Han Nationality), from Xinzhou, Shanxi Province, undergraduate, economist, research direction: data management support, big data analysis and application, blockchain technology research.