Scholar Publishing Group
International Journal of Business Management and Economics and Trade
https://doi.org/10.38007/IJBMET.2025.060114
ISSN 2790-0959 Vol. 6, Issue 1:138-148

Research on Identity Authentication Algorithm for Supply Chain Finance Based on Zero Knowledge Proof and Blockchain

Xin Cui
Kyrgyz State University Named After Ishenaly, Arabaev, 720000, Bishkek, the Kyrgyz Republic
cuixinn666777@163.com

Keywords: Supply chain finance; Blockchain; Zero knowledge proof; Attribute based encryption; data sharing

Abstract: Supply chain finance, a critical tool for industrial chain coordination in the digital economy, faces challenges such as centralized identity authentication, data silos, and privacy risks, with traditional models constrained by single-point failures and inefficient data sharing. While blockchain's decentralized and tamper-proof features offer a solution, existing approaches often lack comprehensiveness. To address this, this study proposes two integrated solutions: first, the ZK-SCFI scheme, which leverages Merkle trees for identity storage, Paillier homomorphic encryption for pseudo-identity generation, and zero-knowledge proofs for privacy-preserving verification, effectively avoiding centralized risks and ensuring transaction non-associability; second, the TRU-SABE framework, combining blockchain and IPFS to enhance ciphertext-policy attribute-based encryption (CP-ABE) with keyword search, user revocation, outsourced decryption, and malicious user tracking, addressing traditional limitations like high computational costs and scalability issues. Experiments demonstrate TRU-SABE's superior efficiency, with user-side decryption overhead reduced to 3TE and storage advantages from factor group structures for attribute keys and ciphertexts, while the hybrid architecture alleviates data silos and storage pressure. A prototype system built on Fisco Bcos consortium blockchain, Spring Boot backend, and Vue.js frontend validates core functionalities, including encrypted data sharing and smart contract-based traceability. This work provides a holistic privacy-preserving solution for supply chain finance, with future directions focusing on balancing privacy with regulatory compliance, optimizing multi-authority key management, and expanding system capabilities to enhance security and efficiency.

1 Introduction

With the rapid growth of global financing demand for small and medium-sized enterprises, supply chain finance, as a key tool to alleviate financing difficulties, has ushered in important development opportunities in the digital economy era. However, traditional models have hindered the financing efficiency of small and medium-sized enterprises due to complex processes,

insufficient information credibility, and limited service scope; Although modern third-party platforms have built seamless information exchange ecosystems through technologies such as cloud computing and artificial intelligence, improving service personalization and operational efficiency, they still face severe challenges in the fields of identity authentication and data sharing. Centralized identity management systems are difficult to meet the security needs of multi-party collaboration due to single point of failure risks, data islanding effects, and privacy leakage risks, while financial data sharing is hindered by inter institutional data closure and lack of privacy protection mechanisms, which not only affects business efficiency but also exacerbates transaction risks. Although existing research has made progress in the field of blockchain identity authentication and data sharing, there are still significant limitations: identity authentication schemes mostly focus on scenarios such as healthcare and the Internet of Things, and there is a lack of research on privacy protection for supply chain finance. Some schemes avoid centralization risks but face problems such as leakage of off chain cache credentials or limited applicability; Although data sharing technology explores features such as attribute based encryption (ABE), searchable encryption, and outsourced computing, it mostly focuses on optimizing a single function and lacks a comprehensive solution to simultaneously address revocation difficulties, high computational costs, and malicious user tracking. Additionally, the vulnerability of centralized storage and the problem of data silos have not been alleviated. The decentralized and tamper proof characteristics of blockchain technology provide a new path to solve the above problems. This study aims to integrate blockchain and traditional cryptographic technology to design an identity authentication and data sharing scheme for supply chain finance. The specific goals include: proposing an identity authentication scheme based on blockchain and zero knowledge proof (ZK-SCFI) to achieve zero knowledge verification and irrelevance of user identity; Build a data sharing scheme (TRU-SABE) based on improved ciphertext policy attribute based encryption (CP-ABE), integrating keyword search, user revocation, outsourced decryption, and malicious tracking functions; Design and implement a supply chain finance data sharing system that combines blockchain and InterPlanetary File System (IPFS) to ensure data privacy and full process traceability. The research contribution is mainly reflected in three aspects: the ZK-SCFI scheme stores identity information through Merkle trees, generates pseudo identities through Paillier homomorphic encryption, and combines zero knowledge proof circuits to verify the integrity of identity attributes, achieving efficient authentication while protecting privacy; The TRU-SABE solution is based on a hybrid architecture of blockchain and IPFS, integrating improved CP-ABE encryption, outsourced decryption, and user tracking mechanisms to solve the problems of revocation difficulty, high computational overhead, and difficulty in tracking malicious users in traditional solutions; The development of the system prototype has validated the encryption storage, decryption download, and full process traceability functions, providing technical support for the secure and transparent operation of supply chain finance business.

2 Correlation theory

2.1 Fundamentals and Core Mechanisms of Blockchain Technology

Blockchain[1]~[3] is regarded as a shared and tamper proof ledger used to optimize transaction records and asset tracking in commercial networks. It utilizes cryptography and consensus algorithms to securely link transaction data, first proposed by Satoshi Nakamoto in 2008 in "Bitcoin: A Peer to Peer Electronic Cash System"错误!未找到引用源。~错误!未找到引用源。. As the underlying technology of Bitcoin, it is a distributed data storage system that builds trust among multiple stakeholders in an untrusted network using a chain structure. The blockchain structure

consists of block header and block body: the block header stores metadata such as version number, previous block hash value, Merkle tree root hash value, timestamp, difficulty value, and random number; The block stores transaction data. The hash value of a block connects adjacent blocks to form a chain structure, and the encryption mechanism (hash function and Merkle tree) is the core.

Hash function 错误!未找到引用源。, as a core component of modern cryptography, converts any length input into a fixed length binary output. It has unidirectionality (unable to reverse derive the original data), fixed output length (easy to store and calculate), sensitivity to input changes (small changes can cause significant changes in hash values), and anti-collision (it is extremely difficult to find two different inputs that generate the same hash value), ensuring data privacy, integrity, and uniqueness. The Merkle tree 错误!未找到引用源。~错误!未找到引用源。 is a tree structure composed of leaf nodes, intermediate nodes, and root nodes (most commonly binary trees, also supporting multi branch trees). Leaf nodes are transaction hashes, intermediate nodes are recursively calculated from child node hashes, and root nodes are unique hash values; Its data storage is flexible (only requiring hash values) and adopts a bottom-up hierarchical computing system (leaf nodes generate intermediate nodes and regenerate into root nodes). Any data modification will cause structural changes, ensuring immutability. When verifying transactions, only a maximum of 2 x $\log_2$ (N) hash values need to be calculated, efficiently verifying data integrity.

Blockchain can be divided into three categories based on network access permissions: public chains (permissionless access, nodes can join freely, and the entire network synchronizes the complete ledger), private chains (centralized control, with a single organization managing all nodes), and consortium chains (multi institutional collaboration, requiring identity authentication and supporting fine-grained access control). According to the docking type, it can be divided into single chain (independent and autonomous, with complete ledger, consensus mechanism, etc.), side chain (cooperating with the main chain to achieve asset transfer or data exchange through cross chain communication), and interconnected chain (the main chain and side chain are mutually linked, supporting cross chain asset transfer).

2.2 Core Concepts and Technical Protocols of Cryptography

The field of cryptography 错误!未找到引用源。~错误!未找到引用源。has constructed a theoretical and technical system for modern data security and privacy protection, with core concepts and technical protocols supporting each other, forming multi-level security solutions. Bilinear mappings 错误!未找到引用源。~错误!未找到引用源。, as fundamental mathematical tools, provide an algebraic framework for encryption protocol design through the mapping of two prime order multiplication cyclic groups to another group, with properties such as bilinear, computability, non degeneracy, and symmetry; Zero knowledge proofs (ZKP) 错误!未找到引用源。~错误!未找到引用源。 have achieved a key breakthrough in privacy protection based on this foundation. Their completeness, rationality, and zero knowledge ensure the authenticity verification of proofs and zero information leakage. They are widely used in scenarios where sensitive data needs to be kept confidential; Merkel's proof verifies data integrity through hash paths, becoming an important means of efficiently verifying data consistency in distributed systems; The Groth16 protocol 错误!未找到引用源。~错误!未找到引用源。, as an efficient zk SNARK scheme, is based on elliptic curve cryptography. It converts the problem polynomial into QAP form and combines R1CS constraint system and number theory transformation to achieve the characteristics of small proof file and fast verification speed, further improving the practicality of zero knowledge proof; The Chinese remainder theorem, as a fundamental tool in number theory, provides a unique solution construction method for solving congruence equations and supports algorithm design related to

modular operations in cryptography; Homomorphic encryption technology, especially the Paillier encryption algorithm [18]~[20] based on the difficulty of high-order residue class problems in composite order groups, achieves the function of directly calculating ciphertext and decrypting results consistent with plaintext through key generation, encryption, and decryption processes, solving the privacy protection problem in sensitive data statistical analysis. These concepts [21-26] and technical protocols together form the core pillars of cryptography research and application, providing a complete solution from theory to practice for data security sharing, privacy computing, and efficient verification.

3 Research method

3.1 Design of identity authentication mechanism for supply chain finance

This article proposes an identity authentication mechanism (ZK-SCFI) that combines blockchain and zero knowledge proof for the supply chain finance field, aiming to achieve efficient and privacy protected identity verification through distributed technology. Its design goals cover five core features: attribute privacy is achieved through Merkle root existence verification, where the verifier only needs to confirm that the attribute meets the conditions without obtaining specific values; Non forgeability ensures that forged vouchers cannot pass system verification, eliminating impersonation and false statements; Reliability guarantee: Users who do not hold valid attributes or whose attributes do not meet the conditions cannot pass verification, while legitimate users can be successfully authenticated; Unlinkability is achieved through anonymous credential presentation, and multiple verification events cannot be associated with the user's true identity; Anti brute force cracking relies on the irreversibility of the Merkle tree structure and hash operations, significantly increasing the cost of attacks. The system architecture includes three roles: credential issuer (regulatory center SV), holder (supplier, purchaser, etc.), and verifier (financial service platform). The process [27-32] is divided into five stages: initialization, credential application, zero knowledge credential generation, identity verification, and credential revocation. The initialization stage completes the generation of key and identity identifiers for each participant; During the voucher application stage, users submit information to SV for verification and obtain verifiable credentials (VC) and hidden identity credentials (HIC); During the zero knowledge credential generation stage, validators design verification circuits, generate keys, and deploy smart contracts. Users generate zero knowledge proofs (Π) based on the proof key; During the identity verification phase, on chain smart contract verification and off chain verification of false identity identifiers are used; After the user initiates a request during the voucher revocation phase, SV calls the Revoke contract to mark VC as invalid. This mechanism provides a secure, efficient, and decentralized identity authentication solution for supply chain finance through the immutability of blockchain and the privacy protection feature of zero knowledge proof.

3.2 Implementation of identity authentication mechanism in supply chain finance

The supply chain finance identity authentication mechanism based on blockchain and zero knowledge proof (ZK-SCFI) proposed in this article implements distributed identity verification through a five stage process: in the system initialization stage, the regulatory center generates elliptic curve encryption parameters and large prime numbers, constructs homomorphic encryption key pairs and EdDSA signature keys, and the service platform synchronously generates ECC public and private keys and blockchain account addresses with users; During the credential application stage, users submit their identity information to the regulatory center. The center constructs a MerkleRoot attribute based on the MerkleTree, combines timestamp signatures to generate

verifiable credentials (VC) and hidden identity credentials (HIC), and maps the VC digest and status to the blockchain; In the zero knowledge credential generation stage, the service platform designs a Merkle tree verification logic that includes arithmetic constraint circuits (C1 to C3), compiles and generates proof keys and verification keys, deploys smart contracts, and users generate zero knowledge proofs by combining proof keys with privacy inputs (such as pseudo identity factors) to ensure that attribute verification does not expose true values; In the identity verification stage, users submit fake identity identifiers, verification codes, and zero knowledge proofs to the service platform. The latter calls on the on chain contract to verify the legitimacy, and verifies identity associations through elliptic curve encryption, generating unlinkable nullifierHash and uploading it to the chain to prevent duplicate verification; During the certificate revocation phase, the regulatory center marks the VC status as invalid through the Revoke contract to achieve certificate lifecycle management. This solution integrates blockchain immutability, zero knowledge proof privacy protection, and homomorphic encryption anti cracking capabilities, providing an efficient, decentralized, and compliant identity authentication solution for supply chain finance.

3.3 Zero knowledge identity authentication mechanism and performance evaluation supported by blockchain

The ZK-SCFI scheme proposed in this article implements distributed identity authentication through a five stage process: in the system initialization stage, the regulatory center generates elliptic curve (ECC) encryption parameters and large prime numbers, constructs homomorphic encryption (Paillier) key pairs and EdDSA signature keys, and the service platform synchronously generates ECC public and private keys and blockchain account addresses with users; During the credential application stage, users submit their identity information to the regulatory center. The center constructs a MerkleRoot attribute based on the MerkleTree, combines timestamp signatures to generate verifiable credentials (VC) and hidden identity credentials (HIC), and maps the VC digest and status to the blockchain; In the zero knowledge credential generation stage, the service platform designs a Merkle tree verification logic that includes arithmetic constraint circuits (C1 to C3), compiles and generates proof keys (PK) and verification keys (VK), deploys smart contracts, and users generate zero knowledge proofs through PK combined with privacy inputs (such as pseudo identity factors) to ensure that attribute verification does not expose true values; During the identity verification phase, users submit a false identity identifier (FDID), verification code (Code), and zero knowledge proof to the service platform. The latter calls the on chain contract to verify the legitimacy of the proof, and at the same time, verifies the identity association through elliptic curve encryption, generates unlinkable nullifierHash, and puts it on the chain to prevent duplicate verification; During the certificate revocation phase, the regulatory center marks the VC status as invalid through the Revoke contract to achieve certificate lifecycle management. The security of the scheme is guaranteed through five aspects: Merkle root signature verification and authentication factor signature verification to ensure unforgeability; Users can selectively disclose attribute information to avoid full exposure; Paillier encryption generates pseudonymous IDs to achieve unlinkability; Unique digital identity identifier and high-strength encryption to prevent impersonation attacks; The immutability of blockchain combined with hash storage of Merkle root values can resist replay attacks. In terms of performance evaluation, the experiment was conducted based on Solidity smart contracts, Circom circuit compiler, and Ganache private chain environment. Time cost analysis showed that Merkle existence verification, due to the use of MIMC hash algorithm, had significantly lower time consumption in each stage compared to EdDSA signature verification; Circuit comparison shows that the ZK-SCFI scheme, due to the use of Circom's built-in EdDSA algorithm, has lower time costs for compiling circuits, generating CRS, and calculating

proofs compared to the ECDSA based scheme; According to the statistics of Gas transaction costs (as shown in Table 1),

Table1. GAS Consumption and Cost Analysis for ZK-SCFI Smart Contracts

Function	GAS Consumption	ETH Spent	USD Cost
GetVC	1,239,481	0.0033465987	$6.48
Upload	507,244	0.0013695588	$2.65
Verifier	409,770	0.0011063790	$2.14
Revoke	256,997	0.0006938919	$1.34
Total	2,415,492	0.0065164284	$12.61

The headquarters deployment cost is $12.6118, with the GetVC contract having the highest GAS consumption due to its involvement in dynamic array storage, but overall it is within an acceptable range. The experimental results show that the ZK-SCFI scheme has high efficiency while ensuring security, meeting the identity authentication requirements of supply chain finance.

4 Results and discussion

4.1Improving the System Model of CP-ABE Data Sharing Scheme

This system consists of six types of entities, with the Supervision Center (SV) serving as a fully trusted entity responsible for system initialization (defining attribute sets, generating global parameters and master keys) and user private key generation; The data owner (DO) encrypts financial data with symmetric keys and uploads it to IPFS, while defining access policies to control file sharing; Data visitor (DV) obtains attribute private keys from SV based on their own attribute set, and can decrypt files when they comply with the access policy; Cloud servers (CS) provide partial decryption services to alleviate the burden on users; The InterPlanetary File System (IPFS) stores encrypted data files to alleviate the storage pressure of blockchain; Blockchain (BC) stores keyword indexes (including file identifiers, descriptions, and policy ciphertexts), utilizing immutability and distributed consensus to ensure data integrity and verifiability. The system includes 10 core algorithms: Setup (SV execution) takes in the security parameter λ and the attribute set U, outputs the global parameter PP and the master key MSK; KeyGen (SV execution) inputs PP, MSK, user attribute set S, and ID, outputs attribute key SK, conversion key TKID, L, and search private key SKu; OffEncrypt (DO execution) takes in the symmetric key and outputs the ciphertext CT of the file; OnEncrypt (DO execution) takes in PP, symmetric key, search token, access policy, and keyword set W, generating ciphertext CT and keyword index I; Trapdoor (DV execution) takes in the search private key SKu and keyword set W ', generating trapdoor TD; Search (CS execution) takes in keyword index I and trapdoor TD, verifying consistency (output 1 or $\perp$); Trans (CS execution) inputs the conversion key TKID, L, and ciphertext CT. If the attributes match the access policy, it outputs the conversion ciphertext IC. Decrypt (DV execution) inputs the attribute key SK and the conversion ciphertext IC, decrypts to obtain the symmetric key and search token; Identify (SV execution) inputs PP and conversion private key TKID, L, verifies legality, and outputs user identification ID. Revoke (SV execution) inputs user identification ID and parameter table T, generates new ciphertext to revoke user permissions. The security model adopts the Selective Keyword Attack (CKA) security model, which defines the interaction process between adversary A and challenger C. In the initial stage, A submits the access policy, and in the system setting stage, C generates the common parameter PP and delivers it to A. In the first query stage, A sends the attribute set S multiple times to obtain the private key SK. In the challenge stage, A selects keywords W1 and W2, and C randomly selects b $\in$ {0,1} to encrypt Wb and send the index to A. In the second query stage, A continues to execute the key query, and finally A outputs a guess

about b. Its victory advantage is defined as:

$$\mathrm{Adv_A} = \left|\Pr[b' = b] - \frac{1}{2}\right| \quad (1)$$

4.2 Model experiment

This article conducts a multidimensional performance analysis of the TRU-SABE data sharing scheme, covering functional characteristics, computing/storage overhead, IPFS file transfer performance, and blockchain throughput, and compares it with existing schemes in reference. Functional analysis shows that the TRU-SABE scheme performs excellently in terms of access structure flexibility (supporting LSSS matrix), keyword search, revocability, traceability, and outsourced decryption functions. Only this scheme possesses LSSS structure, keyword search, user tracking, and outsourced decryption capabilities simultaneously, and the efficiency of bilinear pairing based on prime number groups is better than that of composite number group schemes in the literature.In the comparison of computation and storage costs, the computation cost during the initialization phase is comparable to that in the literature, while the key generation is slightly increased due to the user tracking function; In the encryption stage, the LSSS structure has high overhead, but the efficiency of trapdoor generation, search, and decryption stages is significantly optimized, especially by outsourcing decryption to reduce the user side overhead to 3TE. In terms of storage, the common parameter (PK) and master key (MSK) are similar to those in the literature, and the attribute key (SK) and ciphertext (CT) factor group structure have obvious advantages, which are superior to the composite order group scheme in literature .Experimental verification is based on JPBC library and A-type prime order bilinear group (Zp=160 bits, G=512 bits), with parameter ranges $S \in [10,50]$, $d \in [1,10]$, and $I \in [10,50]$. The results showed that the initialization and key generation time increased linearly with the number of attributes, but significantly better than the literature; In the encryption stage, the LSSS structure has a faster increase in overhead, but more flexible access control has been achieved; The comparison scheme of trapdoor generation and search time efficiency is superior, and stable and low-cost decryption is achieved through semi decryption on cloud servers during the decryption stage.

In IPFS performance testing, the upload/download time of 5MB-100MB files is positively correlated with file size, and the download efficiency is significantly higher than the upload efficiency. The blockchain throughput test was conducted using Caliper tool in the FISCO BCOS network. Under a concurrency gradient of 10-100, the query operation throughput linearly increased to 97.8 TPS, and the write operation remained stable at 137.16 TPS under concurrency of 70-100; Write performance is limited by consensus mechanisms, while query performance depends on node hardware and network quality. Overall, the TRU-SABE solution demonstrates outstanding performance in terms of functional completeness, computational efficiency, and system scalability, providing an efficient solution for secure sharing of financial data.

4.3 Effect analysis

This article focuses on the financing scenarios in the field of supply chain finance and constructs a blockchain based financial data sharing system for small and medium-sized enterprises, aiming to prevent data leakage risks and improve supply chain collaboration efficiency through a controlled sharing mechanism. The system is implemented on the FISCO BCOS 2.0 consortium blockchain platform, using a combination of on chain and off chain storage solutions: blockchain stores key data such as financial file summaries and keyword indexes, IPFS stores encrypted contract financing file ciphertexts, and MySQL and Redis are used to assist in data exchange. The system architecture is divided into five layers (Figure 1)

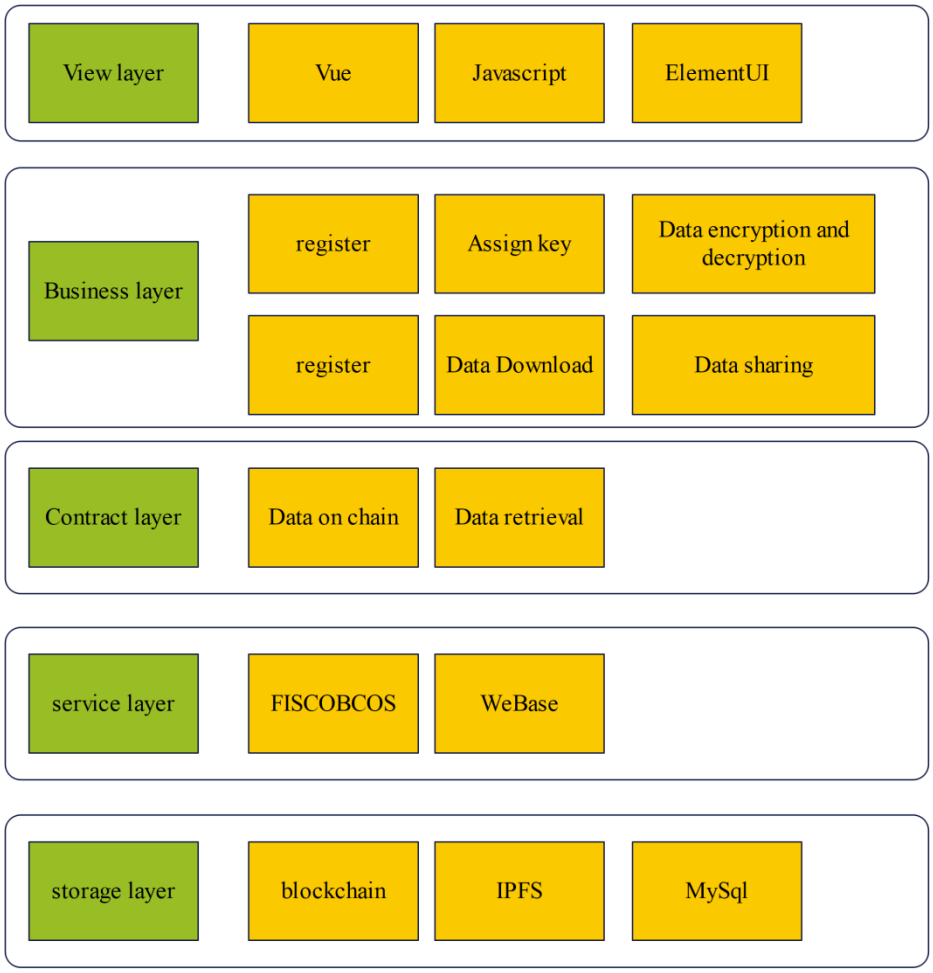

Figure 1 System Architecture Diagram

The view layer is built on Vue.js and ElementUI to create a responsive interactive interface; The business layer implements core logic such as attribute key generation, data encryption and decryption, uploading and downloading; The contract layer uses smart contracts to store data summaries, add keyword indexes, and retrieve ciphertext; The service layer relies on FISCO BCOS and WeBASE middleware to achieve blockchain interaction; The storage layer integrates the distributed storage capabilities of blockchain and IPFS. The system functions are divided into system management module and data sharing module. The system management module supports user registration and login as well as blockchain account generation. Users need to obtain external account addresses, public and private keys, and identity identifiers through smart contracts for their first login. The data sharing module includes four sub functions: the regulatory center generates attribute private keys and searches for private keys based on user attributes; The data owner (service platform) encrypts the financial data symmetrically and uploads it to IPFS, and builds a keyword index to be uploaded on the chain; Data visitors can decrypt and obtain semi decrypted ciphertext by matching the blockchain index through search trapdoors and complying with the access policy; Ultimately achieve data download and complete decryption. The system environment deployment is based on Ubuntu 20.04 and Windows 11, using Java (backend) and Solidity (smart contract) development languages. Blockchain deployment builds a four node consortium chain by modifying the FISCO BCOS configuration file and launching the WeBASE management interface. IPFS adopts the Kubo implementation version, which ensures the normal operation of distributed storage networks by initializing node services through IPFS init and starting node services through IPFS

daemon.

5 Conclusion

Supply chain finance, as a key tool for the coordinated development of industrial chains in the digital economy era, faces challenges such as centralized storage of identity authentication and the lack of data sharing mechanisms, as well as innovative opportunities in technologies such as blockchain and homomorphic encryption. This article focuses on the core issues of identity authentication and data sharing. Firstly, the research status of identity authentication and attribute based encryption (CP-ABE) is systematically reviewed, and the theoretical foundations of cryptographic tools such as Paillier homomorphic encryption, zero knowledge proof, and bilinear mapping are summarized; Secondly, a zero knowledge authentication scheme ZK-SCFI based on Merkle tree and Paillier encryption was designed, which achieves user privacy protection and transaction irrelevance through pseudo identity generation and on chain and off chain collaborative verification; Once again, a traceable, revocable, and searchable outsourced decryption attribute based encryption scheme TRU-SABE was proposed, which combines blockchain to ensure data immutability, alleviates storage pressure through IPFS, and verifies its efficiency advantages in terms of computational and storage costs; Finally, based on the Fisco Bcos consortium chain, Spring Boot backend, and Vue.js frontend, a financial data sharing system was built that includes basic functions such as identity registration and data encryption upload/download, providing technical support for the secure circulation of supply chain financial data.

The outlook section points out that there are still limitations in current research: identity authentication schemes need to explore user behavior supervision mechanisms on the basis of privacy protection; The attribute private key length and centralized management issues of data sharing schemes need to be optimized through a multi authority key generation mechanism; The system needs to further expand its visual interface and advanced authorization functions. Future research will focus on balancing privacy and regulation, optimizing key management, and deepening system functionality to promote the dual improvement of supply chain finance security and efficiency.

References

[1] Li, W. (2025). Discussion on Using Blockchain Technology to Improve Audit Efficiency and Financial Transparency. Economics and Management Innovation, 2(4), 72-79.

[2] Wu, H. (2025). The Commercialization Path of Large Language Models in Start-Ups. European Journal of Business, Economics & Management, 1(3), 38-44.

[3] Wang, C. (2025). Exploration of Optimization Paths Based on Data Modeling in Financial Investment Decision-Making. European Journal of Business, Economics & Management, 1(3), 17-23.

[4] Cai, Y. (2025). Research on Positioning Technology of Smart Home Devices Based on Internet of Things. European Journal of AI, Computing & Informatics, 1(2), 80-86.

[5] Cui, N. (2025). The Practical Application of Traffic Flow Forecasting and Capacity Analysis. Journal of Computer, Signal, and System Research, 2(5), 65-71.

[6] Zhang M. Discussion on Using RNN Model to Optimize the Accuracy and Efficiency of Medical Image Recognition[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 66-72.

[7] Wei, X. (2025). Practical Application of Data Analysis Technology in Startup Company Investment Evaluation. Economics and Management Innovation, 2(4), 33-38.

[8] Pan, H. (2025). Development and Optimization of Social Network Systems on Machine Learning. European Journal of AI, Computing & Informatics, 1(2), 73-79.

[9] Huang, J. (2025). Reuse and Functional Renewal of Historical Buildings in the Context of Cultural Heritage Protection. International Journal of Humanities and Social Science, 1(1), 42-50.

[10] Huang, J. (2025). Promoting Cross-field E-Commerce Development by Combining Educational Background and Technology. Economics and Management Innovation, 2(4), 26-32.

[11] Li, B. (2025). Research on Data-Driven Environmental Policy in Water Resource Management. European Journal of Public Health and Environmental Research, 1(1), 101-107.

[12] Ye, J. (2025). Optimization and Application of Gesture Classification Algorithm Based on EMG. Journal of Computer, Signal, and System Research, 2(5), 41-47.

[13] Hu, Q. (2025). Implementation and Management of a Cross-Border Tax System Oriented Towards Global Tax Administration Informatization. Economics and Management Innovation, 2(4), 94-101.

[14] Lu, C. (2025). The Application of Point Cloud Data Registration Algorithm Optimization in Smart City Infrastructure. European Journal of Engineering and Technologies, 1(1), 39-45.

[15] Han, Wenxi. "The Practice and Strategy of Capital Structure Optimization under the Background of the Financial Crisis." European Journal of Business, Economics & Management 1, no. 2 (2025): 8-14.

[16] Xu Q. AI-Based Enterprise Notification Systems and Optimization Strategies for User Interaction[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 97-102.

[17] Jing, X. (2025). Research on the Application of Machine Learning in the Pricing of Cash Deposit Products. European Journal of Business, Economics & Management, 1(2), 150-157.

[18] Hao, L. (2025). Research on Perception and Control System of Small Autonomous Driving Vehicles. International Journal of Engineering Advances, 2(2), 48-54.

[19] Liu X. The Role of Generative AI in the Evolution of Digital Advertising Products[J]. Journal of Media, Journalism & Communication Studies, 2025, 1(1): 48-55.

[20] Tang X, Wu X, Bao W. Intelligent Prediction-Inventory-Scheduling Closed-Loop Nearshore Supply Chain Decision System[J]. Advances in Management and Intelligent Technologies, 2025, 1(4).

[21] Wu X, Bao W. Research on the Design of a Blockchain Logistics Information Platform Based on Reputation Proof Consensus Algorithm[J]. Procedia Computer Science, 2025, 262: 973-981.

[22] Hui X. Medical Entity Recognition Based on Bidirectional LSTM-CRF and Natural Language Processing Technology and Its Application in Intelligent Consultation[J]. 2025, 6(1),1-8

[23] Zhu P. Construction and Experimental Verification of Automatic Classification Process Based on K-Mer Frequency Statistics[C]//The International Conference on Cyber Security Intelligence and Analytics. Cham: Springer Nature Switzerland, 2024: 391-400.

[24] Liu B. Data Analysis and Model Construction for Crew Fatigue Monitoring Based on Machine Learning Algorithms[J]. optimization, 2024, 8(5): 48-52.

[25] Xu Q. Design and Future Trends of Intelligent Notification Systems in Enterprise-Level Applications[J]. Economics and Management Innovation, 2025, 2(3): 88-94.

[26] Zhang Y. Research on Optimization and Security Management of Database Access Technology in the Era of Big Data[J]. Academic Journal of Computing & Information Science, 2025, 8(1): 8-12

[27] Liu F. Research on Supply Chain Integration and Cost Optimization Strategies for Cross-Border E-Commerce Platforms[J]. European Journal of Business, Economics & Management, 2025, 1(2): 83-89.

[28] An, C. (2025). Exploration of Data-Driven Capital Market Investment Decision Support Model. European Journal of Business, Economics & Management, 1(3), 31-37.

[29] Yang D, Liu X. Collaborative Algorithm for User Trust and Data Security Based on Blockchain and Machine Learning[J]. Procedia Computer Science, 2025, 262: 757-765.

[30] Zhu, Z. (2025). Application of Database Performance Optimization Technology in Large-Scale AI Infrastructure. European Journal of Engineering and Technologies, 1(1), 60-67.

[31] Jing X. Real-Time Risk Assessment and Market Response Mechanism Driven by Financial Technology[J]. Economics and Management Innovation, 2025, 2(3): 14-20.

[32] Zhu, Z. (2025). Cutting-Edge Challenges and Solutions for the Integration of Vector Database and AI Technology. European Journal of AI, Computing & Informatics, 1(2), 51-57.