Scholar Publishing Group
International Journal of Business Management and Economics and Trade
https://doi.org/10.38007/IJBMET.2025.060115
ISSN 2790-0959 Vol. 6, Issue 1:149-159

Research on Secure Data Notarization and Access Control Algorithms for Supply Chain Finance Based on an On-Chain/Off-Chain Hybrid Storage Architecture and Smart Contracts

Meng Liu

School of Economics, Wuhan Donghu College, Wuhan 430212, Hubei, China

Keywords: Supply Chain Finance; Blockchain; On-Chain/Off-Chain Storage; Smart Contracts; Data Notarization.

Abstract: As a key bridge between the real economy and financial capital, supply chain finance generates core data such as transaction documents, logistics information, and financing contracts, whose secure, trustworthy, and controllable management is crucial. Traditional centralized notarization schemes suffer from single points of failure, risks of data tampering, and high trust costs. Although blockchain offers tamper-evident notarization, limited on-chain storage and throughput constrain its direct use in large-scale data scenarios. To address this tension, this paper investigates a secure data notarization and access control algorithm grounded in an on-chain/off-chain hybrid storage architecture and smart contracts. We first construct a layered data management model: high-value, low-volume data hashes (digital fingerprints) and key access-control policies are anchored on-chain to ensure immutability, while complete large-volume raw data are encrypted and stored off-chain (e.g., in IPFS or distributed databases) to ensure scalability. To tackle potential challenges of on-/off-chain consistency and integrity verification under this hybrid architecture, we design an efficient verification mechanism based on cryptographic commitments, ensuring any tampering with off-chain data can be detected quickly and succinctly. Furthermore, to achieve fine-grained privacy protection and compliant use, we propose a smart-contract-based dynamic access control algorithm. By deploying access-control policies as executable code on-chain, the algorithm performs automated logical checks to deliver precise authorization and comprehensive audit logging, ensuring security and transparency throughout data sharing and circulation. Through theoretical security analysis and prototype experiments, the proposed scheme preserves data immutability and traceability while significantly improving the storage efficiency and processing performance of supply chain finance notarization systems, and it enables flexible and secure access control. The results indicate that the coordinated mechanism of on-chain/off-chain hybrid storage and smart contracts offers a feasible technical pathway for building efficient, trustworthy, and secure supply chain finance infrastructure.

1. Introduction

Based on traditional supply chain finance models, financial institutions typically rely on centralized systems to manage financing, transaction, and logistics information. However, as small and medium-sized enterprises (SMEs) become increasingly pivotal within supply chains, the challenges facing traditional financing models — such as information asymmetry, financing difficulties, and low managerial efficiency—have become more apparent. As a decentralized trust mechanism, blockchain shows great potential for improving data transparency and reducing trust costs. Nevertheless, existing blockchain solutions in supply chain finance still face performance bottlenecks, especially limitations in data storage and processing capacity, making it difficult to support efficient notarization and access control for large-scale supply chain data.

Although an on-chain/off-chain hybrid storage architecture offers a path forward, two key challenges remain in its implementation: first, how to ensure the integrity of off-chain data and enable efficient verification to prevent inconsistencies between on-chain notarization and the actual state of off-chain data; second, how to design flexible, fine-grained access control in a decentralized environment that safeguards data privacy while avoiding new single points of failure and privacy leakage. Existing research often concentrates on a single layer and struggles to address these two issues in a coordinated way.

To address these challenges, this study designs and implements a secure data notarization and access control solution for supply chain finance based on an on-chain/off-chain hybrid storage architecture and smart contracts. Specifically, we first propose a data integrity verification mechanism based on cryptographic vector commitments, which can efficiently and accurately verify the integrity of off-chain data and ensure consistency between on-chain and off-chain states. Secondly, this paper designs a dynamic access control algorithm based on smart contracts. The algorithm writes the access rules directly into the blockchain, achieves precise authorisation through the logic of automatic execution, and records every access trace completely. In addition, we experimentally verify that the scheme improves the storage and processing efficiency of the system while guaranteeing data security and trustworthiness.

This research not only provides a set of innovative technical frameworks for the digital transformation of supply chain finance, but also provides a feasible practical path for the secure storage and management of large-scale data, laying the foundation for building a more efficient, secure, and trustworthy supply chain finance system. The next chapters will proceed sequentially, detailing the data integrity verification mechanism, the specific design and implementation of the smart contract access control algorithm, the experimental validation results and their potential application value.

2. Related Research

Blockchain technology can effectively improve the data security and management efficiency of supply chain finance, so it has attracted much attention from academia and industry in recent years.Javaid M. et al. [1] point out that, by strengthening data authenticity, security, and risk management, blockchain is driving financial service providers to adopt smart contracts to improve transactional efficiency and transparency, while demonstrating transformative potential in core processes such as asset ownership transfer. Building on this, Gong Y. et al. [2] conduct a systematic survey of the intersection between blockchain and supply chain finance, summarizing the challenges of traditional models, key factors influencing blockchain adoption, and existing solutions —thereby laying a framework foundation for deeper research in this field.

At the system-architecture level, Fernández-Iglesias M. J. et al. [3] focus on blockchain-based traceability systems. By comparing the advantages and disadvantages of (i) anchoring hash-based proofs on-chain versus (ii) placing full datasets on-chain, they offer key design insights for balancing scalability, data privacy, and storage cost. To further address blockchain performance bottlenecks, Xu C. et al. [4] propose the SlimChain system, which employs a stateless design with off-chain storage and parallel processing. This significantly reduces on-chain storage overhead and increases transaction throughput, providing an important technical pathway for high-performance blockchain storage solutions.

Finally, Lin S. Y. et al. [5] provide a systematic review of smart-contract technical models, operating principles, and applications across multiple domains, and analyze the technical challenges they face[6]. The above research results cover various aspects of financial applications, cross-domain convergence, system architecture[7], performance optimisation and core key technologies, which provide a good foundation for this paper to construct the on-chain-off-chain hybrid storage model and design the access control algorithm for smart contracts, as well as an important methodological reference[8].

2. Design and Implementation of the Secure Notarization and Access Control Mechanism

2.1. System Architecture and Security Model

In order to realise the credible deposit and secure sharing of sensitive data in supply chain finance, this paper designs a mechanism that combines on-chain and off-chain storage and is managed by smart contracts. The mechanism maintains data tampering and full traceability while considering the system's scalability and fine-grained privilege control, and its core architecture contains four logical levels[9].

At the storage level, the system adopts a layered strategy to balance efficiency and security[10]. The on-chain portion uses the alliance chain network to store streamlined metadata, including important information such as data hash commitments, access policy summaries, and audit logs; while raw business data, such as transaction credentials, contract documents, etc., are kept in authorised cloud storage or distributed file systems under the chain. Such a hybrid design not only takes advantage of the blockchain's tamper-resistance, but also significantly reduces the burden of on-chain storage. Further, the data layer organises the on-chain deposited information by constructing Merkle trees, and introduces vector commitment techniques to generate concise commitment values for off-chain data. These methods can achieve efficient integrity verification of large-scale data and establish a reliable data foundation for multi-party collaboration.

The contract layer is the core of the system, like a brain that runs automatically. It leverages a variety of smart contracts to fulfil its functions, including a deposit contract for registering and validating data, a control contract for managing data access rights, and an audit contract for recording all operations. These contracts work together to automate processes such as deposit, authorisation and auditing. They help to standardise the management of data throughout its lifecycle, and also reduce the risks that can be associated with human action through rules for code execution. At another level, the application layer provides users with an intuitive and easy-to-use interface. Through it, supply chain participants can upload data, apply for permissions or query information; regulators also have an independent audit portal to facilitate the monitoring of processes, thus meeting the practical needs of compliance regulation.

To ensure the security of the above architecture, we establish a security model based on the principle of trust minimization. This model assumes that off-chain storage nodes are semi-trusted entities, meaning that while they execute storage tasks according to protocol, they may attempt to access the contents of the data. The blockchain network itself, however, is equipped with Byzantine

fault tolerance. The security objectives of the system encompass four aspects: data integrity, provenance authenticity, access controllability, and privacy protection. Specifically, business data are stored off chain by the data owner, with cryptographic commitments generated on chain for notarization; the off-chain storage provider responds to data requests and produces proofs of possession; data users must pass smart-contract-based authorization checks before gaining access credentials; and regulators can perform look-through audits based on on-chain logs. The collaborative relationships and verification processes among these participants are intuitively illustrated in the system model shown in Figure 1.

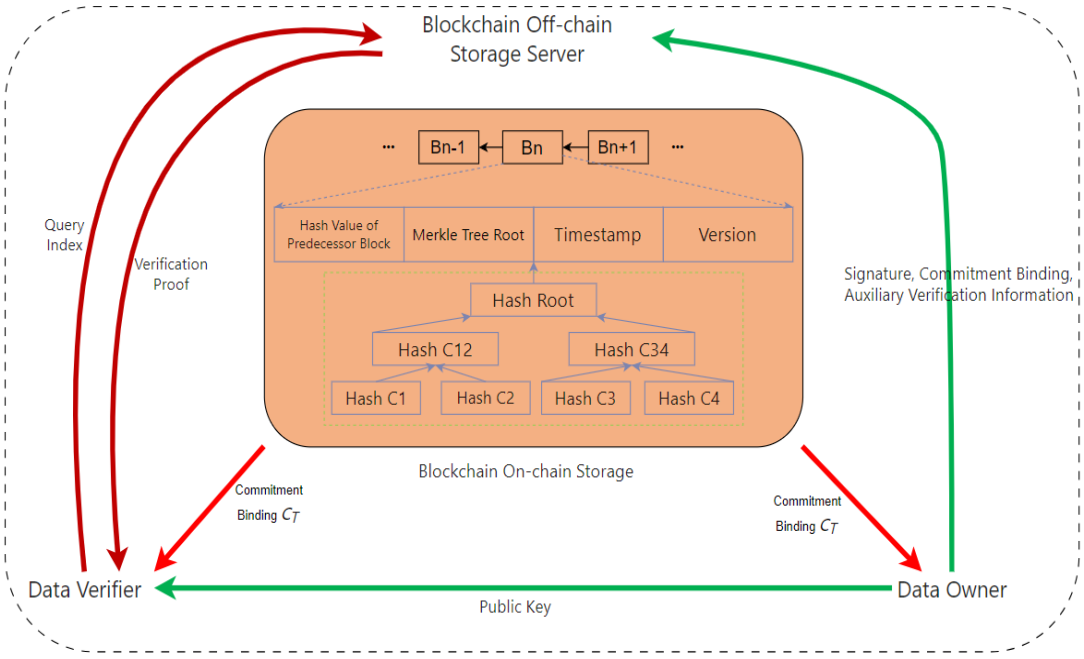

Figure 1. On-chain/Off-chain Collaborative Data Storage Model for Supply Chain Finance

This security model is further validated through a formalized experiment. After generating key pairs and deploying contracts during the system initialization phase, an adversary is allowed to perform a polynomial number of notarization queries, token requests, and verification attempts. Ultimately, the adversary must not be able to forge valid access credentials or pass data verification through unauthorized means. Theoretical analysis shows that if any probabilistic polynomial-time adversary has only a negligible advantage in succeeding in this experiment, then the system meets the required security guarantees.This architecture and model lay a solid foundation for the subsequent integration of cryptographic components such as vector commitments and attribute-based encryption, thereby providing both theoretical assurance and a practical pathway for achieving secure and controllable management of the full lifecycle of supply chain finance data.

2.2. Core Algorithms and Protocol Construction

Building on the above architecture and security model, this section elaborates on the concrete implementation of the cryptographic components and the interactive protocols. With a clear system architecture and security model in place, we further explain the core cryptographic algorithms and interactive protocols upon which the achievement of the security objectives depends. These components constitute the technical backbone of the system, supporting the entire process from data notarization and integrity verification to dynamic updates and fine-grained access control.

Data notarization is the starting point of the system workflow. To maintain data verifiability while benefiting from the scalability of off-chain storage, the system adopts a sub-vector commitment scheme. The data owner regards the original business data as a vector and executes a commitment generation algorithm to produce a fixed-length cryptographic commitment. This promise has two key characteristics: binding, which means that it is not possible to make a promise with different content for the same piece of data; and brevity, which means that the promise itself is short, no matter how big the original data is. Afterwards, the promise is recorded on the blockchain and becomes a reliable basis for testing the integrity of the data. Instead, the raw data, as well as the additional information needed to generate the promise, is stored in a storage server under the chain. By doing so, it avoids the storage pressure of massive data directly on the chain, and also provides the possibility of subsequent rapid verification of the authenticity of the data.

When a validator needs to check whether a certain data is still intact, the system initiates an efficient validation process. The validator sends a request to the off-chain storage server indicating the location of the data to be checked. Instead of returning all the data, the server runs a proof generation algorithm that generates a concise proof for only the requested data fragment. The verifier then calls the verification algorithm to complete the check by combining the promised value stored on the blockchain, the data fragment obtained off-chain, and the corresponding proof. The algorithm utilises cryptographic methods such as bilinear pairing, and the verification result can directly reflect whether the data has not been tampered with since the deposit of the proof, thus providing the verifier with a reliable verification capability. Considering the dynamic update nature of supply chain financial data, the system also integrates a secure data update mechanism. When a data owner needs to modify a piece of data, he or she must first obtain a proof of its current state, and then call the commitment update algorithm to generate a new commitment that reflects the change. To prevent malicious tampering, the system will digitally sign the update operation along with the number of times and the old promise to form an update credential. The smart contract will verify the validity of the credentials, and only after the verification is passed, the commitment on the chain can be updated. This ensures that the whole process of data changes is authentic, trustworthy and traceable. In terms of access control, the system combines attribute-based encryption and smart contracts to achieve finer-grained privilege management. Data owners can flexibly set access policies and store the encrypted data under the chain. The access control smart contract is responsible for enforcing the policy and issuing access credentials. Data users need to prove to the contract that they have the attributes to meet the policy requirements in order to obtain authorisation to decrypt and access the data under the chain. All access behaviours are recorded by the auditing contract, forming a complete set of closed loop of authority management and security auditing, which provides a strong guarantee for data privacy.

In order to make the system run more efficiently, especially in batch auditing scenarios where a large amount of data needs to be audited at the same time, the system is specially designed with a set of aggregation proof protocols.This protocol allows multiple independent proofs for different data positions to be aggregated into a single, compact proof. Smart contracts can execute the key steps of the aggregation algorithm, enabling the verifier to complete the validation of multiple data items in a single operation. This design significantly reduces communication and computation overhead, thereby greatly improving the practicality of the system when handling large-scale data verification tasks.

Through the precise construction of the above core algorithms and protocols, the proposed scheme endows the on-chain/off-chain hybrid storage model with strong cryptographic security properties. As a result, supply chain finance data, while benefiting from efficient storage, achieves a level of trustworthiness and controllability comparable to that of native on-chain storage.

3. Theoretical Security Analysis and Experimental Validation

3.1. Theoretical Security and Correctness Proof

The credibility of a scheme is rooted in its rigorous theoretical foundation. This section aims to demonstrate, starting from formalized security definitions and through logically sound reasoning, that the proposed scheme achieves both security and correctness under the established security model. The analysis shows that the scheme's security properties can be reduced to a set of well-studied classical cryptographic hardness assumptions.

In order to prove the security of a scheme, the first step is to express the security objectives in a clear and unambiguous way. According to the security model described earlier, the scheme has to fulfil two key requirements, namely, to guarantee data integrity and to achieve controlled access. As far as data integrity is concerned, it requires that any adversary within reasonable computing power will not be able to gain a significant advantage in a particular 'game'. The rules of this 'game' are that the adversary can query the 'tools' for data authentication and verification at any time according to his or her own strategy. When the queries are almost complete, the adversary will eventually have to produce a valid proof of the integrity of the data that has never been queried before, and this proof will have to be able to pass the checks of the validation algorithms that we have set up.Similarly, access controllability requires that even after obtaining partial access tokens, the adversary cannot forge a valid token that grants access to data for which they have no authorization.

The security of the proposed scheme is not without foundation; its robustness is built upon well-established cryptographic hardness assumptions. Specifically, the sub-vector commitment scheme underpinning the data notarization and verification mechanism derives its position-binding security property from the hardness of the Computational Diffie–Hellman (CDH) assumption. This implies that if an adversary were able to successfully compromise data integrity (i.e., forge a proof that passes verification), then one could construct an algorithm that, with non-negligible probability, solves the CDH problem. Since the CDH problem is widely regarded as computationally intractable in appropriate groups, our scheme can therefore resist integrity-related attacks. Meanwhile, the introduction of commitment-binding techniques effectively prevents forward automatic update attacks, with security relying on the existential unforgeability of the digital signature scheme employed. These further anchors system security to another well-established cryptographic assumption.

For access control, security is guaranteed by the formal definitions of the adopted attribute-based encryption (ABE) scheme. Its security under chosen-plaintext attacks (CPA) is typically reducible to hardness assumptions such as the Decisional Bilinear Diffie–Hellman (DBDH) assumption or the linear assumption. As an incorruptible policy enforcer, the smart contract ensures transparency and fairness of access control logic through its deterministic execution of code, thereby avoiding the single point of failure and potential abuse risks inherent in centralized authorization servers. All authorization checks and token issuance records are anchored on chain, forming an undeniable audit trail.

The correctness proof concerns whether the scheme can realize its intended functions under honest execution. For the data notarization and verification protocol, correctness requires that as long as all parties execute the protocol honestly, any proof generated by an honest off-chain storage server for valid data must be accepted by the verification algorithm. This requires algebraic derivations to directly show that the verification equation always holds. For example, in the sub-vector commitment scheme, one must rigorously prove that substituting an honestly generated commitment, data subset, and its corresponding proof into the verification equation guarantees its

satisfaction. This property is inherent to the design of the scheme itself and does not rely on any computational assumption, thereby ensuring intrinsic reliability. By the same token, for an access control mechanism to be ‘no problem’, it has to fulfil the requirement that a data user can only successfully decrypt the data and get the correct access if his qualifications (e.g. permissions, identity, etc.) are fully compliant with the set access rules; if they don't comply with the rules, they won't be able to decrypt and access it. If a smart contract is to be ‘error-free’, it relies on its professionally verified (e.g., checked in a rigorous way) or rigorously tested code logic -- which ensures that it will strictly follow the existing state on the blockchain and the input parameters, and execute the rules that have long been set up It's not going to change them.

In summary, by reducing the scheme’s higher-level security properties to the hardness of fundamental cryptographic problems, and by rigorously validating the functional correctness of its core components, the theoretical security of the proposed solution is systematically demonstrated. This provides a solid theoretical foundation for the experimental validation presented in the next section, showing that the design is not only intuitively secure but also formally robust in the cryptographic sense.

3.2. Experimental Performance Evaluation and Comparative Analysis

From the theoretical level, the security of the programme is a solid foundation for it to be trusted; and when it comes to the actual use of the scenario, whether it is good or not, and whether it can work or not, is the key to determining whether it has any practical value. To comprehensively evaluate the performance of the proposed solution, we constructed an experimental testing environment that closely approximates realistic deployment conditions. We then conducted a systematic comparative analysis against existing representative schemes, considering multiple dimensions such as computational overhead, communication efficiency, and scalability.The experimental setup was designed to reflect the typical conditions of consortium blockchain deployments. On-chain components were deployed in a consortium blockchain test network composed of multiple nodes, with smart contracts executed in an Ethereum Virtual Machine (EVM)-compatible environment. Off-chain storage servers and clients were configured using standard commercial server hardware. Industry-standard cryptographic libraries (e.g., the PBC library for bilinear pairing operations) were employed to implement the core cryptographic algorithms, and operation runtimes were precisely measured across different data scales.

Performance evaluation first focused on the computational cost of core operations. Results show that during the data notarization phase, the cost for the data owner to generate vector commitments grows linearly with the size of the data vector—an expected result. As this operation can typically be performed offline, its impact on system responsiveness is minimal. Of greater practical relevance is the performance during the verification phase. Experimental results indicate that data integrity verification by the verifier requires only sub-millisecond execution time and is nearly independent of the total volume of off-chain stored data. This constant-time verification overhead is critical, as it enables even resource-constrained lightweight nodes to efficiently participate in data auditing, thereby greatly enhancing the applicability of the scheme.

To further illustrate the benefits of batch processing, we compared single-record operations with batch-processing modes. When handling large numbers of queries or update requests, batch processing demonstrates significant efficiency gains. For example, when simultaneously verifying ten data records, the total time required under batch verification is substantially less than the sum of ten independent verifications. This improvement stems primarily from the aggregation-proof protocol, which consolidates multiple proofs into a single computation, thereby amortizing fixed costs and significantly reducing system stress under high-concurrency auditing scenarios.

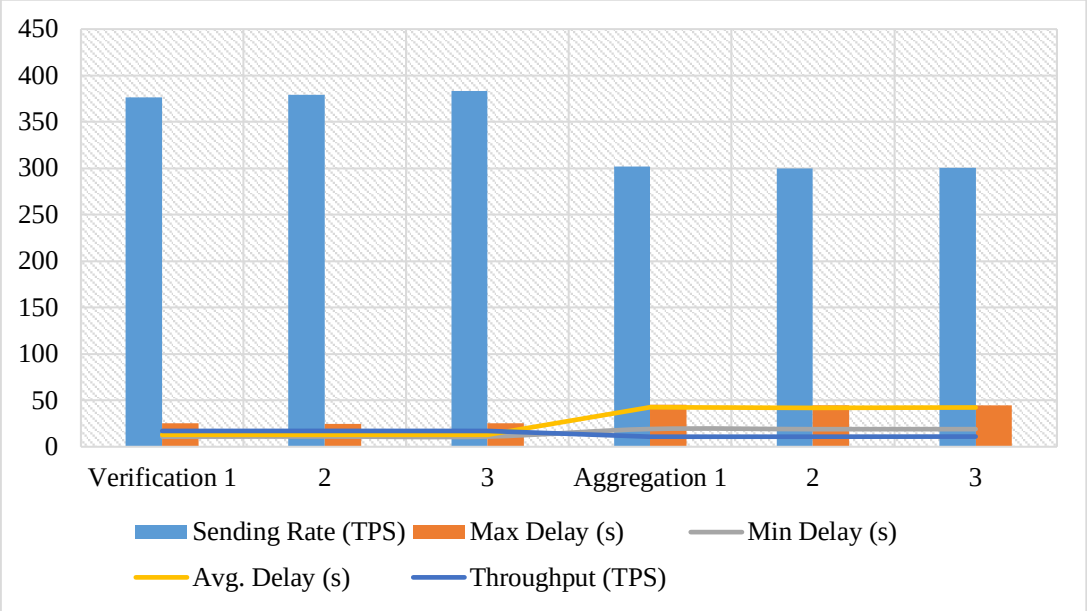

Figure 2. Performance Comparison of Core Operations

As shown in Figure , under high transmission pressure with a sending rate approaching 400 TPS, the verification operation demonstrates stable performance, with an average latency of about 13 seconds and a throughput stabilized at around 17 TPS. This reflects the system’s capability to handle high-frequency single verification requests. By contrast, under a sending pressure of approximately 300 TPS, the aggregation operation exhibits relatively higher average latency, but its throughput remains around 11 TPS. This confirms the effectiveness of the aggregation mechanism in high-concurrency batch scenarios. Although a single aggregation request requires longer processing time, the overall computation and communication overhead is significantly reduced through proof consolidation. This enables the system to effectively avoid sharp performance degradation when faced with a large number of concurrent auditing demands, which is consistent with the previously discussed advantages of batch processing.

In terms of communication overhead, the proposed scheme demonstrates particular advantages. Since only fixed-length commitments are stored on chain, rather than parameters that grow linearly with the data volume, both the system initialization phase and subsequent data updates incur significantly reduced on-chain communication costs. Compared with schemes that require uploading large verification parameters to the blockchain, our approach achieves notable improvements in communication efficiency, which directly alleviates network congestion and reduces transaction fees.Furthermore, we conducted a horizontal comparison of the proposed scheme with several representative existing data notarization approaches. The comparison metrics included on-chain storage cost, single verification time, support for batch verification, and capability for dynamic updates. Comprehensive analysis reveals that while maintaining a comparable level of security to state-of-the-art schemes, the proposed solution demonstrates distinct advantages in verification efficiency and support for dynamic data operations. Especially in the scenarios of ‘handling complex data queries’ and ‘validating a large amount of data at once’, this solution achieves the function of ‘aggregated validation’ with the help of smart contracts. -- In short, it integrates multiple validation requirements for efficient processing, which effectively solves the problem that some solutions in such scenarios are ‘stuck and have a huge performance drop’.

Combining theoretical analysis and practical experimental results, this solution has successfully found a good balance between data security, operational efficiency and practicality. The data from the experiments also fully proves the conclusion that this kind of storage and access control method with on-chain and off-chain coordination not only ensures security at the theoretical level, but also can operate efficiently and adapt to more business scenarios in practice, which is especially suitable for the business needs of supply chain finance, which are "dealing with a large amount of readily-changing data, and often need to verify and access by authority. " business needs. This also provides reliable proof of technical feasibility for it to be used in real business scenarios.

4. Conclusion and Outlook

This study focuses on the important demand for data security management in the field of supply chain finance, and deeply analyses the problems of insufficient storage and low operational efficiency encountered in the practical use of blockchain technology. The core of the problem to be solved is the key issue of ‘how to make a large amount of business data efficiently stored, easily retrieved, and controllably shared under the premise of guaranteeing data security and no loss of trustworthiness’, and then proposed and constructed a set of mechanisms combining the two storage methods of on-chain and off-chain, and then cooperating with the smart contract to collaborate in the management.

The main contributions and findings of this paper can be summarized in three aspects. First, at the system architecture level, a layered collaborative data management model is designed. By anchoring lightweight metadata such as data integrity commitments on the blockchain while storing raw data off chain, this model skillfully balances the tension between blockchain’s immutability and storage scalability. Second, at the algorithmic level, advanced cryptographic primitives are innovatively integrated with smart contracts. In particular, sub-vector commitments enable efficient verifiable notarization and dynamic updates of data; attribute-based encryption combined with smart contracts realizes fine-grained and auditable access-control protocols; and the further design of an aggregation-proof mechanism significantly improves system throughput in batch data verification scenarios. Third, through rigorous formal security proofs and experimental performance evaluations, the effectiveness of the scheme is validated both theoretically and empirically. The analysis demonstrates that the scheme’s security can be reduced to classical computational hardness problems, while experimental results confirm that it achieves notable advantages in verification efficiency, communication overhead, and batch processing capability—meeting the real-time, high-frequency auditing requirements of supply chain finance.

Despite these achievements, several areas remain open for further exploration and refinement. Looking ahead, future research may proceed along the following directions: (i) Enhanced privacy protection. While the current scheme ensures data integrity and access controllability, future work may explore integrating privacy-preserving technologies such as zero-knowledge proofs and secure multi-party computation, enabling data validation and compliance auditing without disclosing sensitive business information (e.g., transaction amounts or supplier identities). (ii) Optimization and extension of access-control models. Research may focus on more flexible policy description languages and more efficient attribute revocation mechanisms to better accommodate the complex and evolving collaboration relationships in supply chains. Meanwhile, blockchain could be further leveraged as the underlying infrastructure for decentralized identity and trusted credentials, enabling cross-organizational identity interoperability and collaborative management. (iii) Deeper integration with real-world business scenarios. In the future research, this scheme can be further combined with the Internet of Things, electronic signature and other systems to achieve automatic verification of trade background and real-time uploading of asset data, and gradually build a credible supply chain

finance system from the starting point to the end point.

This study provides a practical technical path for data security deposit and controllable sharing in supply chain finance. With the increasing maturity of blockchain and other related technologies, as well as the deepening integration with different fields, this blockchain-based data governance model is expected to play a role in more industrial financial scenarios, providing support for the establishment of a transparent, efficient, and credible digital economic environment.

References

[1] *Zhou, Y. (2025). Improvement of Advertising Data Processing Efficiency Through Anomaly Detection and Recovery Mechanism. Journal of Media, Journalism & Communication Studies, 1(1), 80-86.*

[2] *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*

[3] *Huang, J. (2025). Research on Cloud Computing Resource Scheduling Strategy Based on Big Data and Machine Learning. European Journal of Business, Economics & Management, 1(3), 104-110.*

[4] *Liu, Y. (2025). The Importance of Cross-Departmental Collaboration Driven by Technology in the Compliance of Financial Institutions. Economics and Management Innovation, 2(5), 15-21.*

[5] *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).*

[6] *Xu, H. (2025). Research on the Implementation Path of Resource Optimization and Sustainable Development of Supply Chain. International Journal of Humanities and Social Science, 1(2), 12-18.*

[7] *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.*

[8] *Zhang, Xuanrui. "Automobile Finance Credit Fraud Risk Early Warning System based on Louvain Algorithm and XGBoost Model." In 2025 3rd International Conference on Data Science and Information System (ICDSIS), pp. 1-7. IEEE, 2025.*

[9] *Xu, H. (2025). Optimization of Packaging Procurement and Supplier Strategy in Global Supply Chain. European Journal of Business, Economics & Management, 1(3), 111-117.*

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

[11] *Chang, Chen-Wei. "AI-Driven Privacy Audit Automation and Data Provenance Tracking in Large-Scale Systems." (2025).*

[12] *Zhang K. Research on the Application of Homomorphic Encryption-Based Machine Learning Privacy Protection Technology in Precision Marketing[C]//2025 3rd International Conference on Data Science and Network Security (ICDSNS). IEEE, 2025: 1-6.*

[13] *Truong T. The Research on the Application of Blockchain Technology in the Security of Digital Healthcare Data [J]. International Journal of Health and Pharmaceutical Medicine, 2025, 5(1): 32-42.*

[14] *Gao Y. Research on Risk Identification in Legal Due Diligence and Response Strategies in Cross border Mergers and Acquisitions Transactions [J]. Socio-Economic Statistics Research, 2025, 6(2): 71-78.*

[15] Li W. Building a Credit Risk Data Management and Analysis System for Financial Markets Based on Blockchain Data Storage and Encryption Technology[C]//2025 3rd International Conference on Data Science and Network Security (ICDSNS). IEEE, 2025: 1-7.

[16] Zhang, Xuanrui. "Automobile Finance Credit Fraud Risk Early Warning System based on Louvain Algorithm and XGBoost Model." In 2025 3rd International Conference on Data Science and Information System (ICDSIS), pp. 1-7. IEEE, 2025.

[17] 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.

[18] Zhou Y. Cost Control and Stability Improvement in Enterprise Level Infrastructure Optimization [J]. European Journal of Business, Economics & Management, 2025, 1(4): 70-76.

[19] Li, W. (2025). Research on Optimization of M&A Financial Due Diligence Process Based on Data Analysis. Journal of Computer, Signal, and System Research, 2(5), 115-121.

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

[21] 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.

[22] 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.