

From Cumbersome Processes to Automatic and Reliable: The Mechanism and Path of Blockchain Enabling Financial Document Management

Mingye Liu

*School of Economics and Management, China University of Petroleum (Beijing), Beijing, China
lmy_astolpho@163.com*

Abstract. Corporate financial voucher management suffers from redundant processes, poor multi-party collaboration, and high audit costs. In traditional models, voucher pass through handling, cashiering, accounting, and banking—each step fragmented and manual, raising error and fraud risks. Blockchain's decentralization, immutability, traceability, and smart contract automation offer a viable path to rebuild voucher storage and transmission. This paper focuses on mid-to-large-value, multi-party voucher scenarios requiring high traceability and audit verification (e.g., cross-enterprise procurement, large-contract settlements, and pre-IPO audits), proposing a hybrid architecture: on-chain evidence storage as the core trusted anchor, with originals and human oversight entrusted off-chain. Grounded real-world circulation challenges, this paper designs a collaborative model for enterprises, banks, tax authorities, and auditors. Key mechanisms include hash-based evidence anchoring, digital signatures, smart contract payments, ERP system integration, permission and privacy control, exception handling, and version management. This paper evaluates the model's impact on audit efficiency and internal control compliance. The study concludes that blockchain is not a simple replacement but a catalyst for efficiency and trustworthiness through a "on-chain storage + off-chain execution + manual confirmation" hybrid framework. Furthermore, this paper provides implementation recommendations regarding legal adaptation, system integration, performance costs, and security governance, alongside future research directions.

Keywords: Blockchain, Corporate Finance, Audit

1. Introduction

In corporate finance, original vouchers are the legal basis for recording transactions and assigning economic responsibility. Standard procurement payments typically undergoes multiple stages—business handling, cashiering, accounting, and banking—each requiring repeated reviews and manual information transfer. Although this reflects internal control principles like segregation of duties and layered auditing, it creates efficiency bottlenecks, information silos, and risks of tampering, loss, or delay, raising audit costs. Blockchain offers high application value and broad developmental prospects in traditional financial sectors such as auditing and accounting. It

introduces a new technical paradigm to resolve existing dilemmas [1, 2]. Its automated scripting system supports sophisticated smart contracts, currencies, or other decentralized applications [3]. Core features—including distributed ledgers, hash-linked structures, consensus mechanisms, and smart contracts—are inherently suited for multi-party voucher evidence storage and circulation scenarios. By digitizing paper-based instruments, blockchain enhances transmission efficiency, storage security, and retrieval convenience, thereby improving overall societal operational efficiency. It also enables real-time risk detection, strengthening risk management in the bill market [4]. Moreover, blockchain-based electronic invoices eliminate paper printing, promoting green economic development and carbon neutrality goals [5].

Accordingly, this paper focused on mid-to-large-value, multi-party voucher scenarios requiring robust traceability and audit verification (e.g., cross-enterprise procurement with frequent reconciliation, large-contract settlements, and pre-IPO audits). It proposes a principle-driven architecture: using on-chain evidence storage as the trusted anchor while retaining original documents and manual control off-chain, thereby achieving process optimization without compromising existing internal controls or legal validity. Specifically, the model design in this paper preserves the storage of paper or certified electronic originals and adopts PKI digital signatures in accordance with current accounting and electronic signature regulations, ensuring the legal admissibility of the on-chain mechanism.

2. Pain points of traditional voucher processes and the blockchain response

2.1. Process fragmentation and information asymmetry

In traditional models, voucher-related information is fragmented across internal corporate systems (e.g., ERP systems and paper documents), banks (receipts and statements), taxation authorities (invoice systems), and transaction counterparties (contracts and delivery notes). The absence of a unified, trusted data-sharing mechanism among these disparate systems necessitates repetitive retrieval and verification during reconciliation and auditing. For instance, bank receipts are typically downloaded or printed by cashiers and manually handed to accountants for matching against accounting vouchers, causing significant delays and risks such as receipt loss or mismatch with corresponding vouchers.

Blockchain provides a shared, append-only ledger accessible to all participants. As critical financial infrastructure, it can reshape credit mechanisms, lower transaction costs, and mitigate moral hazard, exerting broad impact across the financial sector [6]. By serving as nodes on a consortium blockchain, banks, enterprises, tax authorities, and auditors can upload hash values or summary information of key vouchers. This enables real-time, cross-party verification of data integrity and timestamps, eliminating information asymmetry. However, on-chain data credibility hinges on the verifiability of underlying off-chain sources. To address this, our model integrates multiple off-chain verification mechanisms to ensure uploaded data is authentic and reliable.

2.2. Manual dependency and operational risk

Despite the widespread adoption of financial software, critical steps—including the audit of original vouchers, review of accounting entries, and secondary payment confirmation—still rely heavily on manual judgment, thereby entailing subjective errors and moral risks. Smart contracts within the blockchain can codify rules such as contract terms and payment conditions. When the system detects that preset conditions—such as invoice issuance, delivery note upload, and bilateral digital signature

completion—have been met, it can automatically trigger the generation of accounting vouchers and payment instructions, thereby reducing unnecessary manual intervention.

However, it must be emphasized that smart contracts are not intended to replace compliance reviews by banks or accountants. Exception handling, manual arbitration, and rollback/compensation mechanisms must therefore be designed to ensure both compliance and security.

2.3. High costs of audit evidence collection

In traditional auditing processes, to verify the authenticity of transactions, auditors must trace multi-source information—including contracts, invoices, delivery notes, bank receipts, and accounting vouchers—and confirm that such data has not been tampered with. This process is not only time-consuming but also heavily dependent on the professional judgment of the auditors.

The hash-based evidence storage mechanism of blockchain provides an efficient verification method: enterprises calculate the hash value of original vouchers using a hash function and upload it to the blockchain. During an audit, recalculating the hash and comparing it with the on-chain record allows for a definitive determination of whether the document has been tampered with since the time of storage. However, hash verification primarily proves integrity and cannot independently verify the authenticity of the document at the time of upload; judging authenticity still requires integration with tax receipts, bank statements, third-party certifications, or manual verification. The data collection phase, which originally required seven days, has been shortened to just one day thanks to the automated data aggregation of on-chain records. Similarly, the verification process, which traditionally took five days, has been reduced to 0.5 days due to the immutability and cross-verifiability of the ledger [7].

3. Blockchain model design for voucher evidence storage and transmission

3.1. Overall architecture and participating roles

The model proposed in this paper adopts a consortium blockchain architecture, with the primary participants including: (1) Enterprises (Buyer and Seller): Both parties to the transaction utilize the blockchain platform to sign contracts, transmit delivery notes, and issue invoices. They also perform digital signature confirmation on the final consolidated voucher packages. (2) Banks: Banks provide fund payment services and digital receipts. As controlled participants or via specialized interfaces, they synchronize payment statuses and receipt summary information to the on-chain system while retaining final authority over fund execution and compliance review. (3) Tax Authorities: These entities verify the authenticity and status of invoice data through interfaces or regulatory channels, rather than participating directly in the on-chain consensus process as real-time operational nodes. (4) Audit Institutions: Serving as read-only or authorized nodes, audit institutions perform batch verification of voucher hashes stored on the chain and can retrieve original documents for in-depth inspection as required. (5) Blockchain Platform: This provides the underlying technical support, including smart contract execution, hash evidence storage, identity authentication (via PKI systems), permission management, and private data channels.

Furthermore, internal corporate ERP systems and tax information systems interact with the blockchain platform through APIs. They do not serve as direct on-chain consensus nodes; however, depending on governance requirements, they may opt to connect to specific permission layers.

3.2. Off-chain assurances for on-chain data credibility

The effectiveness of on-chain evidence storage depends on the authenticity of off-chain input data. To mitigate the risk of fraud prior to data upload, this model proposes the introduction of the following off-chain verification mechanisms as prerequisites for on-chain storage:

Proof of Origin: When uploading data, the data generator must simultaneously submit verifiable receipts or API responses from third parties, such as logistics providers, banks, or tax authorities.

Four-Eyes Review / Dual-Signature Mechanism: The on-chain submission of critical vouchers requires confirmation by two independent personnel or systems before it can be executed.

Third-Party Escrow or Regulated Distributed Storage: For high-risk originals or those required by regulation, copies are preserved via regulated third-party institutions or distributed storage systems, which provide timestamp certification.

These off-chain measures are integrated into smart contracts as triggering conditions or signature requirements, thereby enhancing the credibility of on-chain data at its source.

3.3. Core business processes: a case study of a typical procurement transaction

Contract Signing and on-chain Storage: The buyer and seller sign an electronic contract via the platform. The smart contract records key terms and uploads the contract hash to the blockchain, while simultaneously submitting proofs of origin or third-party receipts as trusted evidence.

Dispatch and Delivery Note: The seller uploads the delivery note and submits the logistics receipt. Upon the buyer's confirmation of receipt, the delivery note hash is stored on-chain.

Invoice Issuance and Verification: Based on the contract and delivery note, the seller issues an electronic invoice via the tax system. The invoice hash is uploaded to the blockchain, enabling real-time verification by tax authorities.

Automated Generation of Accounting Vouchers: Once the conditions for the contract, delivery, and invoice on-chain storage are met—and validated by proofs of origin—the smart contract automatically generates an accounting voucher for pre-entry into the ERP system. The voucher ID is then bound to the corresponding on-chain voucher hash.

Manual Audit and Digital Signature: Financial personnel review the entry within the ERP system and grant approval using a PKI-based digital signature. This signature is uploaded to the blockchain to serve as an internal control audit trail.

Payment Workflow and Bank Receipt: The smart contract triggers the payment request and authorization process. The bank node conducts a compliance pre-check and completes the fund transfer upon meeting regulatory and risk control requirements. The bank then uploads the receipt hash to the chain, while retaining final execution authority and the right to perform manual intervention for exceptions.

Voucher Package Integrity Archiving: The hashes of all original vouchers are aggregated via a Merkle tree. The resulting root hash is uploaded as the "fingerprint" of the voucher package; any subsequent modifications will result in a root hash mismatch, ensuring data integrity.

3.4. Voucher modification, revocation, and version control

Regarding scenarios such as invoice reversals (red-ink cancellations), corrections, or supplements, the model adopts a strategy of undeletable historical records paired with status change annotations. All corrections are recorded as new on-chain transaction events, capturing the operator's digital signature and a precise timestamp. Smart contracts manage the associative link between the original

voucher and its subsequent corrections, enabling the audit process to simultaneously verify both the initial records and the correction history, thereby fulfilling archival retention and traceability requirements.

3.5. Detailed explanation of key mechanisms

(1) Hash Chaining for Evidence Storage and Privacy Control: To prevent privacy leakage and storage bloating, the full text of original documents is not stored on-chain; instead, only hashes and essential metadata are recorded. The model employs hash functions with secret parameters, which are transmitted via trusted channels such as Quantum Key Distribution (QKD) or quantum-encrypted communication. By leveraging the principles of quantum physics to guarantee the confidentiality of these secret parameters, the system can resist potential attacks from both classical and quantum computers [8]. The original files are retained by the enterprise or stored using an encrypted distributed file system (e.g., IPFS combined with cryptographic key management). To prevent the misuse of hashes for correlation attacks, sensitive files can be processed with a random salt or a regulated timestamp service prior to on-chain storage. In specific scenarios, privacy-enhancing technologies such as Zero-Knowledge Proofs (ZKP) may also be introduced.

(2) Mart Contract-Driven Payment, Accounting, and Exception Handling: Smart contracts are designed as tools for automated triggering and compliance pre-checking, incorporating exception handling, compensatory transaction logic, and manual arbitration channels. Prior to triggering a payment, the system performs account balance checks, Anti-Money Laundering (AML) screenings, and blacklist comparisons; if an anomaly is detected, execution is suspended and approval personnel are notified. In the event of contract execution failure, the system triggers compensation logic or records pending events to ensure traceability and recoverability. On the blockchain, banks function solely as recipients of instructions, retaining final execution authority and uploading the bank receipt hash only after completing off-chain compliance inspections.

(3) Internal Control Design with Manual Confirmation Retention: To balance operational efficiency with internal control requirements, manual review by financial personnel and Public Key Infrastructure (PKI) digital signature links are retained following the automated generation of accounting vouchers. Vouchers that have not undergone manual confirmation remain in a pre-entry state and are prohibited from entering the official accounting ledgers or the payment execution workflow. This design adheres to the principle of segregation of incompatible duties and mitigates the risk of erroneous execution inherent in automated processes.

(4) Simplification and Boundaries of Audit Sampling: Audit institutions can retrieve the root hash list of on-chain voucher packages and perform hash comparisons on sampled or full datasets to achieve efficient integrity verification. However, a clear distinction must be made between integrity verification and authenticity verification: while hash comparison proves that the data has not been tampered with since the moment of evidence storage, the verification of its authenticity still requires integration with tax receipts, bank statements, third-party certifications, or manual inspections. The model significantly reduces the workload of manual sampling through the linkage of on-chain hashes and multi-institutional node data; however, it does not advocate for the total replacement of substantive authenticity investigations.

4. Implementation challenges and strategies

4.1. Legal and regulatory adaptation

Integrating native blockchain mechanisms (e.g., smart contract execution and decentralized governance) with traditional legal oversight can bridge the gap between "code" and "law." This approach acknowledges the strengths of both systems while addressing their respective limitations [9]. Currently, judicial practice in China has progressively recognized the evidentiary validity of blockchain-based evidence storage in certain cases; however, whether the on-chain storage of financial vouchers meets the requirements of regulations such as the Administrative Measures for Accounting Archives remains to be further clarified. To achieve operational implementation, the following alignment measures are recommended:

Regarding "Original Document Preservation": In response to the requirements in the Administrative Measures for Accounting Archives, paper or certified electronic originals should be retained and periodically archived and countersigned by regulated third parties. On-chain hashes should serve as auxiliary proof rather than the sole evidence.

Regarding the Electronic Signature Law: The current Electronic Signature Law regulates certification service providers based on traditional electronic signature technology and architecture, which is difficult to apply to the operational mechanisms of blockchain. Consequently, separate chapters are needed to define the specific rights and obligations therein [10].

Regarding Judicial Admissibility and Tax Inspection: Communication with regulatory authorities should be established in advance to pilot data-sharing rules, and compliance review processes and law enforcement access channels should be integrated into the consortium governance.

Governance Constraints: The aforementioned measures should be incorporated into the consortium governance charter and participant agreements as mandatory constraints for compliance.

4.2. System integration and governance

The degree of interface standardization varies across corporate ERP systems, core banking systems, and taxation systems; thus, achieving automated interaction necessitates the unification of API specifications, data dictionaries, authentication protocols, and version management mechanisms. It is recommended that a consortium governance committee be established to oversee interface standards, certificate management, node admission, and upgrade strategies. Regarding the implementation path, a phased approach is advisable: initially achieving the automated on-chain storage of voucher hashes and their integration with internal ERP systems, followed by pilot connections to banking and taxation nodes, thereby gradually expanding the scope of participating entities.

4.3. Security and emergency governance

The implementation of the system must incorporate rigorous security governance for keys and nodes. Specifically, Hardware Security Modules (HSM) or entrusted Key Management Services (KMS) should be employed for private key storage, complemented by the establishment of comprehensive protocols for key rotation, backup, and loss recovery. Simultaneously, the consortium blockchain must implement node admission controls, periodic security audits, and continuous log monitoring. The governance charter should explicitly define mechanisms for

emergency response, arbitration, node penalties, and restoration to mitigate risks associated with private key loss, node compromise, or governance failure.

5. Future research directions

This paper primarily completes the conceptual design and mechanistic analysis of a blockchain-based voucher management model. Future research can be further deepened in the following directions:

Systematic Study on Legal and Regulatory Compliance: Systematically review regulations such as the Electronic Signature Law, the Administrative Measures for Accounting Archives, and the Provisions on the Administration of Blockchain Information Services. This aims to clarify the admissibility of this model in judicial evidence collection and tax inspections and to propose suggestions for legal revisions or supporting standards.

Empirical Field Surveys and Pilot Deployments: Conduct in-depth interviews or pilot deployments across enterprises of various industries and scales. This will facilitate an evaluation of the model's practical impact on the workload of financial personnel, approval efficiency, and internal control risks.

Prototype System Development and Testing: Develop a prototype system based on mainstream consortium blockchain open-source frameworks (e.g., FISCO BCOS, Hyperledger Fabric). This involves simulating the complete workflow—from contract signing to receipt archiving—to verify the correctness of smart contracts, the reliability of hash evidence storage, and the stability of API interactions.

Comparative Analysis with Traditional Auditing: Conduct quantitative comparisons within simulated or pilot environments using controlled variables. By applying both traditional sampling audits and blockchain-based hash evidence audits to the same set of vouchers, research can measure differences in time costs, human resources, and detection rates.

Research on Security Incident Response and Key Management Practices: Formulate emergency response procedures and liability attribution mechanisms for scenarios such as cross-institutional key failure or node compromise.

6. Conclusion

The essence of financial voucher management lies in the establishment of a credible recording and responsibility traceability mechanism among multiple parties. While traditional processes ensure security through hierarchical auditing and physical isolation, they do so at a significant cost to operational efficiency. Blockchain technology offers a novel equilibrium: it ensures data immutability through cryptographic evidence storage, enables automated conditional execution via smart contracts, and eliminates information barriers through shared ledgers.

The hybrid model proposed in this paper utilizes blockchain as a trusted anchor, migrating key steps—such as voucher hashing, signature confirmation, and smart contract triggering—to the chain. Simultaneously, it retains original document storage, manual auditing, and bank compliance execution off-chain. The credibility of on-chain data is further safeguarded by off-chain measures, including proof of origin, dual-signature mechanisms, and third-party escrow. This design balances efficiency, security, and compliance, offering the potential to significantly reduce auditing costs and enhance voucher circulation efficiency in scenarios involving mid-to-large-value transactions that require rigorous audit traceability. Looking forward, with further validation through pilot programs and clearer legal regulations, blockchain is poised to become a trusted infrastructure connecting

enterprises, banks, taxation, and auditing, driving the evolution of voucher management from cumbersome processes toward automated trustworthiness.

References

- [1] Huang, G.H. (2016) Research on Blockchain-Based Approaches for Integrated Audit Systems .Fiscal Science, (10): 84-91.
- [2] Yan, S. (2020) Prospects for the Application of Blockchain Technology in the Accounting Field. China Management Informationization, 23(07): 44-46.
- [3] Yuan, Y., Wang, F.Y. (2016) Blockchain: The State of the Art and Future Trends. Acta Automatica Sinica, (4): 481-494.
- [4] Guo, Y.R., Wei, S.S., Lin, K.J., et al. (2024) The Transformation of Financial Instruments Based on "5G + Blockchain" Technology: The Transition from Electronic Instruments to Digital Instruments. Modern Business, (14): 188-192.
- [5] Yuan, X.P., Wang, S.H., Wang, T., et al. (2021) Exploration of the Comprehensive Promotion and Application of Blockchain Electronic Invoices. Western Finance and Accounting, (05): 18-22.
- [6] Qiao, H.S., & Xie, S.S. (2017) Theoretical and Practical Analysis of Blockchain-Driven Financial Innovation. New Finance, (1): 45-50.
- [7] Zhou, X.Q., & He, M, Y. (2025) Impact of Blockchain Technology on Financial Management and Accounting Practices. Academic Journal of Science and Technology, 18(2): 40-47.
- [8] Liu, A., Wen, J., Xu, S.W., et al. (2024) A Comparative Research on Hash Function in Blockchain in the Post Quantum Era. Information Security Research, 10(3): 223-232.
- [9] Isik, A., Meryem, A., Eda, S, S., et al. (2026) Editorial: Blockchain, Web3, and the metaverse: legal, managerial, and financial pathways for future business and governance. Frontiers in Blockchain, 9: 1832534-1832534.
- [10] Zhang, Q.F. (2021) The Compatibility and Application Path of Blockchain with China's Electronic Signature Law. Journal of Fujian Police College, 180.