Blockchain-Based Multi-Chain Data Supervision Mechanism for Traditional Chinese Medicine Traceability System

Rongjun Chen[1], Yun Sun[2], Feng Xue[3], Yongzhi Ma[4],
Xinyu Wu[5], Xianxian Zeng[6], Jiawen Li[7]*, Jinchang Ren[8]*
School of Computer Science, Guangdong Polytechnic Normal University, Guangzhou, China[1,2,3,4,5,6,7,8]
School of Computing-Engineering and Technology, Robert Gordon University, Aberdeen, United Kingdom[8]

***Abstract*—Addressing the challenges of Traditional Chinese Medicine (TCM) traceability systems, including heavy data storage burdens, poor privacy protection, and susceptibility to tampering, this study establishes a highly secure and trustworthy traceability supervision system for the entire Chinese medicine supply chain, which enhances product quality and safety assurance. Centred on the Hyperledger Fabric consortium blockchain as its core architecture, a multi-chain integration framework comprising one regulatory main chain plus five organisational sub-chains is proposed to achieve permission control, data isolation, and privacy. A multi-mode encrypted data storage mechanism is designed, integrating China's national cryptographic algorithms SM4 and SM3 with CP-ABE attribute-based encryption to enable tiered management of private and non-private data. Zero-knowledge proof technology safeguards identity privacy during cross-chain data transmission, while QR codes and environmental data collection mechanisms enhance data entry efficiency and authenticity. The system achieves end-to-end traceability from cultivation and processing through transportation, warehousing, and sales. Comparative performance analysis shows that the proposed framework effectively alleviates data storage pressure, ensures data validity, enhances data security, and improves collaborative efficiency among organizations across the TCM supply chain. The proposed multi-chain integrated Chinese medicine traceability and supervision system enables efficient collaboration and trustworthy traceability across the entire Chinese medicine industry chain, while safeguarding data security and privacy, and has significant application and promotion value. Future integration with artificial intelligence and big data technologies could further enhance the system's intelligent analysis and decision-support capabilities.**

***Keywords*—Blockchain; traceability; multi-chain architecture; Hyperledger Fabric; Traditional Chinese Medicine**

I. Introduction

Several traditional Chinese herbal medicines have been demonstrated to modulate the growth, differentiation, invasion, and metastasis of Hepatocellular Carcinoma (HCC), which may be attributed to their capacity to regulate HCC progression [1]. Traditional Chinese Medicine (TCM) has considerable potential to address certain conditions that remain challenging for Western medicine. Nevertheless, current challenges in the TCM supply chain include unclear germplasm origins, genetic degradation of herbal species, pesticide residues, excessive levels of heavy metals, environmental contamination during harvesting and processing, and inadequate standardization in storage, transportation, and retail management. Therefore, it is necessary to establish a traceability system for traditional Chinese medicinal herbs that balances security and efficiency, enabling end-to-end tracking from cultivation to retail outlets, ensuring the quality of medicinal materials remains under control, and ensuring the safety of their use is traceable.

Existing blockchain-based traceability systems face significant limitations, including degraded performance as data volumes increase and insufficient data privacy, rendering them vulnerable to unauthorized tampering. For instance, Jamil et al. [2] pioneered the use of Hyperledger Fabric to record data in the pharmaceutical supply chain. Their system leveraged blockchain to log drug transactions, aiming to establish a smart healthcare ecosystem that addresses supply chain inefficiencies. While this approach capitalized on the decentralized nature of blockchain from a holistic supply chain perspective, it overlooked critical data-specific issues such as validity and privacy. Similarly, Agrawal et al. [3] proposed a blockchain-enabled network that enables manufacturers to monitor pharmaceutical products effectively throughout the supply chain, enhancing security and transparency. Although this solution improved data controllability, its oversight remained localized and failed to ensure comprehensive regulatory coverage across the entire supply chain.

To address these shortcomings in end-to-end traceability for Chinese herbal medicines, this study proposes a novel, high-security, multi-chain traceability and regulatory framework based on blockchain technology. The architecture consists of one regulatory main chain plus five organisational sub-chains, enabling multi-chain interaction and data fusion. Specifically, we adopt a permissioned consortium blockchain that incorporates the following key features: access control (only authorized participants can join and perform operations on the chain), consensus mechanisms (to guarantee node consistency), high performance and scalability (to meet industry-specific requirements), privacy preservation (to protect personal and commercial confidentiality of stakeholders), and customizability (to support future extensions) [4]. Furthermore, we implement a multi-modal data encryption and storage mechanism to enhance data security while reducing on-chain storage redundancy.

The structure of this study is as follows: Section II briefly introduces the core technology stack involved in this system. Section III presents the system design architecture and

*Corresponding authors.

highlights the core innovative components. Section IV details the system implementation. Section V conducts a comparative analysis of the system across different dimensions. Section VI concludes the study and outlines future directions.

II. Related Work

In recent years, with the frequent occurrence of food safety incidents and rising consumer demand for product transparency, traditional centralized database-based agricultural traceability systems have increasingly revealed critical limitations, including information silos, data tamperability, and a lack of trust. Blockchain technology, owing to its decentralization, immutability, and inherent traceability, has been widely adopted in supply chain traceability research across sectors such as agri-food, pharmaceuticals, and apparel. This study focuses on consortium blockchain-based system architectures. It provides a systematic review and critical analysis of recent representative studies, organized around three core dimensions: system architecture design, platform selection, and data storage with privacy preservation.

A. System Architecture Design: Consortium Blockchain

To overcome the performance, privacy, and controllability limitations of public blockchains, current research predominantly adopts consortium blockchain architectures to enable trusted data sharing among known participants. Hua et al. [5] proposed a three-role node model comprising a registration center, a data node, and a client that flexibly configures Byzantine Fault Tolerance or Paxos consensus algorithms in environments with identified stakeholders, supporting end-to-end traceability of agricultural products from cultivation to retail. Tseng et al. [6] leveraged the Gcoin consortium blockchain to assign unique digital identities to pharmaceuticals. They employed an anti-double-spending mechanism to detect duplicate circulation events, thereby aiding in the identification of counterfeit drugs. Sadri et al. [7] proposed a six-role permission model for blood supply chains, enforcing fine-grained access control to ensure operational compliance across the blood collection, testing, and transportation stages. Although Tsai et al. [8] addressed microfilm copyright protection rather than physical goods, their multi-chain parallel architecture, labeled ABC, TBC, MBC, demonstrated the scalability potential of consortium blockchains in high-concurrency scenarios. Collectively, these works illustrate that consortium blockchains, through participant restriction, enhanced permission management, and improved throughput, have become the prevailing architectural paradigm for high-assurance traceability systems.

B. Platform Selection: Hyperledger Fabric

Hyperledger Fabric has emerged as the preferred platform for traceability applications that require strong privacy and regulatory compliance, thanks to its modular design, channel architecture, pluggable consensus protocols, and fine-grained access control. Chen et al. [9] built a brand apparel anti-counterfeiting system on Fabric, utilizing ECDSA digital signatures and channel isolation to enable trustworthy data sharing across the entire supply chain from raw materials to retail, and to allow third-party arbitration entities to verify signatures and pinpoint falsification points hierarchically. Marchese et al. [10] introduced a dynamic rule engine in the agri-food domain, enabling regulators to inject specific compliance rules, such as temperature thresholds, into chaincode and automatically validate them upon batch registration, significantly enhancing regulatory compliance. Dong et al. [11] constructed a four-organization multi-channel Fabric network involving manufacturers, logistics providers, retailers, and regulators, integrating RFID tags with Golang-based chaincode to record and query food lifecycle data while ensuring enterprise data isolation. These studies consistently exploit Fabric's channel mechanism to achieve natural data partitioning: only authorized entities such as regulators can access cross-channel information, effectively balancing transparency with commercial privacy.

C. Data Storage and Privacy Protection: On-Chain Off-Chain Hybrid Architecture

Given the high storage costs and limited scalability of on-chain data, virtually all Fabric-based studies adopt a hybrid architecture in which only cryptographic hashes are stored on chain, while the original data resides off-chain. Chen et al. [9], Marchese et al. [10], and Dong et al. [11] all store primary business data, such as inspection reports, images, and contracts, in off-chain databases or on IPFS, recording only their hashes in the Fabric ledger. This approach preserves data integrity while mitigating blockchain bloat. Sensitive information, such as transaction prices and supplier identities, is encrypted using AES or ECC before being recorded on the chain, and Fabric's attribute-based access control enforces fine-grained permissions. Hua et al. [5] further recommended tiered authorization for critical operation logs, restricting data access and verification to designated roles. However, most studies inadequately address the availability of off-chain data. If an off-chain storage node fails, consumers may verify hash consistency but cannot retrieve the original content, which poses a risk of a null pointer exception.

Despite these advances in architectural design and privacy protection, several limitations remain. First, most existing Fabric-based systems rely on single-chain or multi-channel architectures and are therefore prone to storage bottlenecks and performance degradation as data volumes grow. Second, current hybrid storage schemes generally lack robust data-availability guarantees and fine-grained security control mechanisms. If an off-chain storage node fails or is maliciously tampered with, the original data may become unrecoverable, and traditional encryption approaches often incur risks of plaintext key storage on-chain or isolated key management off-chain. Third, cross-chain data interoperability and end-to-end regulatory capabilities remain insufficient, making it difficult to achieve truly comprehensive, end-to-end traceability. In addition, traditional non-blockchain traceability systems depend on centralized databases, which are inherently susceptible to data tampering, information silos, and the absence of a credible trust mechanism.

III. System Design

The proposed traceability and regulatory framework is built upon three key mechanisms. First, a multi-chain, integrated data supervision and transmission mechanism isolates organizational subchains, enabling end-to-end oversight while preserving the privacy of user accounts. Second, a multimodal

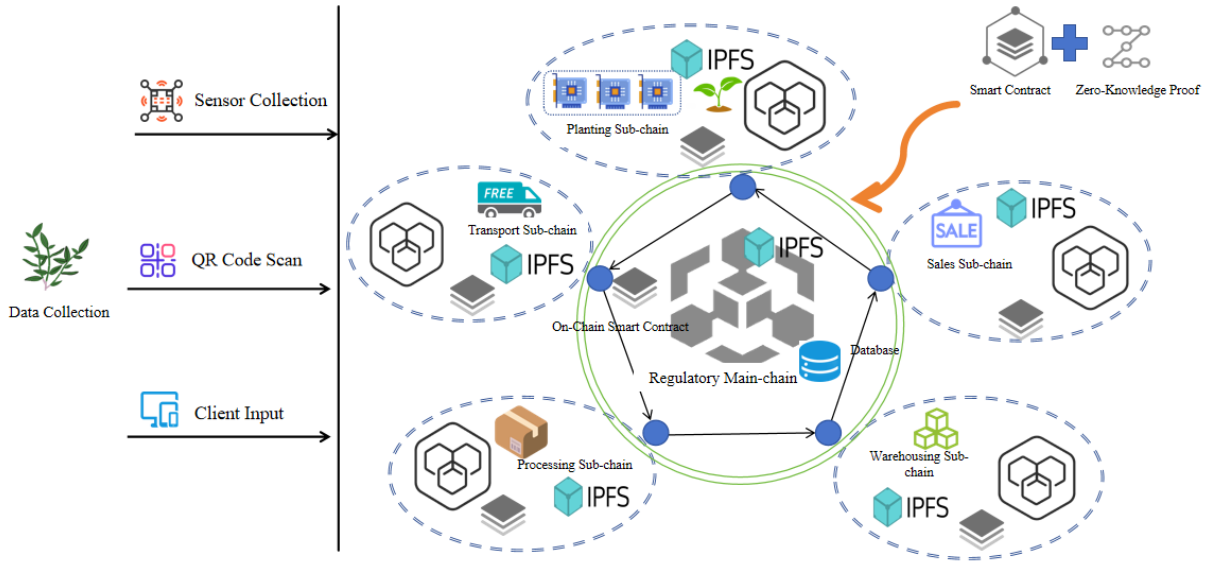

Fig. 1. Architecture diagram of a high-safety TCM traceability supervision system based on multi-chain fusion.

encrypted storage mechanism mitigates on-chain storage pressure, ensures strong data security, and supports fine-grained access control. Third, a QR code-based data entry mechanism, coupled with environmental data acquisition, enhances operational efficiency, safeguards user privacy, and ensures the validity of environmental data. Together, these mechanisms significantly improve inter-organizational collaboration and ultimately realize a highly secure, end-to-end traceability solution for the entire TCM supply chain. The overall architecture is illustrated in Fig. 1.

Five specialized sub-chains are defined: cultivation, transportation, processing, warehousing, and retail. The cultivation sub-chain, as the starting point of the supply chain, is responsible for recording detailed information on the cultivation of TCM materials. The transportation sub-chain records the movement of medicinal materials from planting sites to processing facilities, including transportation time, selected modes of transportation, and related logistics information. The processing sub-chain captures the processing of TCM materials, including the selection of processing methods, processing duration, and key process parameters. The warehousing sub-chain maintains information on the storage of medicinal materials in warehouses, including temperature and humidity conditions, storage duration, and inventory levels. The retail sub-chain records sales information, including the diversity of sales channels, the reasonableness of sales timing, and the stability of sales prices. Each organizational sub-chain thus records the key operational data of its own stage, and together the five sub-chains ensure that consumers can verify end-to-end information for each batch of Chinese medicinal products from growers to retailers.

A. Multi-Chain Integrated Data Supervision and Transmission Mechanism

As shown in Fig. 2, the system establishes a multi-chain integrated data supervision and transmission mechanism centered on the supervisory mainchain as the core hub, which connects downward to five operational subchains: cultivation, processing, transportation, packaging, and sales. All dynamic data must first undergo identity verification through a zero-knowledge proof-based authentication smart contract deployed on the supervisory main chain [12]. An operation permit is granted only upon successful verification. Subsequently, the main chain routes the relevant instruction, along with a hash digest, to the appropriate target sub-chain based on the business type, thereby implementing a closed-loop "verify before transmit" regulatory process. Sensor stream data and QR code scan records, classified as static data, are generated within each sub-chain. Since their authenticity has already been validated locally, they can be directly recorded in the respective subchain ledger. However, after block finalization, each sub-chain must periodically submit its block hash to the supervisory main chain to support global auditing. This mechanism effectively isolates direct interaction between sub-chains and end-user clients while ensuring end-to-end data trustworthiness, traceability, and privacy through centralized orchestration and backup coordination by the main chain.

B. Multi-Modal Encrypted Data Storage Mechanism

Building upon the aforementioned multi-chain organizational structure, this system addresses data security through a hybrid on-chain-off-chain multi-modal encryption and storage strategy. Data are classified according to sensitivity into privacy-sensitive and non-privacy-sensitive data, each assigned a tailored storage approach. As shown in Fig. 3, for privacy-sensitive data, the system employs the Chinese national cryptographic standard SM4 (formerly SMS4.0), a block cipher algorithm that offers high security and superior performance [13], to enhance both transmission efficiency and confidentiality. To protect the SM4 symmetric keys on the chain, the system adopts Ciphertext Policy Attribute-Based Encryption (CPABE) [14], in which user attributes, such as role or orga-

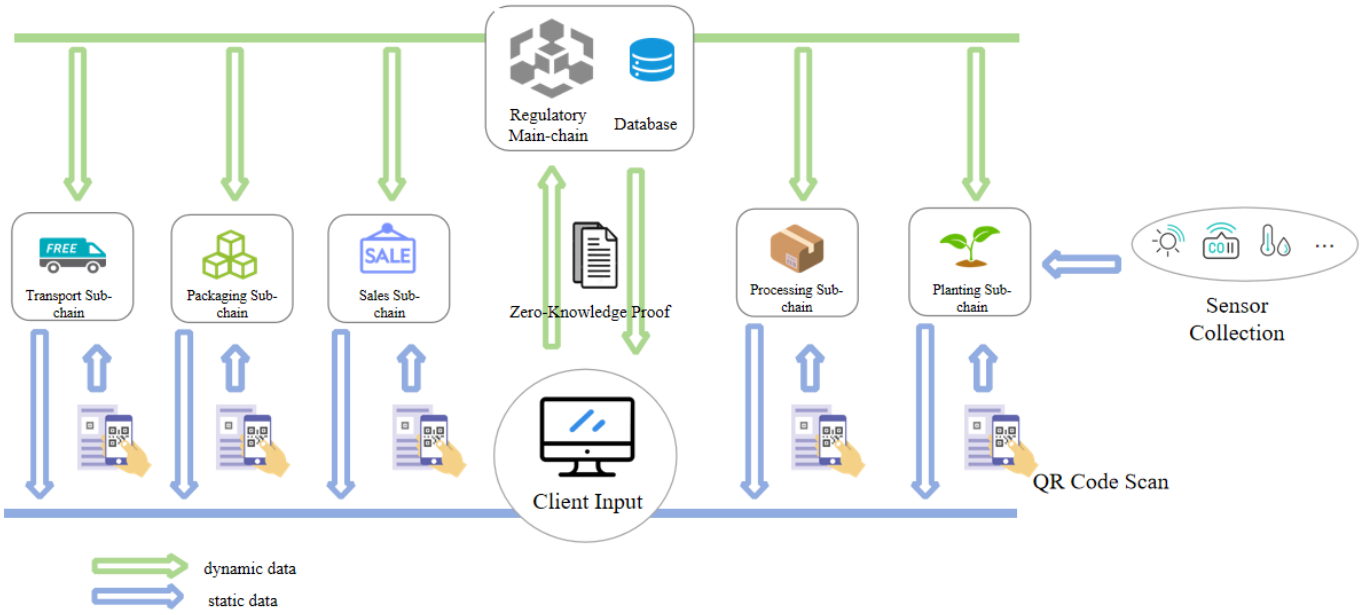

Fig. 2. A schematic diagram of the data regulatory transmission mechanism based on multi-chain fusion.

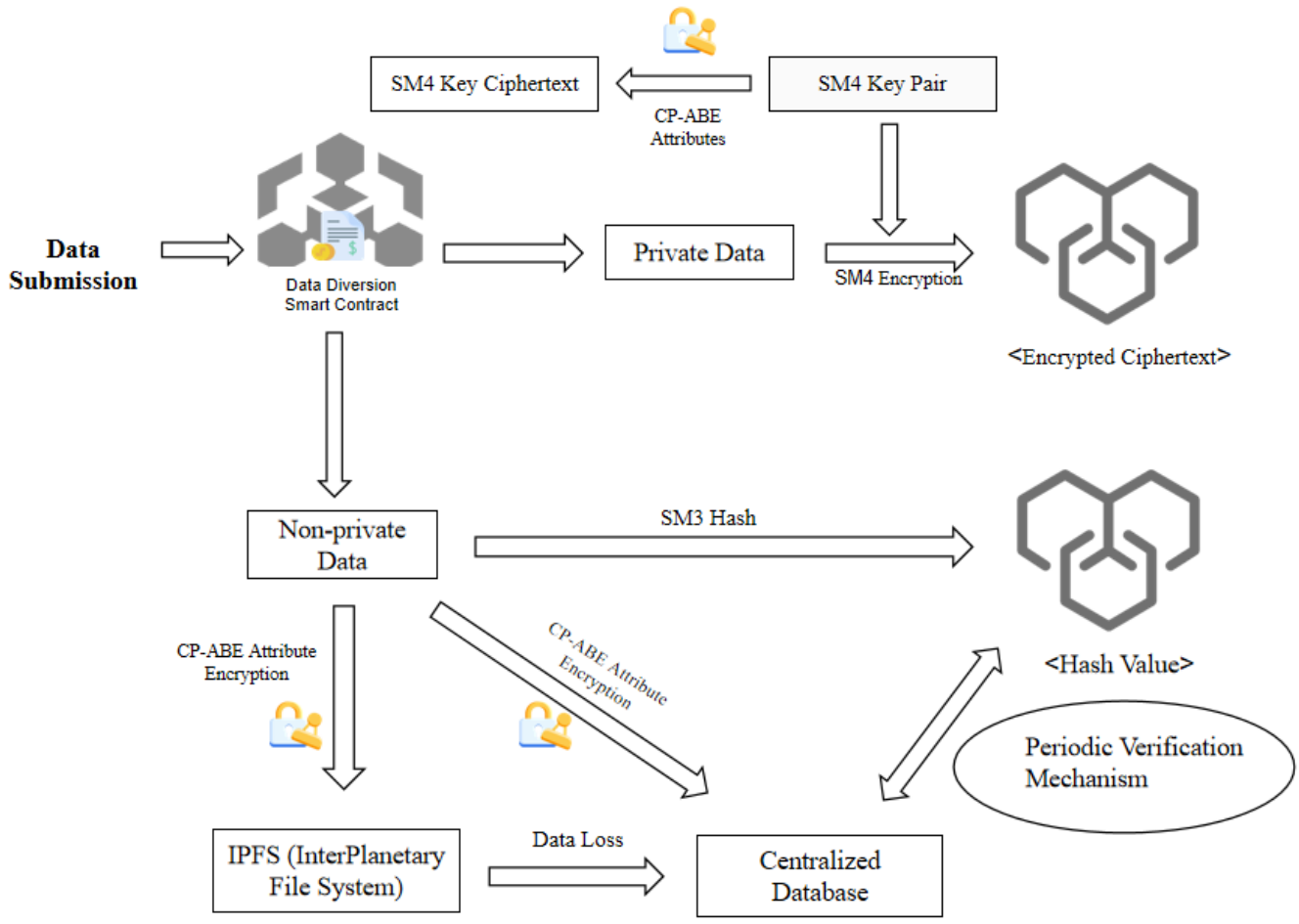

Fig. 3. Schematic diagram of data multi-mode encrypted storage.

nizational affiliation, serve as access policies. Compared with conventional symmetric or asymmetric encryption schemes, CPABE eliminates the risks associated with storing keys in plaintext on-chain or managing them in isolated off-chain repositories. Only users whose attributes satisfy the defined policy can decrypt and retrieve the SM4 key, thereby enabling fine-grained access control. For non-privacy-sensitive data, the system stores the original content in a centralized database to optimize read and write performance. Concurrently, it applies the SM3 cryptographic hash algorithm, a highly efficient national standard, to generate a digest of the data. This digest is then recorded on the corresponding sub-chain. A periodic verification mechanism between the sub-chain and the centralized database ensures the integrity and validity of the off-chain data. To further strengthen resilience against data loss or tampering, the system leverages the Inter Planetary File System (IPFS) [15] as a decentralized backup layer. If the periodic verification detects corruption, deletion, or unauthorized modification in the centralized database, the system automatically restores the affected data from the IPFS backup, ensuring continuous and reliable operation. Although the data shared within the system is accessible internally, external access remains strictly controlled. Therefore, all externally exposed data is encrypted using CPABE with a system-wide root Certificate Authority (CA) as the governing attribute policy. This configuration allows all authorized internal nodes to decrypt while denying access to external entities, thereby maintaining a robust security boundary between the internal consortium and the outside environment.

C. QR Code Generation and Environmental Data Acquisition Mechanism

In practical production scenarios, sub-chain personnel are frequently required to perform traceability-related operations, such as farmers applying fertilizer or irrigating. Conventional approaches, such as manual logbooks or direct client-side data entry, pose significant risks of information leakage or falsification. To address these vulnerabilities, the proposed design leverages the physical isolation property of QR codes. Specifically, a sub-chain user initiates a request via a dedicated mini program to the supervisory main chain, which then invokes a smart contract to generate a time-bound procedural QR code. This approach enhances both the security of traceability records and operational efficiency, as workers need only present the QR code to a scanning device. The scanner automatically captures the QR code content, appends a current timestamp and other contextual metadata, and uploads the complete record to the corresponding subchain for storage. Subsequently, a data-routing smart contract classifies and encrypts incoming data by type before storing it in the appropriate location. This mechanism assumes that all personnel affiliated with the organizational subchains have been pre-registered, with their relevant identity and role information securely collected and transmitted in advance to the supervisory main chain for encrypted storage as privacy-sensitive data. Upon completion of product packaging, the supervisory main chain receives a notification triggering the traceability query workflow. It then invokes a cross-chain traceability smart contract to aggregate traceability records associated with the product. Concretely, using the unique product traceability ID, the system queries and consolidates relevant data from cultivation, processing, transportation, and other pertinent subchains. The integrated traceability dataset is finally encoded into a QR code, known as the traceability information QR code, enabling end users to access a complete, verifiable history of the Traditional Chinese Medicine product with a simple scan.

IV. System Implementation

The chaincode implements the ChaincodeStubInterface to define multiple custom application functions, as listed in Table I. The planting sub-chain is specifically designed to monitor the seed growth environment, ensuring the validity of data submitted to the blockchain. The supervisory mainchain integrates information from all subchains to enable unified oversight and management. By continuously monitoring and analyzing data from all stages of the supply chain, the supervisory mainchain can promptly identify potential quality issues and safety hazards and initiate appropriate corrective actions. All operations executed by the chaincode generate transaction records stored on the blockchain, and any resulting state changes are updated in the state database.

Based on a multi-chain integrated architecture comprising one regulatory main chain and five organizational sub-chains, the system implements a unified identity verification process for all organizational logins. When a user accesses the login interface, the backend identifies the user's organizational affiliation based on their account credentials and directs them to the corresponding organization's main interface. This approach enhances security among organizations by requiring all inter-organizational data exchanges to request permission from the supervisory mainchain. Upon logging in to their respective main interfaces, users can clearly view detailed data for their assigned chain. Within the supervisory chain, every data operation, including creation, modification, and deletion, is meticulously recorded, enabling full traceability and auditability. This comprehensive logging mechanism empowers regulators to conduct effective, holistic oversight, enabling organizations to rapidly pinpoint the source of data anomalies and apply timely corrections. Users of organizational subchains are restricted to performing Create, Read, Update, and Delete (CRUD) operations exclusively on their own sub-chain data. Nevertheless, all such operations must generate corresponding log entries stored on the supervisory mainchain to support potential future traceability requirements. As an illustrative example, the traceability query functionality is displayed in Fig. 4.

V. Comparative Analysis

A. Storage Performance Analysis

The provenance supervision framework based on multi-chain integration not only ensures the security of private data through multi-modal encryption but also alleviates the storage burden inherent in conventional single-chain architectures by distributing data across multiple chains. Specifically, the supervision mainchain is dedicated solely to oversight and stores only a minimal amount of data, while each organizational subchain handles the storage requirements of its respective organization.

TABLE I. CHAIN CODE APPLICATION INTERFACE METHOD

	Method	Parameter	Description
Total Interface Methods of "Five Organizational Subchains + One Regulatory Mainchain"Data Supervision Scope	initLedger	ChaincodeStubInterface	Chaincode Initialization Function
	Invoke	ChaincodeStubInterface	Receive and process requests sent by clients
	createTrace	ChaincodeStubInterface[]string	Input a set of data arrays to add new transaction data records
	updateTrace	ChaincodeStubInterface[]string	Input a set of data arrays to update transaction data records
	deleteTrace	ChaincodeStubInterface[]string	Delete transaction data records
	queryTrace	ChaincodeStubInterface args []string	Input the corresponding traceability ID to query the latest data records
	queryAllTrace	ChaincodeStubInterface args []string	Input the corresponding traceability ID to query the latest data history records
	storeTraceMessage	ChaincodeStubInterface args []string	Multi-mode encrypted storage of data
Interface Methods Unique to the Planting Subchain	envrDataProcess	ChaincodeStubInterface args []string	Detect the similarity of environmental data
Interface Methods Unique to the Regulatory Mainchain	authentication	ChaincodeStubInterface args []string	Authenticate the identity of system login users
	qrCodeGeneration	ChaincodeStubInterface args []string	Generate QR code images for the corresponding data
	dataValidation	ChaincodeStubInterface args []string	Verify the validity of forwarded data
	traceQuery	ChaincodeStubInterface args []string	Integrate traceability information for user queries

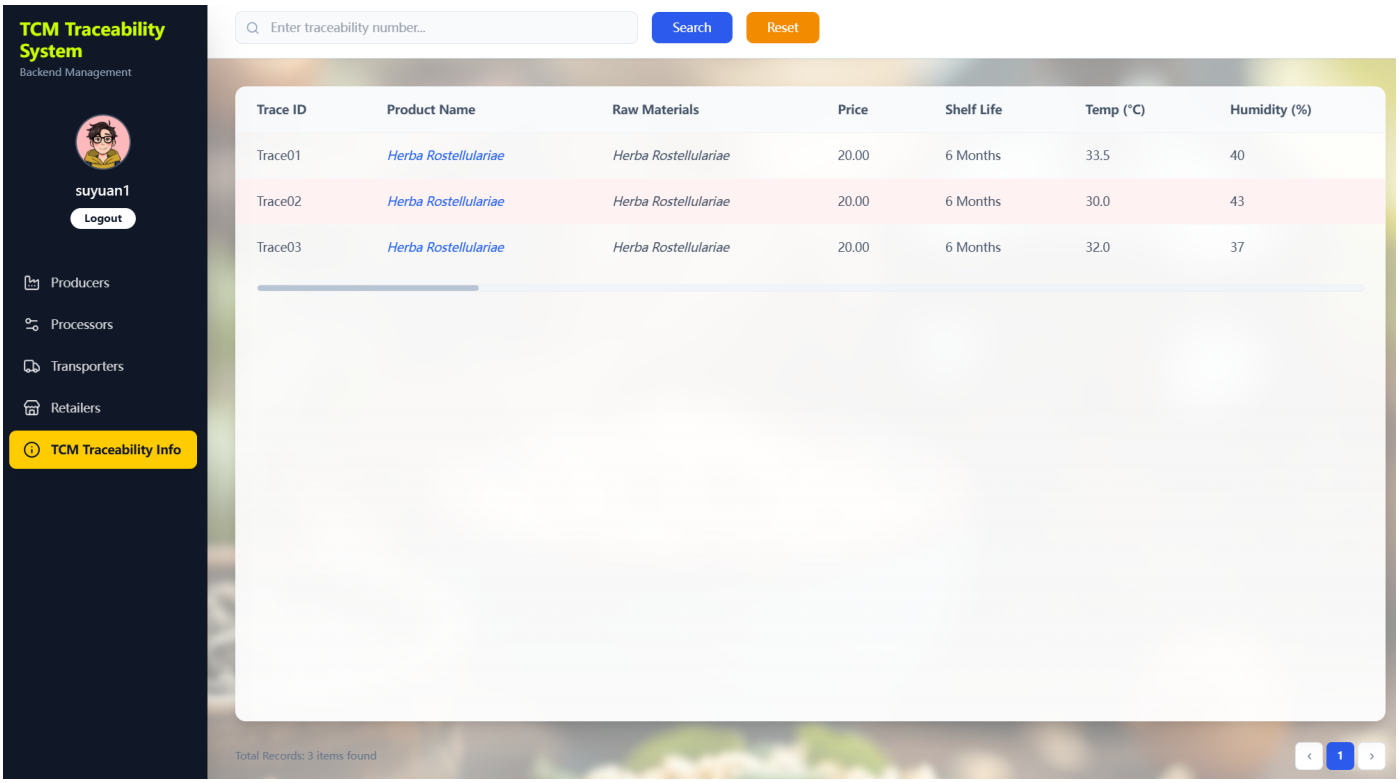

Fig. 4. Traceability information query function demonstration.

In this study, we evaluate the storage consumption of three configurations: organizational subchains (averaged across five subchains), a traditional single-chain system, and the supervision mainchain, as the number of uploaded transactions increases from 1×10^4 to 5×10^4. The results are illustrated in Fig. 5. It should be noted that, although real-world blockchain storage may involve adjustments to parameters such as block size and block generation interval based on transaction volume, this analysis focuses exclusively on the raw storage footprint attributable to the data volume itself, holding all other configuration parameters constant.

B. Comparative Evaluation of Approaches

Building upon the preceding analysis of security and storage performance, this study compares the proposed multi-chain-integrated traceability and supervision framework for Traditional Chinese Medicine with five representative existing traceability and supply chain information management systems, including a blockchain–IPFS-based monitoring system for non-perishable agricultural products that stores encrypted

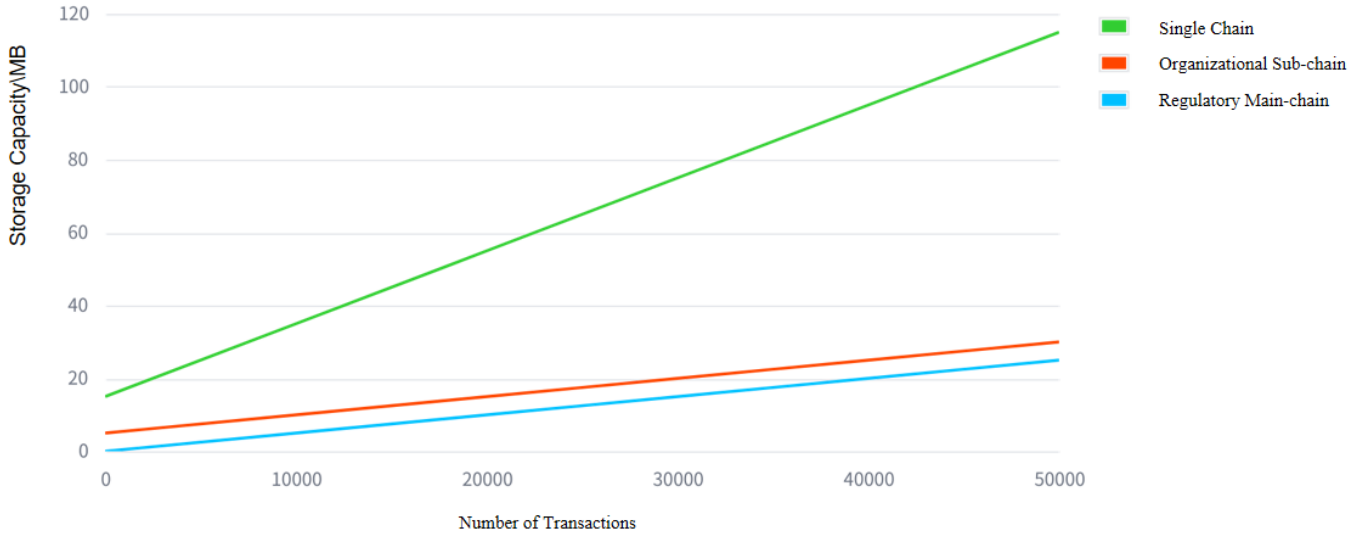

Fig. 5. Storage performance test.

TABLE II. SCHEME COMPARISON AND ANALYSIS

Research Works	[16]	[17]	[18]	[19]	[20]	**This system**
Blockchain Architecture	Single chain	Single chain	Single chain	Single chain	Single chain	Multi-chain
Data Supervision Scope	Partial info	Partial info	Partial info	Partial info	Partial info	Full lifecycle
Privacy Protection	Yes	Yes	Yes	Yes	Yes	Yes
Data Storage Performance	Medium	High	High	Medium	High	High
Data Security	High	Medium	High	High	High	Even higher
Data Validity	Medium	Medium	Medium	Medium	Medium	High
Data Access Control	None	None	None	None	None	Yes
Enterprise Collaboration	Medium	Low	Low	Low	Low	High
Main-chain Supervision Strength	Low	Low	Low	Low	Low	High
Enterprise Responsibility Differentiation	Yes	None	None	None	None	Yes

IPFS hashes on chain to alleviate centralization, reliability, and query-efficiency issues in traditional traceability architectures [16]; a blockchain-based wine supply chain traceability system that records each transaction from grape growers to retailers on chain to provide tamper-resistant, end-to-end provenance verification [17]; a Polygon-based cannabis supply chain solution that combines smart contracts with hybrid on-chain/off-chain storage to support efficient information retrieval and tamper-proof regulatory compliance across multiple stakeholders [18]; a blockchain-enabled vaccination record tracking framework that maintains immutable, privacy-preserving immunization histories across healthcare institutions [19]; and a blockchain- and IoT-driven CO_2 footprint tracking framework that enhances data integrity, transparency, and sustainability assessment in complex supply chains [20]. The comparison results are summarized in Table II. Overall, the proposed system demonstrates clear advantages across multiple dimensions, including secure cross-chain data interaction, scope of data supervision, storage efficiency, traceability and regulatory effectiveness, enterprise-level data management capabilities, strength of mainchain-based oversight, and differentiation of enterprise accountability.

VI. CONCLUSION AND FUTURE WORK

Based on existing research on traceability in TCM, this study addresses key challenges in current blockchain-based traceability systems, including single-chain storage bottlenecks, data security, data availability, and system stability. It also considers the entire TCM supply chain, encompassing cultivation, processing, transportation, sales, and regulatory oversight. To this end, we propose and implement a high-security TCM traceability and supervision system based on Hyperledger Fabric as the consortium blockchain platform. The primary contributions and innovations of this work are summarized in the following three aspects:

First, to address the storage overhead, data security, and availability challenges specific to TCM traceability scenarios, we propose a multi-chain architecture built on Hyperledger Fabric, comprising a supervising mainchain and five organiza-

tional subchains. This multi-chain framework enables secure cross-chain interaction and data fusion, effectively alleviating storage pressure, enhancing data validity, ensuring high data security, and improving inter-organizational collaboration efficiency. Furthermore, we design a multi-modal encrypted storage mechanism to strengthen data confidentiality and support fine-grained access control.

Second, we develop a zero-knowledge proof-based data supervision and transmission protocol that isolates organizational subchains while enabling end-to-end regulatory oversight without compromising user account privacy. Complementing this, we integrate QR code-based data entry and environmental data collection mechanisms, which not only improve operational efficiency but also safeguard user privacy and ensure the authenticity and reliability of environmental monitoring data. Collectively, these mechanisms guarantee the validity, traceability, and high security of data throughout the entire TCM lifecycle, from cultivation and harvesting to processing, storage, transportation, and retail. System performance evaluations confirm that the proposed framework significantly reduces storage burden, enhances data availability and security, and boosts collaborative efficiency across stakeholders in the TCM supply chain.

Third, we have constructed and successfully deployed a comprehensive TCM traceability management system that integrates the proposed multi-chain supervision architecture. The system consists of a Hyperledger Fabric consortium blockchain network, a traceability information management platform, environmental sensing devices, and QR code input terminals. We detail the functional modules, smart contract interfaces, and system demonstrations to ensure high reliability and operational efficiency. Comprehensive system testing, including storage capacity evaluation, was conducted across all stages to verify the effectiveness of each functional module in data recording and traceability. The results demonstrate that the system meets the design requirements for secure traceability management throughout the entire TCM supply chain.

For future work, we plan to incorporate artificial intelligence and big data analytics to further advance this research. By leveraging AI-driven data mining and big data analysis techniques [21–25], we aim to extract actionable insights from the vast volumes of data generated across the TCM supply chain, thereby providing scientific, intelligent, and data-driven decision support for the optimization and management of TCM production and distribution.

ACKNOWLEDGMENT

This study was supported by the Guangdong Basic and Applied Basic Research Foundation (No. 2024A1515010219), the Guangzhou Science and Technology Plan (No. 2024B03J1361, No. 2023B03J1327, and No. 2023A04J0362), the Guangdong Province Ordinary Colleges and Universities Young Innovative Talents Project (No. 2022KQNCX038), the Key Discipline Improvement Project of Guangdong Province (No. 2025ZDJS023, No. 2022ZDJS015, and No. 2021ZDJS025), the Scientific Research Capacity Improvement Project of the Doctoral Program Construction Unit of Guangdong Polytechnic Normal University (No. 22GPNUZDJS17), the Graduate Education Demonstration Base Project of Guangdong Polytechnic Normal University (No. 2023YJSY04002), and the Open Research Fund of the Guangdong Provincial Key Laboratory of Big Data Computing (No. B10120210117-OF08).

REFERENCES

[1] G. Guo, J. Zhou, X. Yang, J. Feng, Y. Shao, T. Jia, Q. Huang, Y. Li, Y. Zhong, P. Nagarkatti, and M. Nagarkatti, "Role of microRNAs induced by Chinese herbal medicines against hepatocellular carcinoma: A brief review," *Integrative Cancer Therapies*, vol. 17, no. 4, pp. 1059-1067, 2018.

[2] F. Jamil, L. Hang, K. H. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics*, vol. 8, no. 5, p. 505, 2019.

[3] D. Agrawal, S. Minocha, S. Namasudra, and A. H. Gandomi, "A robust drug recall supply chain management system using Hyperledger blockchain ecosystem," *Computers in Biology and Medicine*, vol. 140, p. 105100, 2022.

[4] O. Dib, K. L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," *International Journal on Advances in Telecommunications*, vol. 11, no. 1, pp. 51-64, 2018.

[5] J. Hua, X. Wang, M. Kang, H. Wang, and F.-Y. Wang, "Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping," in *Proc. 2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 97-101.

[6] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-W. Liao, "Governance on the drug supply chain via Gcoin blockchain," *International Journal of Environmental Research and Public Health*, vol. 15, no. 6, p. 1055, 2018.

[7] S. Sadri, A. Shahzad, and K. Zhang, "Blockchain traceability in healthcare: blood donation supply chain," in *Proc. 2021 23rd International Conference on Advanced Communication Technology (ICACT)*, 2021, pp. 119-126.

[8] W.-T. Tsai, L. Feng, H. Zhang, Y. You, L. Wang, and Y. Zhong, "Intellectual-property blockchain-based protection model for microfilms," in *Proc. 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2017, pp. 174-178.

[9] C.-L. Chen, X. Shang, W.-J. Tsaur, W. Weng, Y.-Y. Deng, C.-M. Wu, and J. Cui, "An anti-counterfeit and traceable management system for brand clothing with Hyperledger Fabric framework," *Symmetry*, vol. 13, no. 11, p. 2048, 2021.

[10] A. Marchese and O. Tomarchio, "An agri-food supply chain traceability management system based on Hyperledger Fabric blockchain," in *Proc. 23rd International Conference on Enterprise Information Systems (ICEIS)*, 2021, pp. 648-658.

[11] Z. Dong, C. Ma, Y. Wang, and Z. Liu, "Food information traceability system based on Fabric," in *Proc. 2020 International Conference on Aviation Safety and Information Technology (ICASIT)*, 2020, pp. 563-570.

[12] P.-W. Chi, Y.-H. Lu, and A. Guan, "A privacy-preserving zero-knowledge proof for blockchain," *IEEE Access*, vol. 11, pp. 85108-85117, 2023.

[13] J. Liu, Q. Guo, and Y. Tian, "The design of SM4 algorithm based on FPGA and its teaching application," in *Proc. 3rd International Conference on Artificial Intelligence and Education (ICAIE)*, 2025, pp. 374-379.

[14] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763-771, 2014.

[15] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS," in *Proc. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1499-1506.

[16] K. Biswas, V. Muthukumarasamy, and W. L. Tan, "Blockchain based wine supply chain traceability system," in *Proc. 2017 Future Technologies Conference (FTC)*, 2017, pp. 56-62.

[17] S. Babu and H. Devarajan, "Agro-food supply chain traceability using blockchain and IPFS," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 393-399, 2023.

[18] P. Nowvaratkoolchai, N. Thawesaengskulthai, W. Viriyasitavat, and P. Rangsunvigit, "Blockchain-based cannabis traceability in supply chain management," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 2, pp. 75-85, 2024.

[19] G. K. Shwetha, J. A. Rathod, G. Naveen, M. Arkachari, and M. K. Pushparani, "Blockchain-based vaccination record tracking system," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 8, pp. 753-759, 2024.

[20] M. Y. Mofatteh, R. Davallou, C. N. Ishimwe, S. S. Divekar, and O. F. Valilai, "Developing a blockchain based supply chain CO2 footprint tracking framework enabled by IoT," *nternational Journal of Advanced Computer Science and Applications*, vol. 15, no. 10, pp. 7-12, 2024.

[21] R. Chen, H. Huang, Y. Yu, J. Ren, H. Zhao, and Xu Lu, "Rapid detection of multi-QR codes based on multistage stepwise discrimination and a compressed MobileNet," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 15966-15979, 2023.

[22] R. Chen, Y. Huang, K. Lan, J. Li, Y. Ren, X. Hu, L. Wang, H. Zhao, and X. Lu, "A fast adaptive binarization method for QR code images based on dynamic illumination equalization," *Electronics*, vol. 12, no. 19, p. 4134, 2023.

[23] R. Chen, C. Yao, X. Zeng, Y. Ma, J. Yuan, J. Li, H. Zhao, X. Lu, and J. Ren, "Large-scale cross-modal hashing via Kolmogorov-Arnold representation theorem and optimal transport," *Knowledge-Based Systems*, vol. 330, p. 114698, 2025.

[24] R. Chen, P. Wang, B. Lin, L. Wang, X. Zeng, X. Hu, J. Yuan, J. Li, J. Ren, and H. Zhao, "An optimized lightweight real-time detection network model for IoT embedded devices," *Scientific Reports*, vol. 15, p. 3839, 2025.

[25] J. Yuan, X. Zeng, J. Zhou, J. Li, J. Lv, R. Chen, K. Chen, W. Yang, and Y. Zhang, "Data-driven real-time home energy management system based on adaptive dynamic programming," *Electric Power Systems Research*, vol. 238, p. 111055, 2025.