Journal of Engineering, Project, and Production Management
2026, 16(2), 2025-174

Enterprise Financial Information Security Sharing and Encryption Calculation Based on Blockchain Technology

Jiayun Wu
Associate Researcher, Human Resources Department, Wuxi Vocational Institute of Commerce, Wuxi, 214153, China, E-mail: julia_22@163.com

Project Management
Received August 20, 2025; revised October 12, 2025; accepted October 15, 2025
Available online March 7, 2026

Abstract: In the digital economy, the demand for financial data sharing among enterprises is growing rapidly. Traditional financial sharing models face prominent issues, including data security risks, insufficient efficiency and transparency. To enable the encrypted storage and hierarchical access of sensitive financial data, this study proposes a blockchain-based scheme for secure sharing and encrypted computation of enterprise financial information. The blockchain component incorporates credibility evaluation, process optimization, and cross-organizational collaboration models. Its layered architecture optimizes sharing efficiency and supports applications in supply chain finance, among other scenarios. The encryption component is based on the Number Theory Research Unit (NTRU) encryption algorithm, which utilizes polynomial rings, homomorphic encoding, and secure two-party protocols to ensure data privacy and operational integrity. The synergy between these two components provides digital support for the integration of business and finance as well as ecological collaboration. Experimental results showed that the proposed method achieved a stable transaction throughput of 4,500 TPS and reduced audit time by 79.8%. In practical application testing, the proposed method achieved stable financial error and audit variance rates of 0.3% and 0.2%, respectively, with storage costs that stabilized at approximately 0.5 yuan/GB/month. The blockchain-based platform for enterprise financial information sharing and encrypted computation proposed in this study demonstrates high data quality, compliance, and security. This platform effectively solves the problems of low security, inefficiency, and non-compliance.

Keywords: Enterprise financial information sharing platform, blockchain technology, number theory research unit encrypt, cross-organizational collaboration model, homomorphic encoding.

DOI 10.32738/JEPPM-2025-174

---

1. Introduction

Amid the wave of the digital economy and the ongoing digital transformation of enterprises, the financial data generated by enterprises during their operation is growing exponentially. As the core asset and decision-making basis of enterprises, the secure sharing and efficient utilization of financial information have become the key to the coordinated development of enterprises (Kala, 2023). However, traditional data sharing models face severe security and privacy challenges. If core financial data is transmitted in plaintext or stored in an uncontrolled environment, it is highly susceptible to unauthorized access, theft, and abuse. These risks stem from external cyber-attacks, internal leaks, third-party system vulnerabilities, or the inherent risks of cloud platforms (Singireddy, 2024). Such breaches can not only lead to the leakage of trade secrets, damage to corporate reputation, and significant economic losses but also violate increasingly strict global data protection regulations. This could trigger severe legal liability and a crisis of market trust (Radanliev, 2025). Moreover, in Cross-Organizational Collaboration (COC), data sharing is trapped in a "silo" dilemma due to privacy and compliance requirements: circulating sensitive data risk leakage, while excessive restriction hinders resource integration and efficiency (Weerawarna, 2023). Blockchain technology has the characteristics of decentralization, immutability, and traceability, which can provide a new paradigm for building a trusted data sharing environment (Savelyeva, 2022). Encryption computing can achieve collaborative analysis without exposing raw data, and the fusion of the two provides technical possibilities for solving the challenges faced by financial information security sharing. This study aims to improve the security, transparency, and efficiency of an Enterprise Financial Information Sharing Platform (EFISP), reduce operating costs, promote compliance, drive business innovation, and ultimately enhance the overall financial management and corporate competitiveness. This study proposes an innovative scheme for an Enterprise Financial Information Sharing Platform (EFISP) and Encrypted Computing (EC) based on blockchain technology. This study constructs an EFISP with strategic finance, sharing, and business finance centers as the core architecture, and implements data trust evaluation, process optimization, and COC through blockchain technology. Moreover, a Secure Two-Party Computation (SETPC) scheme based on the Number Theory Research Unit Encrypt (NTRUEncrypt) algorithm is designed. This scheme utilizes polynomial rings, homomorphic encoding, and secure two-party protocols to ensure data privacy and operational integrity. This study aims to build a secure sharing and encryption computing platform for enterprise financial information based on blockchain technology and the NTRUEncrypt algorithm to enhance the security, efficiency, and compliance of data sharing. The specific research objectives are threefold: (1) The hierarchical blockchain architecture of EFISP is designed to achieve data trust evaluation, process optimization, and COC. (2) The NTRUEncrypt algorithm is integrated and supports secure computation between both parties. (3) Through experiments, the performance advantages of the platform are demonstrated in transaction throughput, audit efficiency, data quality, and cost control. The research questions are: (1) How to effectively enhance the credibility and collaborative efficiency of enterprise financial information sharing through blockchain technology? (2) How does the NTRUEncrypt algorithm ensure the privacy and computational accuracy of financial data during the sharing process in EC? (3) Does the proposed solution have better data processing efficiency, security, and economy than traditional methods in practical applications? This study proposes the following hypotheses: (1) a blockchain-based financial information sharing platform can significantly improve transaction throughput and reduce confirmation latency. (2) The encryption calculation scheme using the NTRUEncrypt algorithm can effectively prevent data leakage. (3) This integrated solution can significantly reduce financial error rates and audit variance rates while optimizing storage costs. By clarifying the above objectives, questions, and hypotheses, the study provides a clear logical framework and basis for evaluation for the subsequent design, experimentation, and discussion. The theoretical development of the research is reflected in the following aspects: Firstly, a multidimensional theoretical model based on blockchain technology is established to construct EFISP, quantifying the effectiveness of blockchain in financial allocation through mathematical formulas. Secondly, a SETPC scheme based on the NTRUEncrypt algorithm is designed. This scheme introduces theoretical frameworks for polynomial ring definition, public key generation, and homomorphic encryption verification, to ensure data can be computed while encrypted without privacy leakage. The proposed methods are expected to provide theoretical support for enhancing the security of corporate financial data and improving management efficiency.

2. Related Works

Enterprise Financial Information Sharing Platforms (EFISP) and Encrypted Computing (EC) are the core supporting technologies of financial management in the digital economy, making research in this area highly significant. Lv et al. (2023) proposed a network intrusion detection algorithm integrating deep neural network models to address security concerns posed by digital twins in urban networks. During the research process, a trust model based on key hashing self-synchronization within the cloud service system was developed, resulting in high detection precision and efficiency. Naik et al. (2023) proposed a security framework based on a shared responsibility model to address data security and network threats in cloud environments. Their method effectively balanced cloud service efficiency and security. Abraham et al. (2023) proposed a method for the coordinated integration of accounting practices and network security strategies to address threats accounting systems and enhance financial data protection. This method could effectively enhance financial data protection capabilities and strengthen risk response resilience. Wang and Wang (2022) proposed a supply chain finance optimization scheme leveraging blockchain and edge computing to address the low efficiency and high risk of supply chain financing for SMEs. This method could effectively reduce financing costs and risks and improve real-time security. Sharif and Mohammed (2022) proposed an empirical method involving multi-source data collection and statistical analysis for predicting financial losses and future trends caused by cybercrime. This method could effectively quantify the evolution trend of cybercrime and provide data support for formulating targeted defense strategies.

Many industry scholars have also conducted in-depth studies and applied blockchain technology. Gad et al. (2022) proposed a knowledge graph analysis method based on bibliometrics to address the lack of systematic reviews in blockchain technology studies. This method quantitatively analyzed blockchain literature from seven dimensions, including influential papers and research trends, and could effectively reveal the evolution of blockchain technology. Ramzan et al. (2022) employed a classification method based on technological evolution and case analysis to address the lack of systematic evaluation of blockchain applications in the healthcare field. This method clearly demonstrated the application value of blockchain in the medical field. Khan et al. (2022) proposed a supply chain mapping and integration method based on blockchain technology to address the issues of insufficient transparency and sustainability challenges in supply chain management. This method could effectively improve the sustainability performance of the supply chain. Akram et al. (2022) designed a blockchain-based drug traceability system to improve transparency and resolve traceability difficulties in the pharmaceutical supply chain. This system could effectively improve data security, transparency, and regulatory efficiency. Prados Castillo et al. (2024) proposed a blockchain-based method for value chain optimization to meet the needs for efficiency and sustainable development in the tourism industry. This method could effectively improve supply chain efficiency and sustainable management level.

In summary, while existing research on EFISP and EC is promising, it still faces challenges such as inadequate data security, inefficiency, and a lack of trust. Blockchain technology can integrate modern cryptographic techniques to build a multi-layered protection system of “transaction-level encryption, privacy isolation, and permission control.” Furthermore, its features-smart contracts and distributed ledgers-can achieve process automation, information transparency and traceability, and enhanced system resilience. Therefore, based on this, this study proposes an EFISP and EC scheme that utilizes blockchain technology. It can build an enterprise financial information sharing center, improve the data security and process efficiency of the enterprise’s financial information sharing center, and promote the transformation of financial management from "accounting-oriented" to "value-oriented".

3. EFISP and Security EC Solution Design

3.1. Design of EFISP based on Blockchain Technology

Enterprise Financial Information Sharing Platforms (EFISP) and Encrypted Computing (EC)solutions are key to balancing data value extraction with privacy protection in the digital economy. Technologically, such platforms rely on blockchain, multi-party computation, and homomorphic encryption to ensure the immutability and minimize exposure of data during the sharing process (Nour, 2022). From a social perspective, their successful operation relies on reconstructing trust mechanisms between enterprises, thereby reducing the friction costs of traditional contract execution. The secure EC solution enables collaborative analysis by sharing algorithms rather than migrating raw data, which meets compliance requirements, promotes cross-organizational knowledge flow, and aligns with the principle of "data element marketization" (Zhang, 2022). However, the widespread adoption of this model faces three major challenges. First, technological complexity creates high entry barriers for small and medium-sized enterprises. Second, the existing legal framework is ambiguous in determining the ownership of encrypted data. Third, a lack of industry standards could perpetuate "data silos" in a new form. Moving forward, a multi-pronged approach-combing policy guidance, technological inclusiveness, and an ethical consensus is needed to translate the technological ideal of "secure sharing for financial data into socio-economic practice. Amid the digital economy and enterprise transformation, the value of financial information has evolved from a traditional "internal accounting tools" to a "core resources of COC" (Ahmad, 2022). However, the current inter-enterprise financial information sharing faces multiple challenges. Financial systems are often built on independent databases with inconsistent standards and incompatible interfaces, creating "data islands" that lead to delayed information transmission and high verification costs (Haque, 2022). Furthermore, traditional sharing relies on credit endorsement of centralized institutions, which poses risks of data tampering and privacy breaches. The collaboration process is often cumbersome, failing to meet the demands of efficient operations (Wen, 2023). Blockchain technology has the characteristics of a distributed ledger, tamper-proof, traceable, and smart contracts, which can provide a technical path to overcome the above difficulties and build an EFISP based on blockchain technology. Thus, blockchain technology is both a practical requirement for digital transformation and a key means for driving management change through technological innovation (Manzoor, 2022; Malik, 2023; Liu, 2023). Among them, the EFISP architecture is shown in Fig. 1.

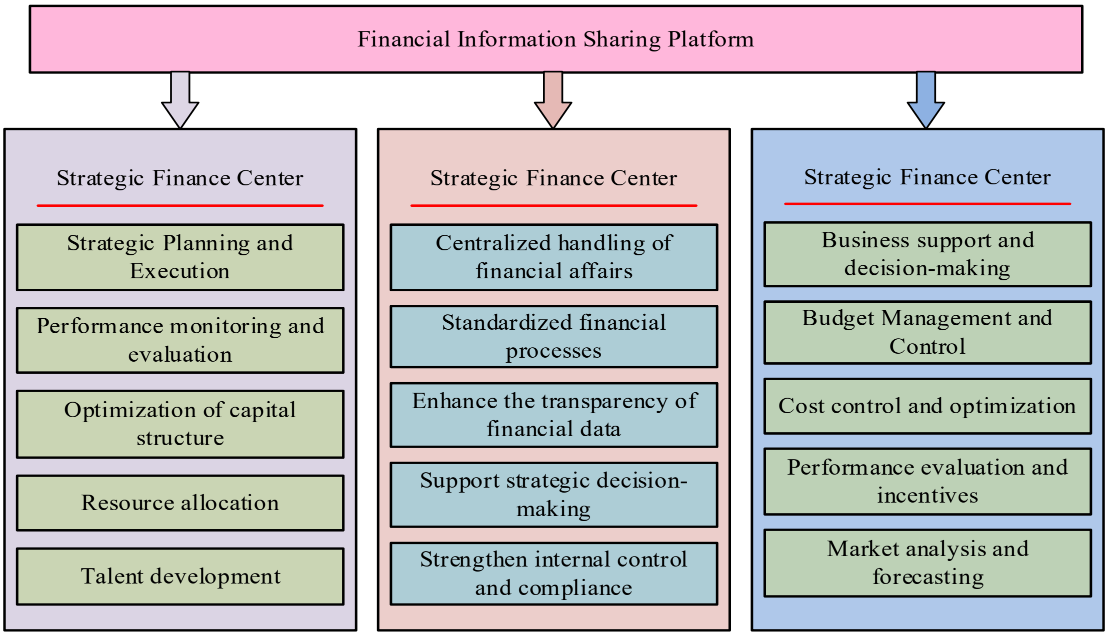


Fig. 1. Architecture of EFISP

As shown in Fig. 1, the core architecture of the EFISP consists of a strategic finance center, a shared service center, and a business finance center, which are responsible for strategic planning, shared services, and business empowerment, respectively. This platform optimizes resource allocation, strengthens internal control compliance, and deepens decision support through process standardization, data integration, and business-finance collaboration, building an efficient and intelligent financial management system to support the implementation of enterprise strategies and value enhancement. To improve audit efficiency and risk control capabilities, this study incorporates several factors: data volume contribution, smart contract execution integrity, latency control, and cross-chain verification strength. The blockchain-powered financial data credibility evaluation model quantifies the trustworthiness of an individual financial transaction on the network. This provides a basis for data screening and priority management within financial sharing centers (Bag, 2023). The specific formula of the model is shown in Eq. (1).

$$T_i = \alpha \cdot \frac{V_i}{V_{\text{total}}} + \beta \cdot \frac{C_i}{C_{\max}} + \gamma \cdot \left(1 - \frac{D_i}{\Delta t}\right) + \delta \cdot \log(1 + S_i) \tag{1}$$

In Eq. (1), is the credibility score of the -th financial data. , , , and are weight coefficients representing the importance of each dimension. is the data volume of the -th data. is the total data volume of all data in the current batch. is the number of completed smart contract execution steps associated with the -th data transaction. is the maximum possible number of execution steps for this type of business smart contract. is the delay from the generation of the -th data to its upload on the chain. Δt is the maximum tolerance delay threshold set by the system. is the number of cross-chain nodes participating in the -th data validation. Next, to reflect the nonlinear impact of highly trusted data on process acceleration, this study introduces an efficiency optimization model for blockchain financial sharing centers, which weights business process completion and resource utilization rates by credibility (Chittipaka, 2023). The specific expression is shown in Eq. (2).

$$\eta = \frac{\sum_{i=1}^{n} T_i \cdot P_i \cdot R_i}{\sum_{i=1}^{n} P_i \cdot R_i} \cdot \left(1 - e^{-\lambda \cdot \overline{T}}\right) \tag{2}$$

As shown in Eq. (2), represents the efficiency of financial process optimization. is the total number of financial transactions involved in the evaluation. is the actual completion rate of the -th business process. is the proportion of system resources occupied by the -th transaction. is the average credibility of all businesses. is the marginal benefit attenuation coefficient of credibility, which represents the diminishing marginal effect of high credibility data on efficiency improvement. Subsequently, to provide a decision-making basis for optimizing scenarios like cross-enterprise financial settlement and audit reconciliation, this study incorporates factors such as data exchange latency, the scale of blockchain network fragmentation, and cross-organizational node participation. It quantifies the comprehensive efficiency of blockchain-based financial sharing centers in COC data through a COC data efficiency model, as shown in Eq. (3).

$$\Phi = \frac{\sum_{j=1}^{m} \left[\phi_j \cdot \left(1 - \frac{L_j}{L_{\max}}\right) \cdot \tanh(\kappa \cdot H_j) \right]}{\sum_{j=1}^{m} \phi_j} \cdot \left(1 + \theta \cdot \frac{N_{\text{cross}}}{N_{\text{total}}}\right) \tag{3}$$

In Eq. (3), Φ represents the efficiency of cross organizational data collaboration. is the total number of cross organizational business links involved in collaboration. is the weight of the -th business link. is the average data exchange delay of the -th link. is the maximum tolerable delay threshold set by the system. is the proportion of hash computing power of the blockchain shard where the -th link is located. is the scale efficiency coefficient of sharding, used to control the extent to which sharding technology improves efficiency. is the actual number of cross organizational nodes participating. is the total number of theoretically accessible cross organizational nodes. To guide enterprises in finding the optimal solution between data security and operational costs, this study introduces a privacy computing cost-benefit balance model to evaluate the input-output ratio of financial data privacy protection technology in the blockchain environment (Khan, 2023). The expression is shown in Eq. (4).

$$\Omega = \frac{\sum_{k=1}^{p} \left[\omega_k \cdot (B_k - C_k) \right]}{\sum_{k=1}^{p} \omega_k \cdot B_k} \cdot \left(1 - \mu \cdot \frac{E_{\text{privacy}}}{E_{\text{total}}}\right) \tag{4}$$

As shown in Eq. (4), is the net profit efficiency of privacy calculation. is the number of types of privacy computing technologies applied. is the business weight of the -th technology. is the annualized business value added brought by the -th technology. is the average annual computation resource cost of the -th technology. is the penalty coefficient for privacy energy consumption, representing the strength of environmental and social governance constraints. is the average annual energy consumption of the privacy computing module. is the total energy consumption of the financial shared center. Next, to guide enterprises to accurately allocate limited resources to high-priority strategic areas, this study introduces a strategic resource dynamic allocation efficiency model to quantify the strategic resource dynamic allocation efficiency of the strategic financial sharing center under the empowerment of blockchain. It guides the compression effect of resource allocation redundancy by comparing the deviation between actual resource investment and strategic planning goals, combined with blockchain technology, as shown in Eq. (5).

$$\Psi = \frac{\sum_{r=1}^{s} \left[\psi_r \cdot \left(\frac{F_r^{\text{actual}}}{F_r^{\text{plan}}}\right)^{\gamma} \cdot \left(1 - \frac{H_r}{H_{\max}}\right) \right]}{\sum_{r=1}^{s} \psi_r} \cdot (1 + \xi \cdot \text{COR}_{\text{blockchain}}) \tag{5}$$

In Eq. (5), represents the efficiency of dynamic allocation of strategic resources. is the total number of strategic resource categories. is the strategic weight of the r -class resource. is the actual allocation amount of Class resources. is the strategic planning target value for the r -class resource. is the penalty coefficient for target deviation, representing the efficiency loss of amplifying the deviation from the target. is the scheduling delay for Class resources. is the maximum scheduling delay threshold that the system can tolerate. is the optimization rate of resource allocation cost by blockchain technology. Finally, to reveal the network effect value of blockchain in integrating supply chain finance, tax collaboration, and other scenarios, this study introduces a financial ecosystem collaborative value capture model. This model measures the value increment created by the industrial ecological network constructed by the financial sharing center through blockchain by comparing the financial value of the individual actions of enterprises with the value after ecological collaboration, and introducing the attenuation factor of ecological governance coordination cost (Li, 2022). The calculation is shown in Eq. (6).

$$\Xi = \frac{\sum_{e=1}^{t}\left[\xi_e \cdot \left(V_e^{\text{ecosystem}} - V_e^{\text{standalone}}\right)\right]}{\sum_{e=1}^{t}\xi_e \cdot V_e^{\text{standalone}}} \cdot \left(1 - \varphi \cdot \frac{G_{\text{coordination}}}{G_{\max}}\right) \tag{6}$$

In Eq. (6), is the ecological synergy value capture rate. is the number of partners involved in ecological collaboration. is the strategic importance weight of the e -th partner. is the annualized financial value of the -th partner in ecological collaboration. is the benchmark financial value when the -th partner leaves the ecosystem. is the cost penalty coefficient for ecological governance, representing the frictional losses reflecting cross organizational coordination. is the average annual governance cost of ecological synergy. is the maximum ecological governance cost threshold that enterprises can afford. Overall, the framework model of the new financial information sharing center for enterprises is shown in Fig. 2.

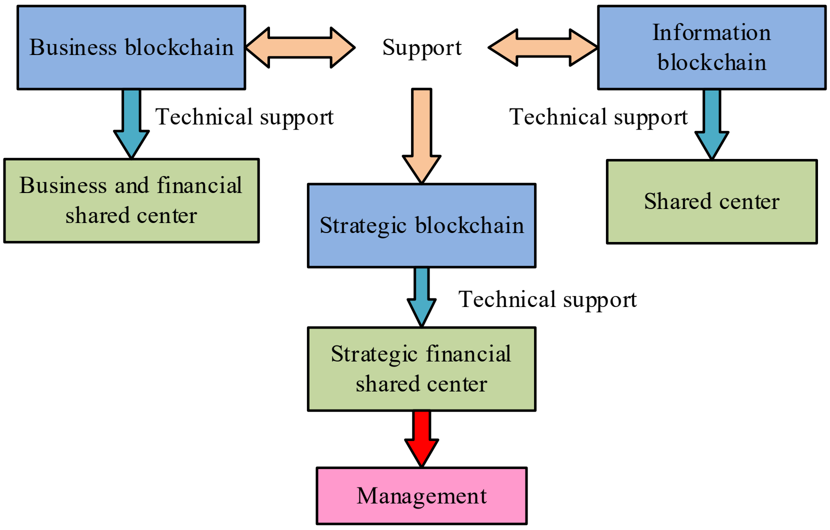


Fig. 2. Framework model of new financial information sharing center for enterprises

In Fig. 2, the blockchain module (blue area) of the new financial information sharing center framework model for enterprises is supported by business, information, and strategic blockchains as the core. Through technical support, two central centers (green area), “Business Financial Sharing Center” and "Strategic Financial Sharing Center”, are constructed, forming a three dimensional management architecture of “data interaction process collaboration decision support” (pink area). Each module is interconnected through bidirectional data exchange, enabling the efficient integration of business, information, and capital flows. This study introduces a collaborative coupling model of blockchain technology, which characterizes the suppression of overall efficiency by the exponential decay term of the technology gap, guiding enterprises to avoid the trap of "technology stacking" and achieve maximum network effects. The specific formula is shown in Eq. (7).

$$\Gamma = \frac{\sum_{k=1}^{3}\left[\omega_k \cdot \left(\frac{E_k^{\text{actual}}}{E_k^{\text{potential}}}\right)^{\theta_k}\right]}{\sum_{k=1}^{3}\omega_k} \cdot \exp\left(-\lambda \cdot \sqrt{\sum_{k=1}^{3}\left(1 - \frac{S_{ij}}{S_{\max,ij}}\right)^2}\right) \tag{7}$$

In this Eq., Γ represents the collaborative coupling efficiency of three types of blockchain technologies. ω_k is the strategic weight of the k -class blockchain. E_k^{actual} is the actual performance output of Class k blockchain. $E_k^{\text{potential}}$ is the theoretical maximum efficiency of the k -class blockchain. θ_k is the non-linear efficiency adjustment coefficient. S_{ij} is the degree of technical compatibility between Class i and Class j blockchains. $S_{\max,ij}$ is the ideal maximum degree of interaction adaptation between technologies. $S_{\max,ij}$ is the coefficient of punishment intensity for technological gap, which reflects the tolerance threshold of enterprises towards the difficulty of integrating heterogeneous systems. Finally, to reveal the scalability of the ecosystem, this study introduces a cross chain value flow value-added model to measure the financial value achieved by three types of blockchain through cross chain protocols, as shown in Eq. (8).

$$\Lambda = \sum_{k=1}^{3}\left[\varphi_k \cdot \left(\frac{V_k^{\text{cross-chain}}}{V_k^{\text{intra-chain}}}\right)^{\beta_k}\right]\cdot\left(1+\delta\cdot\frac{N_{\text{alliance}}}{N_{\max}}\right) \tag{8}$$

In Eq. (8), Λ is the multiple of cross chain value flow appreciation. φ_k is the value conversion coefficient of the k -class blockchain in cross chain scenarios. $V_k^{\text{cross-chain}}$ is the value created by the k -class blockchain through cross chain interaction. $V_k^{\text{intra-chain}}$ is the value created by Class k blockchain when running in isolation. β_k is the non-linear amplification factor of value. δ is the scale benefit adjustment coefficient of the alliance, which reflects the strength of network externalities. N_{alliance} is the number of enterprises participating in cross-chain alliances. $N_{\max}$ is the theoretical maximum number of accessible alliance members. Overall, the operational process of EFISP based on blockchain technology is shown in Fig. 3.

As shown in Fig. 3, EFISP is a blockchain-based technology, builds a three-dimensional process system. This system encompasses the following stages: “data trust evaluation, layered blockchain collaboration, shared central integration, technology deep integration, multi-scenario application”. In the diagram, the blue section corresponds to the data credibility evaluation and hierarchical blockchain collaboration module; the green section represents the shared center integration and the deep technology integration modules: and the pink section represents multi-scenario application modules. This system enhances process efficiency via the business chain, breaks through organizational boundaries via the information chain, and empowers resource allocation through the strategic chain. By integrating innovative methods like privacy computing and cross-chain technology, it facilitates the efficient sharing and value transformation of financial information without compromising data security. Implemented in scenarios like supply chain finance, tax collaboration, and audit risk control, it provides a comprehensive digital financial solution covering the entire life cycle of enterprises, helping to deepen the integration of business and upgrade ecological collaboration, significantly improving the transparency and management efficiency of enterprise finance. In addition, the platform has achieved automated compliance review of the financial process through the built-in business verification mechanism of smart contracts. Furthermore, the immutability and real-time auditing capabilities of blockchain enable any abnormal transactions to be detected and triggered immediately, significantly reducing financial error and audit discrepancy rates alike. The platform passively protects data and actively participates in business error prevention and control through process embedding, rule execution, and real-time monitoring.

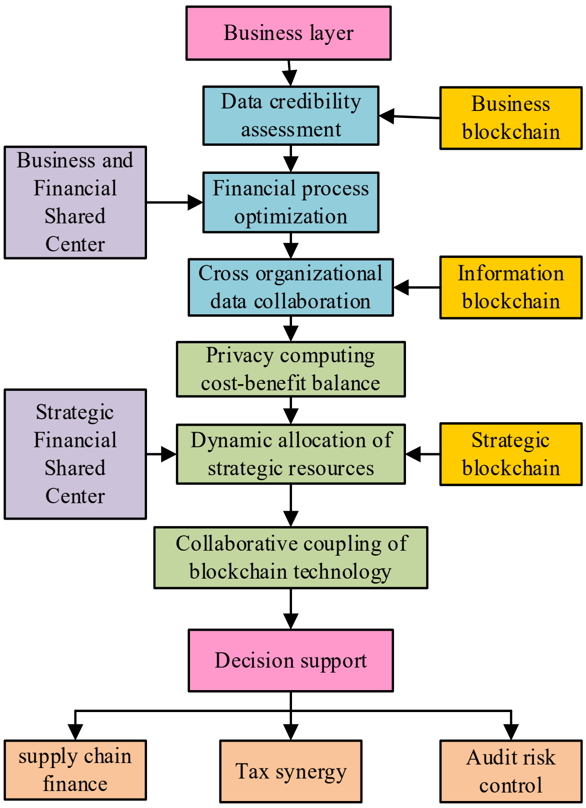


Fig. 3. Operation process of EFISP based on blockchain technology

3.2. Design of SETPC Scheme based on NTRUEncrypt Algorithm

The EFISP based on blockchain technology can effectively crack data silos, improve collaborative efficiency, enhance data credibility, reduce trust costs, promote deep integration of business and finance, and assist enterprises in digital transformation (Luo, 2023). However, the platform relies on keys for data access and control. If the private key is leaked or lost, it may lead to data leakage or inability to access, thus posing significant security issues (Garai, 2023). The NTRUEncrypt algorithm has lattice-based cryptographic properties and can achieve financial collaborative computation between two parties under the premise of "data availability but invisibility" through efficient public key encryption and secure computing mechanisms (Mojisola, 2022). Therefore, to solve the contradiction of sensitive information being easily leaked in financial data sharing and the need to expose raw data for cross-organizational calculations, this study designs a SETPC scheme based on the NTRUEncrypt algorithm. The Convolutional Polynomial Ring (CPR) is defined as the fundamental operational domain of the NTRUEncrypt algorithm, where all polynomial operations are performed to optimize the efficiency of polynomial multiplication while providing security support for lattice-based difficult problems. The specific expression for its definition is shown in Eq. (9).

$$\mathsf{R}_q = \mathsf{Z}_q[x]/(x^N - 1) \tag{9}$$

Eq. (9) shows, R_q is the CPR of module q, Z_q is the integer ring of module q, $x^N - 1$ is the polynomial module, the structure of the ring is defined, and N is the polynomial order. Among them, the NTRU public key is generated by multiplying the inverse of the private key with a random ternary polynomial, which is the basis of the encryption process (Kouhizadeh, 2023). Its expression is shown in Eq. (10).

$$h(x) = F_q(x) * g(x) \in \mathsf{R}_q \tag{10}$$

Eq. (10) defines, $h(x)$ is a public key polynomial, $F_q(x)$ is the inverse of private key $f(x)$ in R_q, $g(x)$ is a random ternary polynomial, and $*$ is a convolution multiplication on ring R_q. Next, the study uses the NTRU encryption formula to encrypt plaintext into ciphertext polynomials through public keys and random perturbations, as expressed in Eq. (11).

$$e(x) = p \cdot h(x) * r(x) + m(x) \bmod q \tag{11}$$

Eq. (11) shows, $e(x)$ is a ciphertext polynomial. p and q represent moduli, and $r(x)$ is a random three valued polynomial. $m(x)$ is a plaintext polynomial with coefficients in $\left[-\frac{p}{2}, \frac{p}{2}\right]$. In summary, the execution diagram of the two side NTRUEncrypt is shown in Fig. 4.

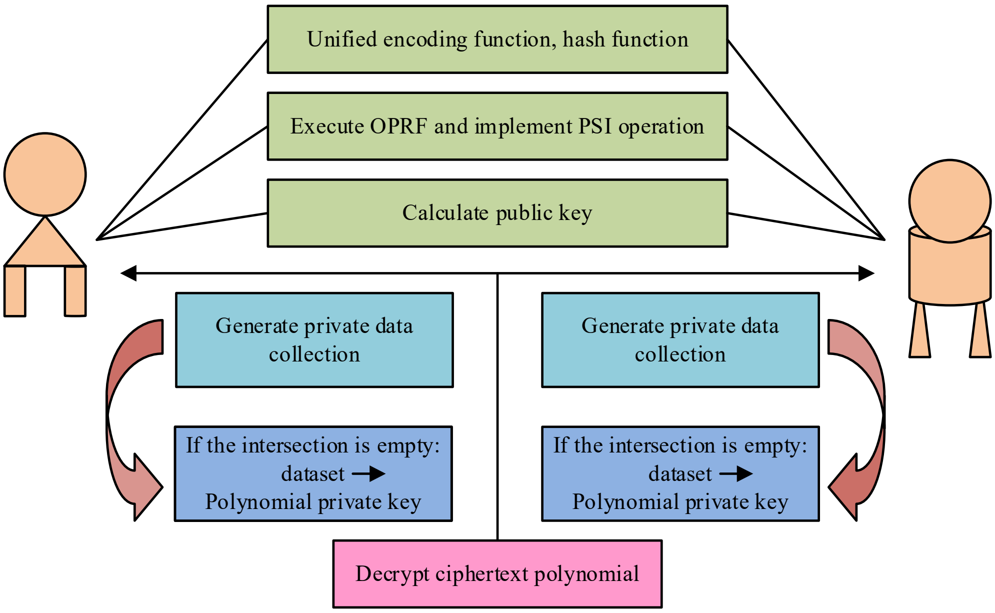


Fig. 4. Execution diagram of two-party NTRUEncrypt

Fig. 4 explains the execution process of the two-party NTRUEncrypt which includes unified encoding and hash preprocessing, Oblivion Pseudo Random Function (OPRF), and Private Set Intersection (PSI) operations to calculate the public key, generating polynomial private keys based on the private data set, and finally decrypting the ciphertext polynomial. These links reflect the technical logic of two parties collaborating to complete encryption and intersection calculation under privacy protection. The communication parties are defined as Alice and Bob. To achieve secure two-party polynomial multiplication, Alice and Bob collaborate to calculate the product without leaking their respective polynomials, as shown in Eq. (12).

$$g(x)\left(a_0+a_1x^1+a_2x^2+\cdots+a_Nx^N\right)=\sum_{i=0}^{N}A_i(x)+\sum_{i=0}^{N}B_i(x) \tag{12}$$

In Eq. (12), $g(x)$ is the polynomial held by Bob. $a_0, a_1, \dots, a_N$ are the polynomial coefficients held by Alice. x^N is the weight coefficient. $A_i(x)$ and $B_i(x)$ are intermediate polynomials calculated through unintentional protocol. The column concatenation matrix obtained by Alice and Bob through data mapping is shown in Fig. 5.

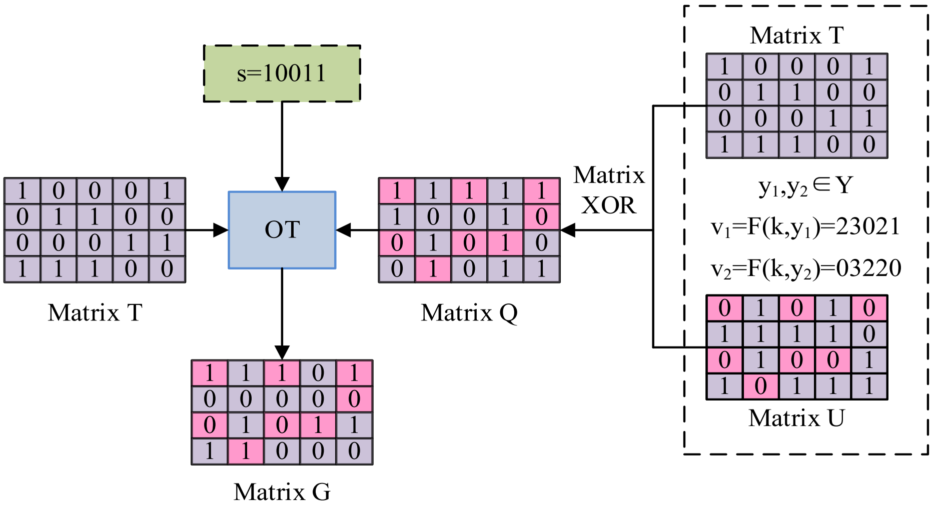


Fig. 5. All column concatenation matrices generated by data mapping execution

As depicted in Fig. 5, data mapping research is conducted around binary matrices. Matrix T and matrix G are transformed by OT to generate matrix Q. Matrix Q is XORed with matrix T to obtain matrix U and S as binary parameters. The Y set generates corresponding values through the function F. Among them, the study performed hash operations based on binary bit strings to generate mapping values, whose expression is shown in Eq. (13).

$$\Upsilon = H\left(G_1\left[v[1]\right]\Box G_2\left[v[2]\right]\cdots\Box G_k\left[v[k]\right]\right) \tag{13}$$

Eq. (13) shows, H is the cryptographic hash function negotiated by both parties. G is a binary bit matrix. $v[k]$ is the component value output by the pseudo-random function. $G_i\left[v[k]\right]$ is the bit value of the $v[k]$-th row selected from the i-th column of matrix G. $\Box$ is a bit string connection operation. To reduce the computational cost of polynomial operations, the study introduced the Chinese Remainder Theorem homomorphic encoding to encode numerical data into polynomials, and its homomorphism supports efficient and secure computation (Zhou, 2023). The specific expression is shown in Eq. (14).

$$\begin{cases}\phi : R \to \prod_{i=1}^{n} R / m_i R \\ \phi(f(x)) = \left(f(1) \mod m_1, f(-1) \mod m_2, \dots, f(\omega_N^{n-1}) \mod m_n\right)\end{cases} \tag{14}$$

Eq. (14) expresses that, R is a polynomial ring in the NTRU algorithm. $\prod_{i=1}^{n} R / m_i R$ is the direct product space after CRT decomposition. ϕ is a homomorphic mapping function that maps the elements in polynomial ring R to the direct product space after CRT decomposition. ω_N is the primitive N-th unit root, satisfying $\omega_N = e^{\frac{2\pi i}{N}}$. m_i is the modulus used in CRT decomposition. m is the plaintext message to be encrypted. Next, to ensure that the addition and multiplication results of ciphertext and plaintext are consistent and maintain the homomorphism of addition and multiplication, this study introduces homomorphic addition and multiplication verification formulas for verification, as shown in Eq. (15).

$$\begin{cases}E(m_1+m_2) \equiv E(m_1)+E(m_2) \bmod (q, x^N-1) \\ E(m_1 \cdot m_2) \equiv E(m_1) \cdot E(m_2) \bmod (q, x^N-1)\end{cases} \tag{15}$$

As seen in Eq. (15), $E(\cdot)$ is the NTRU homomorphic encryption function. m_1 and m_2 are two plaintext polynomials involved in addition and multiplication operations. $\equiv$ is a congruence symbol, indicating that the polynomials on both sides are equal in terms of coefficient modulus and polynomial modulus. q is the encryption modulus. $x^N - 1$ is a circular polynomial. The security parameters and collision difficulty of NTRUEncrypt algorithm are shown in Table 1.In Table 1, as the security level increases, the difficulty of cracking the NTRUEncrypt algorithm shows an exponential increase. In summary, the SETPC process based on NTRUEncrypt algorithm is shown in Fig. 6.

In Fig. 6, the SETPC model based on NTRUEncrypt algorithm achieves adaptive processing of data type and operation type through hierarchical judgment: for polynomial data, addition operation relies on homomorphic encryption to be directly executed on the ciphertext; Non-addition operations rely on NTRUEncrypt OT to ensure the privacy of complex operations; Non-polynomial data are first mapped to NTRU ring structure through CRT encoding to ensure compatibility in subsequent calculations. The overall design balances efficiency and security, utilizing NTRU's lightweight encryption advantages and cryptographic protocols to provide an efficient solution for data privacy protection in collaborative computing between two parties.

Table 1. Security parameters and collision difficulty of NTRUEncrypt

Security level	N	q	p	Calculation frequency
General safety	320	1024	3	2300
Standard security	339	1024	3	2360
High security	428	1024	3	2450
Maximum security	634	1024	3	2510

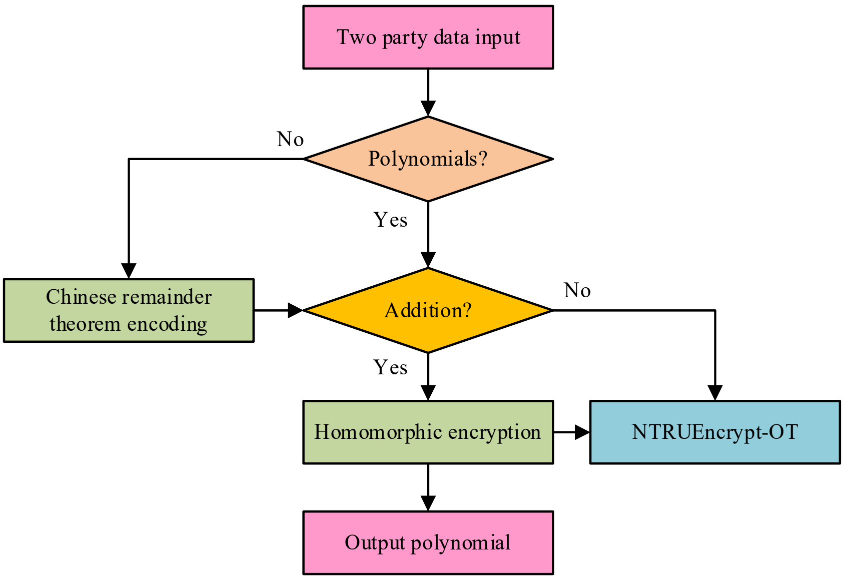


Fig. 6. Two-party computation process for secure encryption based on NTRUEncrypt algorithm

4. EFISP and EC Scheme Verification based on Blockchain Technology

4.1. EFISP and EC Scheme Performance Testing

To verify the performance of EFISP and EC solutions based on blockchain technology, this study constructs a simulation model. The experimental setup is shown in Table 2.

Table 2. Test environment and specific configuration

Testing Environment	Specific Configuration
CPU	Intel Core i7-12700H
RAM	32GB DDR4
Storage	1TB NVMe SSD (system disk) + 2TB SATA SSD (data disk)
Operating system	Ubuntu Linux 20.04 LTS
Blockchain platform	Hyperledger Fabric
Encryption algorithm library	OpenSSL 3.0+
Performance testing tool	Hyperledger Caliper 0.8+

As shown in Table 2, this study conducts performance testing using the specific configurations listed in the table, using a publicly available blockchain testing network dataset. The research method is compared with the Super Chaotic Bidirectional Authentication Method (SCBAM) and the National Secret Algorithm (NSA). Three methods are compared for transaction throughput and confirmation delay time when facing different concurrent user numbers. The results are shown in Fig. 7.

As shown in Fig. 7 (a), the transaction throughput of all three methods gradually increase with the number of concurrent users. Among them, the propsed method reaches a stable value of 4,500 transactions/s when the concurrent users are 8,000. The SCMAM method reaches a stable value of 2,900 transactions/s when the concurrent users are 6,000 users. In contrast, the NSA method shows an abnormal decrease when the concurrent users are 8,000. In Fig. 7 (b), the system has a time threshold of 2,000 ms for transaction confirmation delay time when facing different transaction volumes. The delay time of the research method is generally below the time threshold, with only 1,750 ms for transaction confirmation delay time when the transaction volume is 100 thousand transactions. Among the other two methods, the transaction confirmation time of the SCBAM method and the NSA method ultimately exceeds the time threshold, but the NSA method shows an abnormal decrease when the transaction volume is 80 thousand transactions. Overall, compared to the comparative methods, the research method has better system scalability and concurrency resistance. Based on the above content, a systematic optimization is carried out from four aspects to achieve high transaction throughput: blockchain architecture design, consensus mechanism optimization, data sharding technology, and lightweight encryption computing. (1) The platform adopts a layered design of business, information, and strategic chains, and each chain processes financial transactions of different priorities in parallel, and automates the execution process through smart contracts. (2) On the Hyperledger Fabric platform, Kafka/Raft consensus algorithm is used to replace traditional Proof-of-Work (PoW). (3) The NTRUEncrypt algorithm is based on lattice cryptography and has the characteristics of high computational efficiency and small key size. It supports direct operation of ciphertext under homomorphic encryption. (4) High reliability data is prioritized through a credibility evaluation model, and system resource allocation is optimized using a resource dynamic configuration model. These technical measures work together to enable the system to maintain a high throughput of 4,500 transactions per second even when the number of concurrent users reaches 8,000, which is significantly better than the comparative solution. Next, the study compares the cracking time of the three methods using different key lengths, as well as the consensus achievement time when facing different consensus types. The results are shown in Fig. 8.

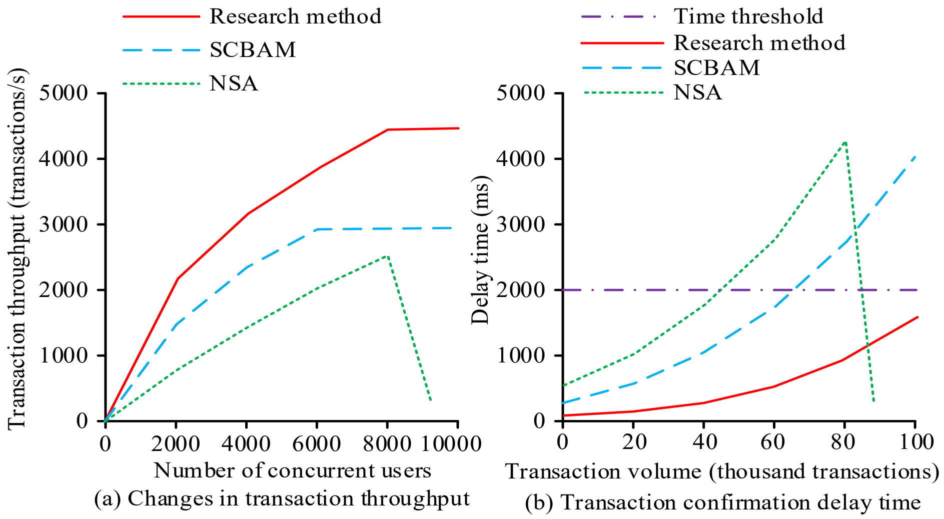


Fig. 7. Transaction throughput and transaction confirmation delay time

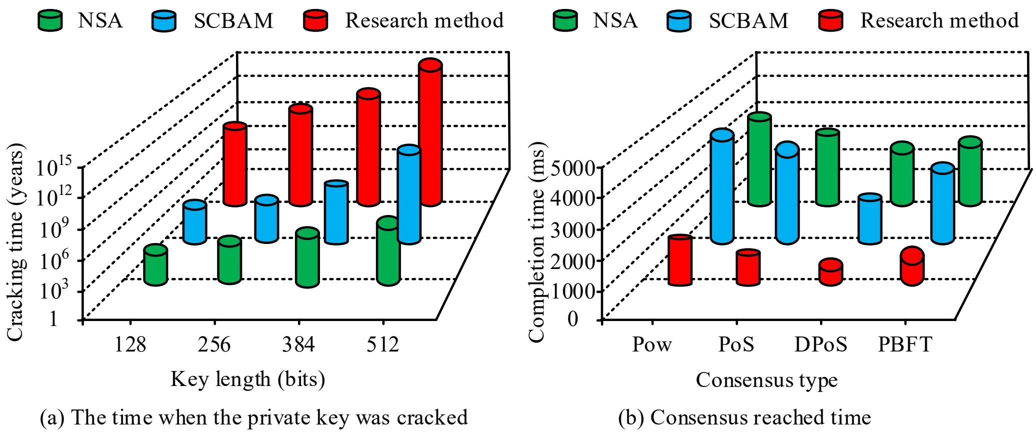
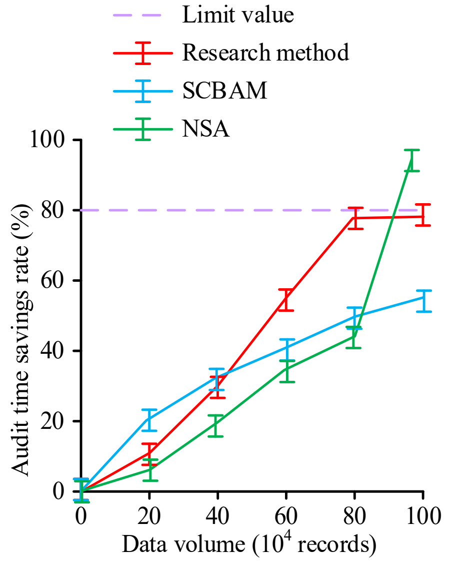


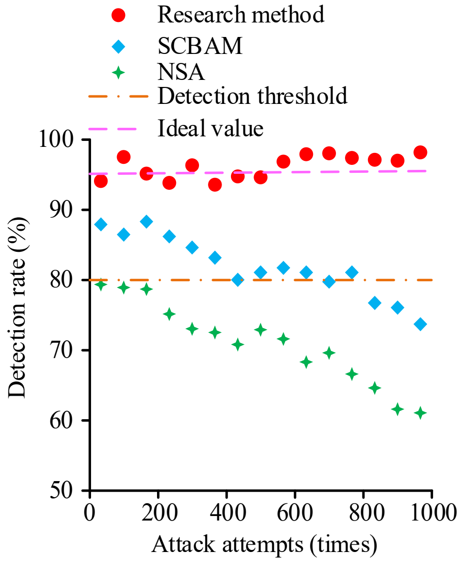
Fig. 8. Time for private key cracking and consensus reaching

Fig. 8 (a) shows that the keys for cracking time in all three methods increase with key length. The cracking time of the private key is approximately 5.6 * 107 years, 9.9 * 108 years, 5.2 * 2010 years, and 6.7 * 2014 years when the key length is 128 bits, 256 bits, 384 bits, and 512 bits. The cracking time for the other two methods are significantly lower across all keys lengths. Fig. 8 (b) compares consensus achievement times. The proposed method achieves consensus in 1,780 ms, 980 ms, and 120 ms for workload, equity, and delegated equity proofs, compared to520 ms for a Byzantine Fault-Tolerant (BFT) consensus. The NSA and SCBAM methods achieve consensus in significantly longer times than the research method for different types of consensus. These results demonstrate the superior security and consensus efficiency of the proposed method. The comparison of audit times and data tampering detection rates of all three methods for different data volumes and attack attempts is shown in Fig. 9.

As shown in Fig. 9 (a), the maximum audit time saving rate is 80%, with the remaining 20% being rigid time-consuming tasks such as manual review and communication. As the amount of data increases, the overall audit time savings rate of research methods gradually increases. At a data volume of 800,000, the proposed method's saving rate plateaus at 79.8%, which is infinitely close to the maximum value. The audit time saving rate of SCBAM at a data volume of 1 million is only 58.6%, significantly lower than the research method. The audit time savings rate of NSA sharply increases when the data volume is 800,000, and eventually exceeds the maximum value, resulting in obvious system errors. In Fig. 9 (b), the ideal data tampering detection rate is 95%, and the detection threshold is 80%. The proposed method shows the overall detection rate of data tampering in the face of different attack strategies around the ideal value. Its detection rate is generally above 90%. The detection rate of SCBAM is distributed below the detection threshold when the number of attack attempts is 800-1000, while the overall detection rate of NSA is distributed below the security threshold. This demonstrates the proposed method's superior efficiency and dynamic defense capabilities. In summary, the proposed Blockchain-based EFISP and EC solutions demonstrate high efficiency, security, and robustness.



(a) Efficiency improvement rate of financial audit



(b) Data tampering detection rate

Fig. 9. Efficiency improvement rate of financial audit and data tampering detection rate

4.2. The Actual Application Effect of EFISP and EC Solutions

Following the performance verification, this study further validated the proposed method in a practical application. This study uses a publicly available dataset of desensitized enterprise finance to build a secure blockchain sharing and EC collaborative verification platform for enterprise finance. The research methods are compared with SCBAM and NSA. Fig. 10 shows the financial error and audit variance rates for the three methods over the system's operational timeline.

As shown in Fig. 10 (a), both the financial error rate and audit variance rate for the proposed method decrease over time. When the system runs for one month, the financial error rate of the research method is 5.0%, the audit variance rate is 4.0%, and both decrease rapidly with the increase of system running time. After nine months, these values stabilize at 0.3%, and 0.2%, respectively. In Fig. 10 (b), SCBAM's financial error rate fluctuates persistently between 3.0% and 4.0%, with an audit variance rate consistently greater than 2.0%, indicating platform instability. In Fig. 10 (c), the financial error rate of NSA slowly decreases and eventually reaches a stable value of 0.9% after 9 months of system operation. However, its audit variance rate begins to increase after three months of system operation, showing a divergence phenomenon. Overall, proposed methods delivers superior data quality and compliance. Fig. 11 compares the transaction volumes successfully processed by three methods under different concurrent loads, as well as the data synchronization time across varying numbers of nodes.

Fig. 11 (a) shows the transaction processing success rate under concurrent load. The ideal scenario is a linear relationship with a slope of 1.The proposed method's performance curve closely approximates this ideal line without any anomalies. When the concurrent transaction volume is 4,000 transactions/s, the transaction volume of SCBAM stabilizes at 3,400 transactions/s and does not continue to rise. The successful processing of transaction volume by NSA shows an abnormal decrease in the curve of concurrent transaction volume when the concurrent transaction volume is 4,000 transactions per second. Fig. 11 (b) presents data synchronization times,with a system threshold of 200 ms. The data synchronization time of the proposed method is 45 ms, 58 ms, 89 ms, and 99 ms when the number of nodes is 10, 40, 70, and 100. The other two methods have significantly longer data synchronization times across all node counts. The data synchronization time of SCBAM exceeds the system's time threshold when there are 100 nodes, while NSA remains above the system's time threshold overall. These results confirm the superior stability and scalability of the proposed method. Fig. 12 compares the labor cost savings rates over the system's operational timeline and the storage cost distributions at different data scales for the three methods.

As seen in Fig. 12 (a), the system achieves a break-even point when the labor cost savings rate reaches 15%. After 5 months of system operation, the manpower savings rate of the proposed method exceeded 15%, and continued to increase with the increase in system operation time. By the time the system was running for 20 months, it had reached 47.8%. Among the other two methods, the labor cost savings rate of the SCMAM method began to decline after 12 months of system operation, while the labor cost savings rate of the NSA method reached a stable value of 14.9% after 12 months of system operation. In Fig. 12 (b), the industry's storage cost benchmark is 3 yuan/GB/month. The overall distribution of storage costs under different scales of data is below the industry benchmark value, and as the scale of data increases, the distribution of storage costs gradually decreases, eventually approaching 0.5 yuan/GB/month. In the other two methods, when the data volume exceeds 3,000 GB, the overall storage cost of the SCBAM method is distributed above the industry benchmark value. The overall distribution of storage costs for NSA methods is above industry benchmark values for data volumes of different scales. Overall, this research method provides enhanced cost optimization effects and storage efficiency in comparison to other methods. Fig. 13 compares the success rates of three methods in resisting different attack intensities, as well as their compliance coverage under different regulatory types.

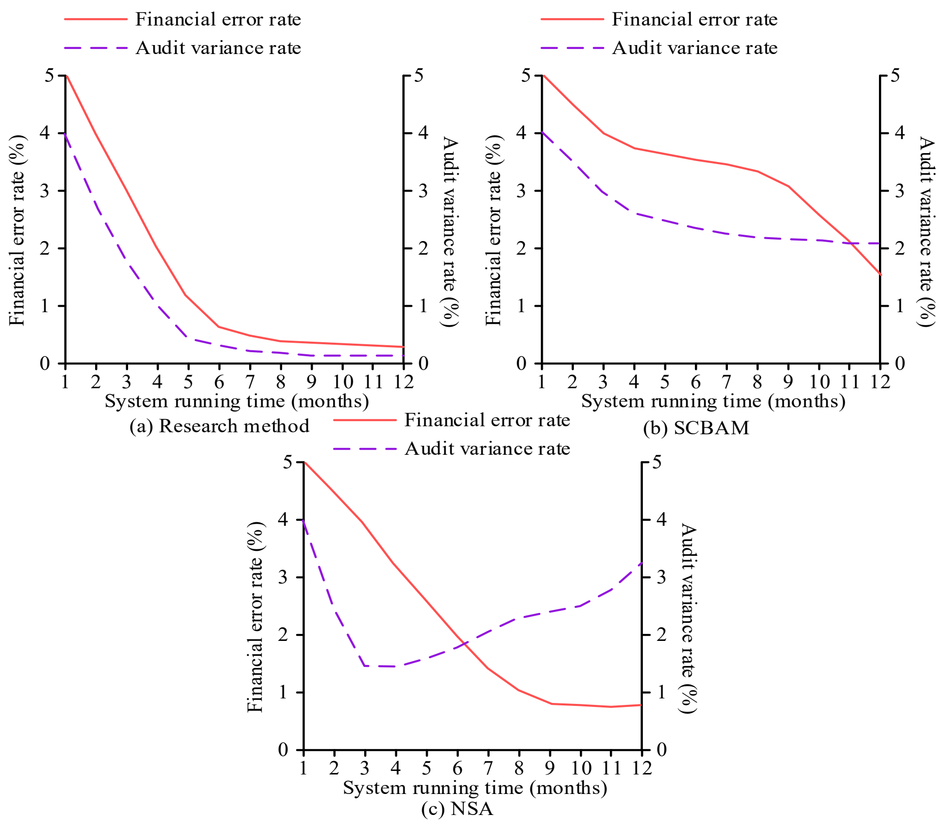


Fig. 10. Data quality and compliance status

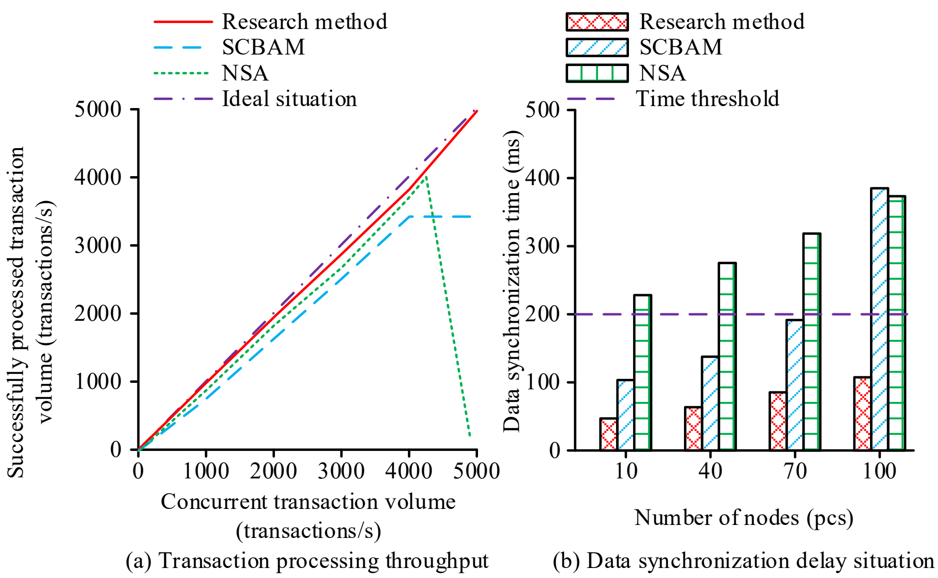
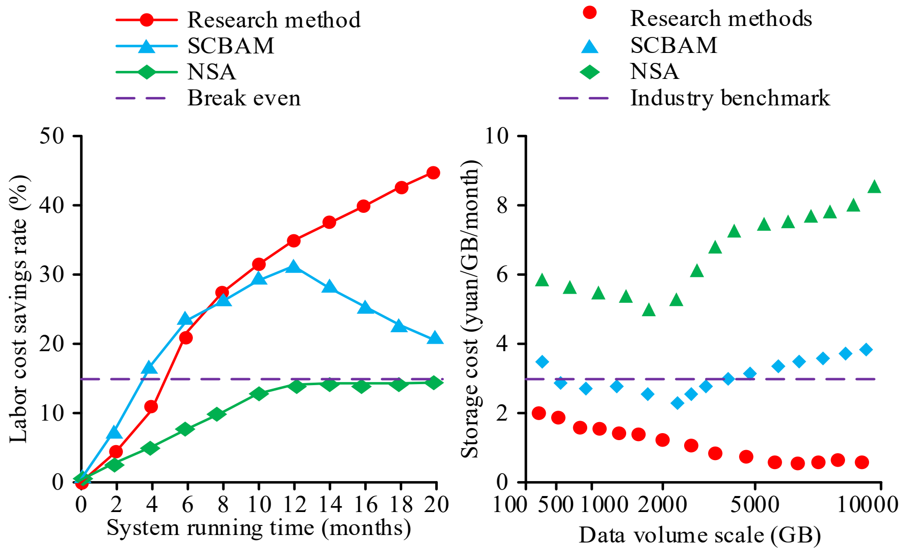
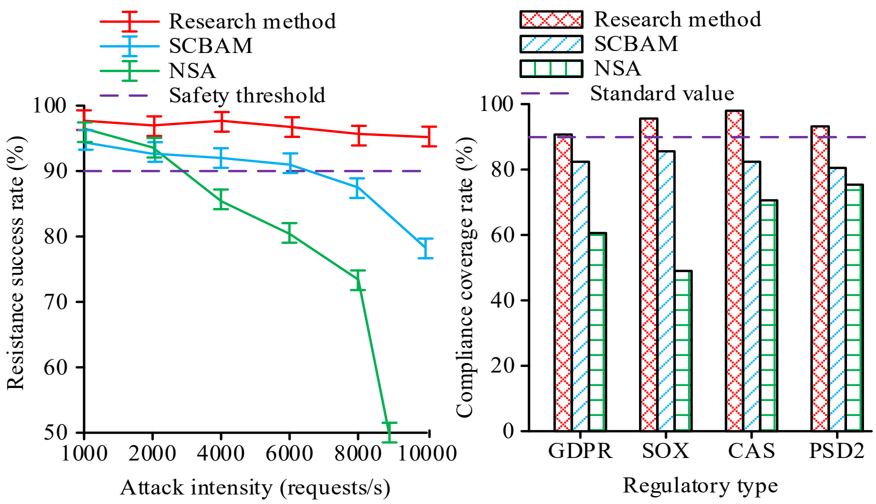


Fig. 11. Transaction processing throughput and data synchronization delay



(a) Changes in labor cost savings rate (b) Growth of storage expenses

Fig. 12. Labor cost savings rate and storage expense growth



(a) Attack resistance success rate (b) Regulatory compliance rate

Fig. 13. Success rate of attack defense and regulatory compliance situation

In Fig. 13 (a), the security threshold for the success rate of system defense is 90%. The overall success rate of the proposed method in resisting different attack intensities is above the security threshold. When the attack intensity is 1,000 and 10,000 requests/s, the success rates of the research method's defense are 96.8% and 94.6%, with the latter only decreasing by 2.2%. The success rate of SCBAM defense gradually decreases with the increase of attack intensity, and drops below the security threshold when the attack intensity is 6,800 requests/s. The success rate of NSA defense drops above the security threshold when the attack intensity is 2,900 requests/s, and rapidly drops below 50% when the attack intensity is 8,000 requests/s. In Fig. 13 (b), the system has a compliance coverage rate of 90% for different types of regulations. The compliance coverage rate of various regulatory types in the research method is above the standard value. The compliance coverage rates of the research methods for the *General Data Protection Regulation, Sarbanes Oxley Act, Chinese Enterprise Accounting Standards,* and *Revised Payment Services Directive* are 90.8%, 95.3%, 99.4%, and 93.5%. The compared method has significantly lower compliance coverage for different types of regulations in comparison to the research method, and is consistently lower than the standard compliance coverage. The proposed method has superior security and compliance. Overall, the proposed EFISP and EC solutions based on blockchain technology have exceptional data quality, compliance, stability, scalability, cost optimization effects, storage efficiency, and security.

5. Discussion

5.1. The Significance of Research Results

The proposed enterprise financial information security sharing and encryption calculation scheme based on blockchain technology has achieved a 79.8% audit time saving rate, due to the synergistic effect of the inherent characteristics of blockchain technology and encryption calculation. First, the distributed ledger and immutability of blockchain ensured the authenticity and integrity of financial data, eliminating the need for auditors to repeatedly verify data sources and significantly reducing data verification time. Second, smart contracts enabled automated execution of audit processes, such as automatic reconciliation, compliance checks, and abnormal transaction tagging, replacing traditional manual review processes. In addition, the traceability of blockchain enabled every transaction on the audit chain to be quickly traced, improving audit transparency and response speed. Finally, the encryption calculation module supported auditing related calculations directly in ciphertext state through the homomorphic properties of the NTRUEncrypt algorithm, which protects data privacy and avoids time overhead and security risks during the decryption process. The comprehensive application of these technologies has shifted audit work from "post-inspection" to "real-time monitoring", thereby achieving efficient savings in audit time. The financial error rate was as low as 0.3%, and the audit variance rate was only 0.2%, thanks to data encryption and permission control, as well as the platform's embedded error prevention mechanism during the design phase. Smart contracts automatically executed financial rules, avoiding omissions in manual processing. Real-time data verification and a cross-organizational node consensus mechanism ensured the consistency of business data. Meanwhile, the immutability of blockchain prevented errors that may arise from tampering afterwards. These mechanisms worked together to upgrade the platform from a "data security layer" to a "business quality control layer"which significantly improved the accuracy and compliance of enterprise financial information.

5.2. Comparison with Existing Research

Compared to similar solutions, the proposed method had significant advantages in efficiency, safety, and cost. The stable transaction throughput of SCBAM was only 2,900 transactions/s, and the audit time savings rate was less than 60%. The NSA experienced an abnormal decrease in data volume of 800,000, resulting in instability. The throughput of the research method reached 4,500 transactions/s, with an audit savings rate of 79.8%. Through the distributed ledger and smart contract automation of blockchain technology, the system's operating costs have been effectively reduced, and its scalability and compliance have been improved. The private key cracking time of the research method was 6.7 * 10^14 years when the key length was 512 bits, far exceeding that of SCBAM and NSA. This method utilized NTRUEncrypt's lattice-based encryption mechanism, combined with trust evaluation and encryption protocol, to achieve multidimensional protection and enhance the security of the system.

5.3. Limitations of Research and Deployment Challenges

The proposed blockchain-based EFISP and EC scheme has demonstrated high efficiency, security, and cost advantages in performance testing and practical applications. However, when deployed on a large-scale in actual enterprise environments, there are still multiple challenges, mainly reflected in the three levels of technology, law, and regulation. The technical challenges: (1) Existing financial systems of enterprises are mostly based on heterogeneous platforms and databases, and integration with blockchain platforms requires unified data standards and interface protocols. (2) In high-concurrency and large-scale cross-organizational scenarios, blockchain consensus mechanisms may introduce latency, affecting real-time processing efficiency of financial data. (3) Homomorphic encryption and multi-party secure computation involve a large number of polynomial operations, which require high computational resources and energy consumption. Legal and compliance challenges: (1) The plan must comply with regulations such as the General Data Protection Regulation (GDPR) and the Cybersecurity Law of the People's Republic of China. However, cross-border data sharing may face jurisdiction conflicts and data localization requirements. (2) The automatic execution mechanism of smart contracts has a connection problem with traditional contract law, and its legal effect and dispute resolution mechanism are not yet clear in most countries, which may lead to compliance risks. Regulatory and standardization challenges: (1) The application of blockchain technology in the financial sector is still in a regulatory gray area. (2) Currently, there is a lack of unified blockchain financial data formats, encryption algorithm standards, and cross-chain protocols. (3) For small and medium-sized enterprises, the technical investment and labor costs required for blockchain node deployment, key management, and system maintenance are relatively high. Therefore, future research should focus on lightweight blockchain architecture, cross-chain interoperability protocols, and AI-driven dynamic compliance engines to improve the systems overall practicality and usability.

5.4. Comprehensive Benefits and Broad Appeal of Research

The proposed EFISP scheme based on blockchain and EC demonstrates significant comprehensive benefits in technical performance, economic benefits, and social value. (1) In technical performance, the solution achieves process automation and data immutability through the distributed ledger and smart contracts of blockchain. Combined with the homomorphic encryption capability of NTRUEncrypt algorithm, it ensures the privacy and integrity of data during sharing and computation. (2) In economic benefits, the plan significantly reduces the operating costs of enterprises in data storage, human resource auditing, and compliance management. (3) In social value, the plan supports COC and ecological co-construction, which helps to break down "data silos", promote transparency and standardization in scenarios such as supply chain finance, tax collaboration, and joint auditing, and is in line with the national policy guidance on data element marketization and network security legislation. Moreover, enterprise managers can use this platform to enhance financial management efficiency and risk control capabilities. Technical developers can conduct secondary development and integration based on their open-source frameworks. Policy and regulatory agencies can refer to its architecture design to promote industry data sharing standards. The academic community can further explore the integration and application of blockchain and cryptography in finance based on this foundation. Therefore, the proposed method has strong appeal to a wider audience.

5.5. Cross-Disciplinary and Cross-National Applicability of Research Results

The study proposes a blockchain-based solution for secure sharing and EC of enterprise financial information, which is suitable for enterprise financial management scenarios and has broad potential for cross-disciplinary and cross-border applications. Its cross-domain applicability includes four aspects: (1) In supply chain finance, research solutions can achieve trustworthy sharing of financial data between upstream and downstream enterprises in the supply chain through blockchain, improving financing efficiency and risk control capabilities. (2) In healthcare, the research scheme combines the homomorphic encryption feature of NTRUEncrypt to achieve privacy protection and cross-institutional collaborative analysis of patient medical records. (3) In public governance, research plans can enhance data transparency and audit efficiency, supporting the construction of a "digital government". The cross-border applicability is reflected in two aspects: strong adaptability to technological infrastructure and the ability to cope with cultural and management differences.

6. Conclusion

This study innovatively proposed an EFISP and EC solution based on blockchain technology to address the problems of high single-point of failure risk and easy data tampering or leakage in traditional financial information systems that rely heavily on centralized architecture. This study constructed EFISP using blockchain technology and combined it with the NTRUEncrypt algorithm achieving secure EC. In the experiment, when the transaction volume was 100 thousand transactions, the transaction confirmation delay time of the research method was only 1,750 ms. Moreover, the data synchronization time of the research method was only 99 ms when the number of nodes was 100. When the system ran for 20 months, the labor cost savings rate of the research method reached 47.8%. These results indicate that the proposed platform ensures data security through blockchain and encryption technology, and proactively reduces business level errors in financial processing through mechanisms such as smart contracts, real-time auditing, and process automation. The platform's full process intervention from data generation, transmission, to storage and auditing has achieved a transformation from "passive protection" to "active prevention and control", providing systematic support for the accuracy and reliability of enterprise financial management. Overall, the proposed method has effectively improved operational efficiency, security, and robustness of the EFISP.

Funding

The research is supported by the General Project of Philosophy and Social Sciences Research in Jiangsu colleges and universities, “Innovations in Teacher Assessment Reform for Vocational Colleges in the New Era” (Project Number 2024SJYB0704).

Institutional Review Board Statement

Not applicable.

Declaration of Artificial Intelligence (AI) Tools

The author confirmed that no AI tools were used in the preparation of this manuscript.

References

Abrahams, O., Ewuga, K., Kaggwa, S., Uwaoma, U., Hassan, O., and Dawodu, O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews*, 20(3), 1743-1756.

Ahmad, S., Mehfuz, S., Urooj, S., and Alsubaie, N. (2024). Machine learning-based intelligent security framework for secure cloud key management. *Cluster Computing*, 27(5), 5953-5979. DOI: 10.1007/s10586-024-04288-8.

Akram, W., Joshi, R., Haider, T., Sharma, P., Jain, V., Garud, N., and Singh, N. (2024). Blockchain technology: A potential tool for the management of pharma supply chain. *Research in Social and Administrative Pharmacy*, 20(6), 156-164. DOI: 10.1016/j.sapharm.2024.02.014.

Bag, S., Rahman, S., Gupta, S., and Wood, C. (2023). Understanding and predicting the determinants of blockchain technology adoption and SMEs' performance. *The International Journal of Logistics Management*, 34(6), 1781-1807. DOI: 10.1108/ijlm-01-2022-0017.

Chittipaka, V., Kumar, S., Sivarajah, U., Bowden, H., and Baral, M. (2023). Blockchain technology for supply chains operating in emerging markets: an empirical examination of technology-organization-environment (TOE) framework. *Annals of Operations Research*, 327(1), 465-492. DOI: 10.1007/s10479-022-04801-5

Gad, G., Mosa, T., Abualigah, L., and Abohany, A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University-Computer and Information Sciences*, 34(9), 6719-6742.

Garai, S., Paul, K., Kumar, M., and Choudhury, A. (2023). Intra-annual national statistical accounts based on machine learning algorithm. *Journal of Data Science and Intelligent Systems*, 2(2), 12-15. DOI: 10.47852/bonviewjdsis3202870.

Haque, M., Kumar, V., Singh, P., Goyal, A., Upreti, K., and Verma, A. (2023). A systematic meta-analysis of blockchain technology for educational sector and its advancements towards education 4.0. *Education and Information Technologies*, 28(10), 13841-13867. DOI: 10.1007/s10639-023-11744-2.

Kala, M. (2023). The impact of cyber security on business: how to protect your business. *Open Journal of Safety Science and Technology*, 13(2), 51-65.

Khan, A., Mubarik, S., Kusi-Sarpong, S., Gupta, H., Zaman, I., and Mubarik, M. (2022). Blockchain technologies as enablers of supply chain mapping for sustainable supply chains. *Business strategy and the environment*, 31(8), 3742-3756. DOI: 10.1002/bse.3029.

Khan, S., Haleem, A., Husain, Z., Samson, D., and Pathak, D. (2023). Barriers to blockchain technology adoption in supply chains: the case of India. *Operations Management Research*, 16(2), 668-683. DOI: 10.1007/s12063-023-00358-z.

Kouhizadeh, M., Zhu, Q., and Sarkis, J. (2023). Circular economy performance measurements and blockchain technology: an examination of relationships. *The International Journal of Logistics Management*, 34(3), 720-743.
Li, X. (2022). An evolutionary game-theoretic analysis of enterprise information security investment based on information sharing platform. *Managerial and Decision Economics*, 43(3), 595-606. DOI: 10.1002/mde.3404.
Liu, W., Liu, X., Shi, X., Hou, J., Shi, V., and Dong, J. (2023). Collaborative adoption of blockchain technology: A supply chain contract perspective. *Frontiers of Engineering management*, 10(1), 121-142.
Luo, N., Yu, H., You, Z., Li, Y., Zhou, T., Jiao, Y., Han, N., Liu, C., Jiang, Z., and Qiao, S. (2023). Fuzzy logic and neural network-based risk assessment model for import and export enterprises: A review. *Journal of Data Science and Intelligent Systems*, 1(1), 2-11. DOI: 10.47852/bonviewjdsis32021078.
Lv, Z., Chen, D., Cao, B., Song, H., and Lv, H. (2023). Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins. *IEEE Transactions on Computers*, 73(3), 656-668.
Malik, N., Appel, G., and Luo, L. (2023). Blockchain technology for creative industries: Current state and research opportunities. *International Journal of Research in Marketing*, 40(1), 38-48.
Manzoor, R., Sahay, S., and Singh, K. (2025). Blockchain technology in supply chain management: an organizational theoretic overview and research agenda. *Annals of Operations Research*, *348*(3), 1307-1354.DOI: 10.1007/s10479-022-05069-5.
Mojisola, O., Misra, S., Febisola, F., Abayomi-Alli, O., and Sengul, G. (2022). An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). *Egyptian Informatics Journal*, 23(2), 291-301.
Naik, S. (2023). Cloud-based data governance: ensuring security, compliance, and privacy. *The Eastasouth Journal of Information System and Computer Science*, 1(01), 69-87.
Nour, B., Pourzandi, M., and Debbabi, M. (2023). A survey on threat hunting in enterprise networks. *IEEE communications surveys & tutorials*, 25(4), 2299-2324. DOI: 10.1109/comst.2023.3299519.
Prados-Castillo, F., Guaita Martinez, M., Zielińska, A., and Gorgues Comas, D. (2023). A review of blockchain technology adoption in the tourism industry from a sustainability perspective. *Journal of Theoretical and Applied Electronic Commerce Research*, 18(2), 814-830. DOI: 10.3390/jtaer18020042.
Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.
Weerawarna, R., Miah, S., and Shao, X. (2023). "Emerging advances of blockchain technology in finance: a content analysis," *Pers. Ubiquitous Comput.,* 27(4), 1495-1508, DOI: 10.1007/s00779-023-01712-5.
Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., and Al Ghamdi, M. A. (2022). Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management*, 70(8), 2874-2890.
Savelyeva, T. and Park, J. (2022). Blockchain technology for sustainable education. *British Journal of Educational Technology*, 53(6), 1591-1604.
Sharif, U. and Mohammed, A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, 15(1), 138-156.
Singireddy, S., Adusupalli, B., Pamisetty, A., Mashetty, S., and Kaulwar, K. (2024). Redefining financial risk strategies: The integration of smart automation, secure access systems, and predictive intelligence in insurance, lending, and asset management. *Journal of Artificial Intelligence and Big Data Disciplines*, 1(1), 109-124.
Wang, L. and Wang, Y. (2022). Supply chain financial service management system based on block chain IoT data sharing and edge computing. *Alexandria engineering journal*, 61(1), 147-158.
Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., and Zhang, W. (2023). A survey on federated learning: challenges and applications. *International journal of machine learning and cybernetics*, 14(2), 513-535. DOI: 10.1007/s13042-022-01647-y.
Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A., and Luzcando, E. (2022). Practical adoption of cloud computing in power systems—Drivers, challenges, guidance, and real-world use cases. *IEEE Transactions on Smart Grid*, 13(3), 2390-2411. DOI: 10.1109/tsg.2022.3148978.
Zhou, K. (2023). Financial model construction of a cross-border e-commerce platform based on machine learning. Neural Comput. Appl., 35(36), 25189-25199. DOI: 10.1007/s00521-023-08456-6.

Jiayun Wu earned her Bachelor of Science in accounting and financial management from Soochow University (2005) and her LL.M. from Jiangnan University in Wuxi (2011). She currently serves as an associate researcher as well as the deputy director of the Human Resources Department at Wuxi Vocational Institute of Commerce. She also actively gained hands-on experience in accounting through frontline roles at various companies. Building on working and practical experience, she has published more than 10 academic papers. Her research interests include human resource management, human resource cost management and accounting information management.