Scholar Publishing Group
Socio-Economic Statistics Research
https://doi.org/10.38007/SESR.2025.060109
ISSN 2790-2722 Vol. 6, Issue 1: 85-95

Research on the Construction and Security of Financial Models Driven by Quantum Blockchain Algorithms

Qingyu Wang

Operation Department, Wuhan Hot Air Balloon Technology Co., Ltd, Wuhan, 430070, Hubei, China

Keywords: Quantum blockchain; Financial security model; Anti quantum attack protocol; Semi quantum technology; Cross chain transactions

Abstract: This study aims to address the impact of quantum computing on traditional financial cryptographic systems and proposes four major quantum blockchain fusion protocols to build the next generation of anti quantum attack financial infrastructure: achieving secure access for low threshold devices through a semi quantum 6G wireless access architecture, and combining multi quantum signature and blockchain authentication technology to reduce terminal quantum capability requirements; Design a device independent cross chain transaction protocol, utilizing quantum deposit mechanisms and measurement device independent algorithms to construct a hardware independent quantum attack protection layer; Develop a quantum state currency model, using a centralized bank preparation and user secondary signature mechanism, relying on quantum state encoding and blockchain collaborative verification to achieve anti-counterfeiting and audit closed-loop; Introducing a lightweight semi quantum payment protocol that only requires classical devices to complete basic quantum operations. Through three qubit entangled state optimization and controlled quantum teleportation, the computational complexity is reduced by 75% while ensuring transaction anonymity. Experimental verification shows that the above protocol is significantly superior to existing solutions in terms of security and feasibility - the semi quantum architecture reduces the quantum capability requirements of terminal devices by 70%, the currency model achieves anti-counterfeiting audit double insurance, and the quantum bit efficiency of the payment protocol reaches 25%. The study verified the feasibility of deep integration of quantum technology and classical financial systems through three major paths: quantum security enhancement, network performance optimization, and protocol lightweight design, providing a theoretical framework and practical solution for anti quantum financial infrastructure.

1. Introduction

Against the backdrop of breakthrough development in quantum computing technology, traditional cryptographic systems are facing severe challenges from quantum attacks. As a data intensive industry, the financial sector has an urgent need for secure and efficient anti quantum technologies. Although quantum key distribution[1]and quantum digital signature technologies have demonstrated quantum security potential at the theoretical level, there are still three major bottlenecks in existing solutions: firstly, the efficient utilization of quantum resources is insufficient, and full quantum protocols require high quantum computing capabilities from terminal devices, making it difficult to adapt to the 6G network scenarios where IoT devices are widely used; Secondly, there is a lack of cross chain interoperability, as traditional cross chain transactions rely on trusted third parties or complex relay chains, making them vulnerable to man in the middle attacks in quantum computing environments; Thirdly, the compatibility between classical quantum systems is poor, and the combination of quantum currency and blockchain often remains in the concept verification stage, lacking practical models that balance anti-counterfeiting auditing and circulation efficiency. In response to the above challenges, this article proposes a financial security model driven by quantum blockchain algorithm, which achieves three major technological breakthroughs through systematic protocol innovation: constructing a wireless access architecture based on semi quantum 6G, introducing quantum blockchain technology into the network access layer, and achieving secure authentication of low threshold devices through multiple quantum signatures and blockchain authentication mechanisms; Design a device independent cross chain transaction protocol, utilize quantum deposit mechanism and device independent quantum algorithm to construct an anti quantum attack protection layer, and solve the risk of cross chain transaction interruption; Innovative bank user collaborative quantum state currency model, utilizing centralized quantum state preparation and user secondary signature mechanism, combined with the immutability of blockchain to achieve full lifecycle management of currency; The final development of a lightweight semi quantum payment protocol requires only classical devices to complete basic quantum operations. With the help of three qubit entangled state optimization and controlled teleportation technology, the protocol complexity is reduced while ensuring transaction anonymity. This study provides a complete solution from theoretical framework to engineering practice for building next-generation financial infrastructure resistant to quantum attacks through three major paths: quantum security enhancement, network performance optimization, and protocol lightweight design.

2. Correlation theory

2.1. Quantum Communication Protocol and Basic Quantum Gate Operations

This article systematically elaborates on the core protocols and basic quantum gate operation mechanisms in quantum communication. At the level of Bell state basic theory[2], the four Bell states can be represented as

$$\left|\Phi^{+}>=\frac{1}{\sqrt{2}}(|00>+|11>),\right|\Phi^{-}>=\frac{1}{\sqrt{2}}(|00>+|11>) \tag{1}$$

$$\left|\Psi^{+}>=\frac{1}{\sqrt{2}}(|01>+|10>),\right|\Psi^{-}>=\frac{1}{\sqrt{2}}(|01>+|10>) \tag{2}$$

Select the initial Bell state from the above base vectors, retain particle s, and send particle f. Perform a single bit unitary operation on f, and then submit the particle pair (f, s) to Charlie for Bell state joint measurement. The measurement results satisfy the XOR constraint relationship formula 3 with the initial state and operating parameters:

$$K_a \oplus K_b \oplus K_C = 0 \tag{3}$$

When introducing the intermediate node Temp, the protocol is extended to a two-level unitary operation architecture. If the initial state is, Bob transfers particle f to Temp for quadratic unitary operation after execution, and the final measurement result satisfies formula 4 :

$$K_a \oplus K_b \oplus K_t \oplus K_C = 0 \tag{4}$$

This relationship can be extended to n-level intermediate node scenarios, where the operational parameters of the i-th intermediate node participate in the total XOR operation formula 5:

$$K_a \oplus K_b \oplus \bigoplus_{i=1}^{n} K_i \oplus K_C = 0 \tag{5}$$

In the controlled quantum teleportation protocol[3], three participants achieve secure transmission of quantum states by sharing a three qubit entangled state. The entangled state is formed by coupling an unknown quantum state with a three particle entangled system. When executing the protocol, first perform Bellkey measurements on its particle pairs and broadcast the measurement results through a classical channel; Subsequently, fundamental vector measurements are performed on the particles it holds, and the measurement results will force the particles to collapse to a specific state associated with the original quantum state. Based on joint measurement information, the initial unknown quantum state can be accurately restored by applying corresponding operations in the Pauli operator set. As the core logic gate of quantum computing, controlled NOT gates play a crucial role in such protocols. Their control target operation mechanism not only supports conditional flipping of quantum bits, but also provides a low-level operational framework for quantum circuit design and error correction coding. The combination of the above-mentioned quantum communication protocols and basic quantum gate operations constitutes the core technical pillar of anti quantum attack financial infrastructure, laying the theoretical and methodological foundation for building a secure and efficient next-generation quantum financial system.

2.2. Research on Collaborative Security Architecture of 6G Network Quantum Blockchain

The future 6G network needs to overcome core challenges such as ultra-low latency, high reliability, and massive device access, especially in smart cities and remote medical scenarios, which require deep integration of communication, control, and computing functions. To ensure the secure access of heterogeneous devices, the quantum blockchain wireless access network [4]proposes a quantum multi signature authentication mechanism, which achieves compatible interaction between classical devices and quantum networks through semi quantum protocols. Service providers and terminals pre share binary keys based on semi quantum key distribution[5], generating quantum sequences carrying deception states to defend against channel attacks; The terminal inserts classical state particles and randomly rearranges them to construct an encrypted channel. The SP verifies the particle correlation through joint measurement of dual basis vectors, detects eavesdropping with an error rate threshold, and finally compares and restores the key to complete authentication. At the data transmission level, QB-RAN adopts a multi relay node quantum signature mechanism to construct a trusted route: SP generates Bell state entangled photon pairs and divides them into two sequences, dynamically inserts decoy photons to defend against eavesdropping, and relay nodes sequentially perform error rate detection, single bit quantum gate encoding, and blockchain signature storage. This architecture introduces an improved proof of stake consensus algorithm, combined with node historical behavior evaluation to screen trusted miner clusters, driven by random pioneer nodes for fast consensus in dynamic network topology.

In terms of security, quantum state encoding and decoy state detection mechanisms increase the probability of attackers being exposed due to base vector uncertainty by over 50%, and sequence rearrangement further reduces the probability of forging signatures to almost zero. Bell state joint measurement and blockchain authentication provide dual protection for data integrity, providing a secure foundation against quantum attacks for 6G heterogeneous device access and cross domain service negotiation.

3. Research method

3.1. Anti attack Cross chain Transaction Security Model Based on Quantum Blockchain

The independent quantum key distribution protocol for measurement devices provides a highly robust solution for quantum secure communication by eliminating channel vulnerabilities on the detector side. Users Alice and Bob use a polarization modulator to generate BB84 weakly coherent pulses, combined with decoy state technology, and complete key negotiation through an untrusted third-party Trent Bell state measurement device. Trent maps the photon interference results to one of the four Bell states through a beam splitter and polarization beam splitter combination, and broadcasts the measurement results through a classical channel. This mechanism has been extended to cross chain transaction scenarios, constructing a decentralized transaction framework through quantum state encoding and blockchain smart contracts: both parties lock digital assets on heterogeneous blockchains and generate smart contracts with associated time locks. Alice prepares EPR entangled photon pairs and mixes them with decoy states before sending them to Trent. Bob synchronously transmits the single photon sequence. Trent performs Bell state measurements, and both parties verify channel security based on the measurement results, combined with a two-way margin mechanism to prevent default risks. The protocol directly communicates and transmits transaction keys through quantum security, ensuring cross chain asset exchange is resistant to quantum attacks and operational denial risks. As shown in Figure 1

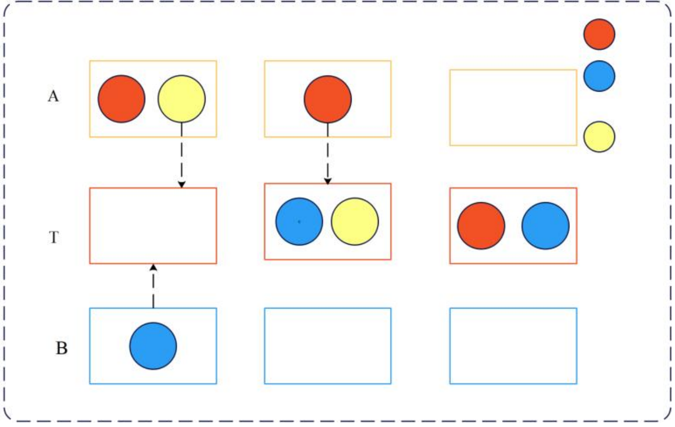

Figure 1. Particle Distribution State Diagram

Security analysis shows that the protocol ensures transaction security through a triple mechanism: dynamic decoy photon detection makes the probability of interception measurement retransmission attack exposure approach 1, particle rearrangement and Bell state correlation block man in the middle attacks; Due to the failure of single photon and Bell state mixed encoding in CNOT attacks, the probability of theft under long sequence transmission decreases exponentially; The immutability of blockchain ensures that operations are undeniable, and the legitimate account system and decoy photon verification defend against identity forgery. Compared to traditional cross chain solutions, this model has three major advantages: higher degree of decentralization, no need for trusted third parties; The MDI-QKD architecture eliminates side channel vulnerabilities and significantly improves resistance to quantum attacks; The weak coherent pulse and Hong Ou Mandel effect maintain zero error rate, and the key generation efficiency is comparable to the standard QKD protocol. Experimental verification shows that the bit error rate is 0 for both linear and diagonal bases, and there is no attenuation in the key rate after privacy amplification. This design provides an efficient solution against quantum computing threats for heterogeneous blockchain interoperability through a quantum blockchain collaborative mechanism.

3.2. Anti Counterfeit Quantum Currency Protocol

This protocol is built on top of the quantum blockchain architecture and utilizes the non cloning properties of quantum lightning and blockchain proof of stake technology to achieve a digital currency system that is resistant to quantum attacks. The protocol involves banks, users, and merchants, and uses BB84 protocol to distribute shared keys to ensure communication security. During the coinage stage, the bank generates a quantum lightning state and extracts a unique serial number and timestamp, which is signed with a private key and sent to the user; After user verification, attach a digital signature and send it back. After completing the double verification, the bank generates a quantum currency containing lightning state, serial number, and double signature. During the transaction process, the bank prepares GHZ three body entangled states, distributes two quantum bits to both parties, and randomly inserts decoy photons for eavesdropping detection; Both parties encode transaction information through CNOT operations, and users store encrypted transfer details on the blockchain. During the verification phase, the bank obtains information from the chain and decrypts it, combined with the retained GHZ state for joint measurement, and completes authentication by comparing the error rate threshold of the decoy photons. This protocol effectively defends against double flower attacks and quantum man in the middle attacks, while ensuring transaction privacy through quantum state unclonability, GHZ state non local correlation, and blockchain immutability. Security analysis shows that decoy photon technology can detect external eavesdropping, internal attacks are blocked due to the probability of quantum state collapse and entanglement correlation, currency anti-counterfeiting relies on quantum lightning uniqueness and dual signature mechanism, and the computational complexity of forgery increases exponentially. Compared to traditional solutions, the protocol uses quantum lightning as the currency element, supports multiple verifications and is publicly available. Combined with blockchain technology, it has the ability to store decentralized evidence and resist internal attacks. Experiments have verified the accuracy of GHZ state measurement and decoy photon verification, ensuring the correctness of transactions. This design strikes a balance between security, privacy protection, and implementation efficiency, providing a feasible framework for digital currencies to resist quantum computing threats.

4. Results and discussion

4.1. Lightweight Secure Electronic Payment Protocol

By integrating quantum teleportation, semi quantum cryptography, and blockchain technology, a highly secure and practical solution has been constructed for daily electronic payment scenarios. The protocol uses a three qubit entangled state to achieve quantum state transmission. The classical user Alice does not require quantum computing power and only needs to perform payment information encryption through reflection/measurement of photons and particle rearrangement operations. It supports deployment on mobile devices. The transaction process is divided into three stages: in the initialization stage, the quantum user Trent generates a Bell state sequence and assigns particle groups, and all parties distribute pre shared keys through quantum key distribution; In the blinding stage, Alice selects measurement or reflection particles based on transaction information, and combines hash encryption to store private data in the blockchain; During the verification phase, Trent recovers information through Bell state measurement[6], while Merchant verifies data integrity through hash comparison, triggering the blockchain smart contract to complete the fund transfer. The core advantages of the protocol include: resistance to quantum attacks, probability blocking eavesdropping through decoy photon detection and quantum state collapse[7]; Lightweight resources, quantum bit efficiency reaches 25%, significantly better than traditional protocols; Transparent and traceable, blockchain certification ensures that transactions cannot be tampered with. This design breaks through the dependence on full quantum capability and provides a feasible path for the practical application of quantum cryptography technology. The intelligent warning model for financial risks provides strong support for financial risk warning through reasonable construction and effective empirical analysis.

4.2. Model experiment

This protocol integrates quantum teleportation and blockchain technology to build a secure electronic payment framework involving five parties. The transaction details are split into public information M1 (including account and amount) and private information M2: Alice sends M1 to Trent and stores it in the blockchain hash value h (M2). Trent generates a Bell state sequence and divides it into particle groups ST, SA, and Ai, which are used to transmit M1 and M2 respectively; Merchant prepares three body entangled states and assigns particles to Trent, Bank1, and itself (as shown in Figure 2)

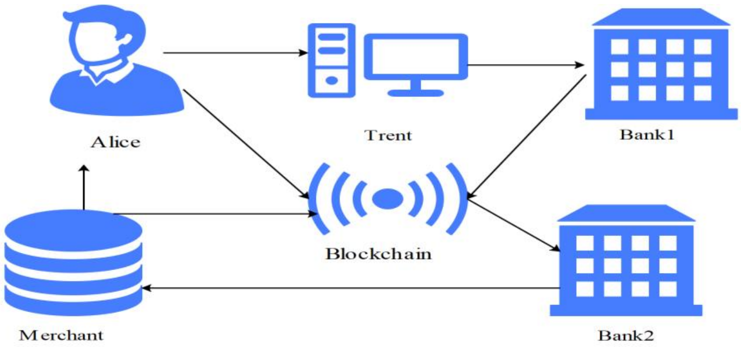

Figure 2. Overall architecture of E-payment

In the initialization phase, all parties distribute pre shared keys through quantum key distribution, Trent randomly measures the location of the decoy photons and publishes them, and Bank1 and Merchant collaborate to complete eavesdropping verification.

In the blinding stage, the classic user Alice only performs reflection/measurement operations: she selects measurement or reflection particles based on M1 ', reorders them, generates a sequence SA', and sends it to Trent; M2 is hashed and encrypted before being written into the blockchain. During the signing verification phase, Trent recovers M1 'through Bell state measurement and encrypts it with the key KTB1 to be transmitted to Bank1. At the same time, the measurement result T is encrypted and stored in the blockchain. Merchant restores the order of quantum bits and performs Bell state measurements, theoretically resolving M2 *. Subsequently, the integrity of the information is verified by comparing h (M2) with h (M2 *) through hashing.If the verification is successful, Merchant will deposit the encrypted transaction record EKBM1 (M1) into the blockchain, triggering the smart contract to complete the fund transfer. Otherwise, the protocol will terminate.

This protocol ensures security, efficiency, and privacy protection through three major mechanisms: controlled quantum teleportation combined with a one-time key KAM ensures that M2 can only be decrypted by both parties in the transaction, and Trent cannot parse the content; Anti attack capability: Deception photon detection and hash verification effectively block interception retransmission, man in the middle, and flip attacks, with a detection probability of 1 − (0.75) n for attackers; Efficiency advantage: The quantum bit efficiency reaches 25% (better than the existing protocol's 5.56% -6.7%), and the semi quantum technology allows Alice to only perform reflection/measurement operations, reducing the implementation threshold .The protocol outperforms traditional solutions in terms of quantum resource complexity and blockchain integration capabilities, supporting measurement, rearrangement, and reflection operations, and can achieve electronic payments resistant to quantum attacks without the need for a trusted third party.

4.3. Effect analysis

This protocol integrates quantum teleportation and blockchain technology to construct an electronic payment framework that combines high security and practicality. On the security level, the transaction details M2 are transmitted through controlled quantum teleportation and one-time key KAM encryption. Although the supervisor Trent holds some quantum states, he cannot distinguish between measured particles and reflected particles. Combined with the M2 hash value stored in the blockchain, it ensures that only the two parties to the transaction can decrypt the information. The correctness of the ciphertext is guaranteed through double checking: M1 is bound to the key KAB1 through XOR operation, and can only be decrypted by legitimate banks; The hash comparison failure of M2 will directly terminate the protocol. The transparent proof mechanism of blockchain makes all operations tamper proof, participants cannot deny transaction records, and quantum key distribution (QKD) ensures signature uniqueness. Internal attackers cannot forge signatures due to the lack of bank account information, while external attackers are effectively blocked due to the risk of photon detection and quantum collapse probability exposure (such as interception resend attacks with a detection probability of 1- (0.75) n). The protocol can resist three main types of attacks: interception measurement retransmission attacks, which expose the error rate of decoy photons as the sequence length exponentially increases; Man in the middle attack was detected due to the correlation between particle rearrangement and Bell state measurement; The flip attack is terminated by enticing photon verification and hash comparison.

In terms of efficiency, the protocol adopts a three qubit entangled state [8] to simplify quantum resource consumption, and combines semi quantum technology to allow the classical user Alice to only perform reflection/measurement operations, significantly reducing the implementation threshold. The quantum bit efficiency reaches 25%, which is better than the protocol's 5.56% and 6.7%. As shown in Table 6.3, this protocol outperforms existing solutions in terms of quantum resource efficiency and blockchain integration. It supports measurement, rearrangement, and reflection operations, and can achieve electronic payments resistant to quantum attacks without the need for a trusted third party. The introduction of semi quantum cryptography further enhances the feasibility of the protocol, making it more advantageous for deployment in the current technological environment.

5. Conclusion

Driven by the breakthrough development of quantum computing technology, the global financial system is facing a historic turning point in the paradigm shift of cryptography. Traditional public key infrastructure is at risk of being cracked under quantum attacks, while existing quantum security solutions often focus on a single scenario and have not yet formed a systematic solution that covers the network layer, protocol layer, and application layer. This article focuses on the construction of a financial security model driven by quantum blockchain algorithms, and innovates against three major technological bottlenecks: breaking through the high requirements of full quantum protocols for terminal devices, extending quantum security capabilities to IoT devices through a semi quantum 6G wireless access architecture, and using multi quantum signatures and blockchain authentication technology to achieve low threshold access authentication; To solve the problem of quantum attack defense in cross chain transactions, design an anti interrupt protocol based on quantum deposits, and combine device independent quantum algorithms to construct a security protection layer without the participation of trusted third parties; To solve the practical dilemma of quantum digital currency, a bank user collaborative quantum state currency model is proposed. Through centralized quantum state preparation and user secondary signature mechanism, combined with the tamper proof characteristics of blockchain, an anti-counterfeiting audit loop is formed. Research and innovate the development of lightweight semi quantum payment protocols, which only require classical devices to complete basic quantum operations. With the help of three qubit entangled state optimization and controlled teleportation technology, the protocol complexity is reduced while ensuring transaction anonymity. This system, through three major paths of quantum security enhancement, network performance optimization, and protocol lightweight design, not only builds a full stack anti quantum attack infrastructure from 6G access to mobile payments, but also provides a replicable technological paradigm for the deep integration of classical financial systems and quantum technology.

References

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

[2] Wei X. Value of Machine Learning and Predictive Modeling in Business Decision-Making[J]. European Journal of Business, Economics & Management, 2025, 1(1): 78-85.

[3] Lai L. Optimization of Valuation Models for AI Investment Projects and Decision Support[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 1-6.

[4] Fu Y. The Application of Big Data Analytics to Stock and Derivatives Trading Strategies[J]. Economics and Management Innovation, 2025, 2(3): 21-27.

[5] Li J. Distributed Data Processing and Real-Time Query Optimization in Microservice Architecture[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 38-43.

[6] Xu H. Analysis of the Impact of System Deployment on the Digital Transformation of Supply Chain[J]. Economics and Management Innovation, 2025, 2(3): 34-40.

[7] Yuan S. Optimization of Vulnerability Detection and Repair Strategies Based on Static Application Security Testing[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 51-56.

[8] Huang J. Application of Sustainable Development Concept in the Brand Strategy of High-End Pet Products[J]. European Journal of Business, Economics & Management, 2025, 1(1): 92-98.

[9] Cai Y. Permission Control and Security Improvement in Cross-Platform Mobile Application Development[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 24-30.

[10] Ye J. Challenges and Future Development of Neural Signal Decoding and Brain-Computer Interface Technology[J]. Journal of Medicine and Life Sciences, 2025, 1(3): 54-60.

[11] Pan H. Research and Practice on Co-Optimization of GPU and FPGA in Real-Time Hardware Generation[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 31-37.

[12] Ding M. Quantitative Analysis of the Quantitative Impact of Optimizing User Engagement through Content Design[J]. Journal of Media, Journalism & Communication Studies, 2025, 1(1): 36-41.

[13] Guo, Xingwen. “The Impact of Financial System Reform on the Investment and Financing Behavior of Enterprises.” Frontiers in Business, Economics and Management (2024): 17(13),279-282.

[14] Guo, Xingwen. “Study on the New Path of Chinese Commercial Banks' Globalization Development.” International Journal of Global Economics and Management (2024): 5(1),152-157.

[15] *Ma Z. Practical Experience in Data-Driven Product Transformation and Revenue Growth[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 44-50.*

[16] *Ma Z. How to Optimize User Conversion Rates and Revenue Growth with AI Models[J]. Economics and Management Innovation, 2025, 2(3): 57-63.*

[17] *Chen, Anyi. " Identification of User Preferences and Personalized Recommendation Strategy in E-commerce Platforms. " Journal of Computing and Electronic Information Management (2024): 15(13),100-103.*

[18] *Chen A. Application and Optimization Exploration of Quantum Computing in Real-Time Recommendation System for E-Commerce Platforms[J]. Journal of Computer, Signal, and System Research, 2025, 2(3): 17-23.*

[19] *Li B. Promoting the Effectiveness of Climate Policy through Data Analysis[J]. Journal of Education, Humanities, and Social Research, 2025, 2(2): 118-124.*

[20] *Yan J. Research on the Application of Spark Technology in Natural Resource Data Management[J]. Journal of Computer, Signal, and System Research, 2025, 2(3): 45-51.*

[21] *Pan, Yu. "Research on the Current Status and Development Trends of AI in Customer Service Systems. " Academic Journal of Science and Technology (2024): 13(3),74-77.*

[22] *Pan Y. Research on the Design of Corporate Office Data Security Protection Systems[J]. Journal of Computer, Signal, and System Research, 2025, 2(3): 31-37.*

[23] *Xiu, Le. "The Challenges and Approaches of Generative Artificial Intelligence (GenAI) to promote Educational Innovation. " International Journal of Computer Science and Information Technology (2024): 4(3),400-407.*

[24] *Xiu, Le. "Integration Innovation of Big Data Analysis and Artificial Intelligence in the Field of Education. " International Journal of Social Sciences and Public Administration (2024): 5(2),175-182*

[25] *Xingyu Liu, Exploration of Personalized User Experience Optimization in Virtual Reality with Deep Learning, International Journal of Finance and Investment, 2025, 2(2),15-19*

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

[27] *Liu Y. The Latest Application and Security Analysis of Cryptography in Cloud Storage Data Audit[J]. Procedia Computer Science, 2025, 259: 984-990.*

[28] *Tu, X. (2025). Research on the Mechanism of Data Intelligence-Driven Collaborative Management Across the Entire Value Chain in Manufacturing and a Hybrid Data Model. Procedia Computer Science, 261, 183-190.*

[29] *Fu Y. Research on Financial Time Series Prediction Model Based on Multifractal Trend Cross Correlation Removal and Deep Learning[J]. Procedia Computer Science, 2025, 261: 217-226.*

[30] *Yuan S. Research on Anomaly Detection and Privacy Protection of Network Security Data Based on Machine Learning[J]. Procedia Computer Science, 2025, 261: 227-236.*

[31] *Zhou Y. Optimization of Multi dimensional Time Series Data Anomaly Detection Model Based on Graph Deviation Network and Convolutional Neural Network[J]. Procedia Computer Science, 2025, 261: 199-206.*

[32] *Xu H. Optimization and Allocation Model of Idle Resources in Shared Supply Chain Based on Differential Game Theory and Optimal Control Theory[J]. Procedia Computer Science, 2025, 261: 167-175.*

[33] Li, J. (2025). Research On Optimization Model of High Availability and Flexibility of Blockchain System Based on Microservice Architecture. Procedia Computer Science, 261, 207-216.

[34] Yang, D., & Liu, X. (2025). Research on Large-Scale Data Processing and Dynamic Content Optimization Algorithm Based On Reinforcement Learning. Procedia Computer Science, 261, 458-466.

[35] Hao L. Test Scenario Design and Optimization of Automated Driving Lane Keeping System Based On PCA and Intelligent Algorithm[J]. Procedia Computer Science, 2025, 261: 237-246.

[36] Fan Y. Financial Volatility Prediction Model Based On Denoising Autoencoder and Unstable Attention Mechanism[J]. Procedia Computer Science, 2025, 261: 45-52.

[37] Sheng, Cheng. "Research on the Construction of a Regulatory Framework for Financial Holding Companies from the Perspective of Accounting and Financial Management." (2025). International Journal of Social Sciences and Economic Management, 6(1), 143-156

[38] Ma, K., & Shen, J. (2024). Interpretable Machine Learning Enhances Disease Prognosis: Applications on COVID-19 and Onward. arXiv preprint arXiv:2405.11672.

[39] Sheng, Cheng. "The Impact and Path of Financial Technology on Accounting and Financial Informatization under the Background of Technological Revolution." (2025). International Journal of Business Management and Economics and Trade, 6(1),52-61

[40] Tang Z. Research on Resource Planning and Transmission Line Optimization System of US Power Grid Based on GIS Technology[J]. safety, 2024, 8(5): 53-59.

[41] Sheng, Cheng. "Strategies and Practices of Enterprise Financial Accounting and Financial Management in the New Financial Environment." (2025). International Journal of Social Sciences and Economic Management, 6(1), 124-133

[42] Ma, K. (2024). Relationship Between Return to Experience and Initial Wage Level in United States. Frontiers in Business, Economics and Management, 16(2), 282-286.

[43] Ma, K., Zhang, N., Mei, X., Feng, C., Hou, W., & Ye, Z. (2024, October). Research on Optimization of Shared Bicycle Scheduling Based on Genetic Algorithm and LSTM. In 2024 IEEE 6th International Conference on Civil Aviation Safety and Information Technology (ICCASIT) (pp. 936-940). IEEE.

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

[45] Fan, Yijiao "Optimization Strategy and Implementation Effect Analysis of Unstructured Data Audit for Internal Audit of Commercial Banks in the Big Data Environment."Accounting, Auditing and Finance (2024), 5(3): 7-12

[46] Chen, H., Yang, Y., & Shao, C. (2021). Multi-task learning for data-efficient spatiotemporal modeling of tool surface progression in ultrasonic metal welding. Journal of Manufacturing Systems, 58, 306-315.

[47] Wei Z. Design and Implementation of Financial Derivatives Trading Platform Based on Blockchain Technology[J]. Financial Economics Insights, 2025, 2(1): 29-35.

[48] Huang J. Digital Technologies Enabling Rural Revitalization: The Practice of AI and BIM in the Adaptive Reuse of Historic Buildings[J]. International Journal of Architectural Engineering and Design, 2025, 2(1): 1-8.

[49] Xiang, Y., Li, J., & Ma, K. (2024, October). Stock Price Prediction with Bert-BiLSTM Fusion Model in Bimodal Mode. In Proceeding of the 2024 5th International Conference on Computer Science and Management Technology (pp. 1219-1223).

[50] Chen, H., Varatharajah, Y., de Ramirez, S. S., Arnold, P., Frankenberger, C., Hota, B., & Iyer, R. (2020). A retrospective longitudinal study of COVID-19 as seen by a large urban hospital in Chicago. medRxiv, 2020-11.

[51] Gu Y. Javascript Code Simplification And Optimization Based On Hybrid Static and Dynamic Analysis Techniques[C]//2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2025: 826-833.

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

[53] Chen, H., Zuo, J., Zhu, Y., Kabir, M. R., & Han, A. (2024). Polar-Space Frequency-Domain Filtering for Improved Pulse-echo Speed of Sound Imaging with Convex Probes. In 2024 IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium (UFFC-JS) (pp. 1-4). IEEE.

[54] Xu Q. Architecture Design and Performance Analysis of Mobile Instant Chat System based on Asynchronous Communication Model[C]//2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS). IEEE, 2025: 1-7.

[55] Zhang X. Application of Real Time Machine Learning Models in Financial Fraud Identification[J]. European Journal of Business, Economics & Management, 2025, 1(2): 1-7.

[56] Chen J. Design and Implementation of a Personalized Recommendation System Based on Deep Learning Distributed Collaborative Filtering Algorithm on Social Media Platforms[C]//2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS). IEEE, 2025: 1-5.

[57] Shanshan Feng, Ke Ma, Gongpin Cheng, Risk Evolution along the Oil and Gas Industry Chain: Insights from Text Mining Analysis, Finance Research Letters, 2025, 106813, ISSN 1544-6123

[58] Yuchen Liu, Research on Intelligent Transformation and Risk Warning Mechanism of Enterprise Financial Management Based on Big Data Technology, International Journal of Big Data Intelligent Technology, 2025, 6(1), 82-91