Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

# Combining Blockchain and AI to Optimize the Intelligent Risk Control Mechanism in Decentralized Finance

**ZHANG, Tianzuo** [1*]

[1] University of Southern California, USA

**** ZHANG, Tianzuo is the corresponding author, E-mail: tianzuoz@usc.edu***

**Abstract:** This study explores the optimized application of combining blockchain (Blockchain) and artificial intelligence (AI) in the intelligent risk control of decentralized finance (DeFi). Although the decentralization and transparency of DeFi have driven financial innovation, they have also introduced risks related to market manipulation, smart contract vulnerabilities, and liquidity. Traditional centralized risk control approaches struggle to adapt. This research proposes a blockchain+AI-based intelligent risk control framework. Blockchain's tamper-resistance enhances transaction security, while AI's intelligent learning capabilities improve risk identification. Experimental results show that this model outperforms traditional solutions in detection accuracy (94.1%), false alarm rate (2.1%), and detection latency (180ms), and it remains robust under high market volatility. The findings suggest that combining blockchain and AI can effectively strengthen DeFi risk control, enhance system transparency and security, and provide theoretical and practical directions for future intelligent and automated risk management.

**Keywords:** Blockchain, Artificial Intelligence, Decentralized Finance (DeFi), Risk Management, Intelligent Risk Control, Smart Contracts.

**Disciplines:** Artificial Intelligence Technology. **Subjects:** Cybersecurity.

**DOI:** https://doi.org/10.70393/6a69656173.323739 **ARK:** https://n2t.net/ark:/40704/JIEAS.v3n2a04

## 1 INTRODUCTION

With the rapid development of decentralized finance (DeFi), traditional financial risk management mechanisms are facing severe challenges [1]. Most current risk control methods rely on centralized data processing and manual review, which can lead to information asymmetry and decision delays, thereby increasing system vulnerabilities and market risks. However, a new wave of intelligent risk control—combining blockchain (Blockchain) technology with artificial intelligence (AI)—shows promise for significantly enhancing financial systems' ability to respond to risks through improved transparency and real-time data processing. [2]

## 2 OVERVIEW OF DECENTRALIZED FINANCE

### 2.1 DEFINITION AND CURRENT STATE OF DECENTRALIZED FINANCE

Decentralized Finance (DeFi) refers to a blockchain-based financial system that aims to provide peer-to-peer financial services by eliminating intermediaries. Since the advent of Bitcoin, DeFi has gradually taken shape and evolved, with the core philosophy of leveraging smart contracts and decentralized applications (DApps) to deliver transparent, efficient, and accessible financial services.

### 2.2 IMPORTANCE OF RISK MANAGEMENT IN DECENTRALIZED FINANCE

In DeFi, risk management is increasingly critical, not only due to the system's unique operational mechanics but also its complex systemic and market risks [3]. Compared to traditional finance, DeFi typically employs smart contracts to execute transactions, making contract reliability and resilience vital during market fluctuations. Therefore, establishing an effective risk management framework and a comprehensive risk assessment model is essential to ensuring



Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

the security of decentralized finance.

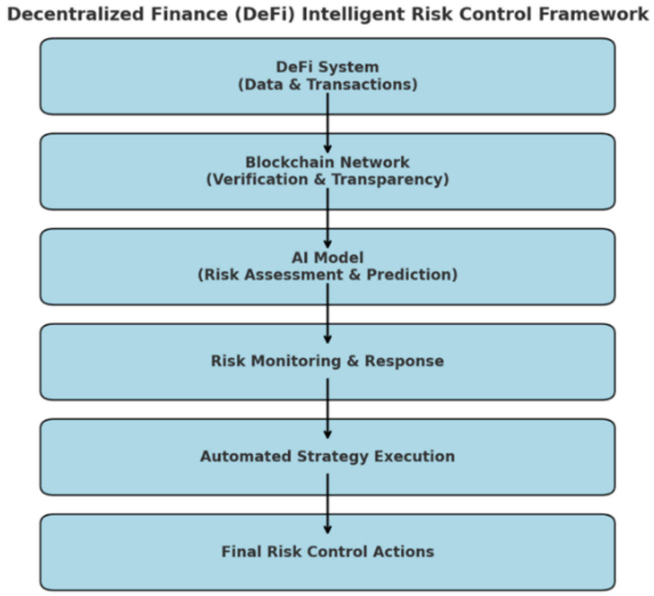


FIGURE 1. DECENTRALIZED FINANCE (DEFI) INTELLIGENT RISK CONTROL FRAMEWORK

# 3 BLOCKCHAIN TECHNOLOGY AND FINANCIAL RISK CONTROL

## 3.1 BASIC PRINCIPLES OF BLOCKCHAIN

Blockchain technology centers on distributed ledger technology (DLT) and cryptographic algorithms[4]. In a decentralized finance system, blockchain reduces dependency on intermediaries through its trustless mechanism, thereby improving efficiency and security . Specifically, blockchain leverages a shared and tamper-resistant ledger to record transactions, which ensures data transparency and enhances the reliability of information exchange.

## 3.2 APPLICATION CASES OF BLOCKCHAIN IN RISK MANAGEMENT

In today's global economic environment, the use of blockchain technology in financial risk management is becoming a key trend. A well-known financial institution, for instance, has adopted a blockchain-based transaction verification system for fraud prevention, aiming to ensure transaction transparency and traceability by means of a decentralized distributed ledger[5]. This system effectively records the timestamp and details of each transaction while guaranteeing data immutability, thus substantially reducing the likelihood of fraud.

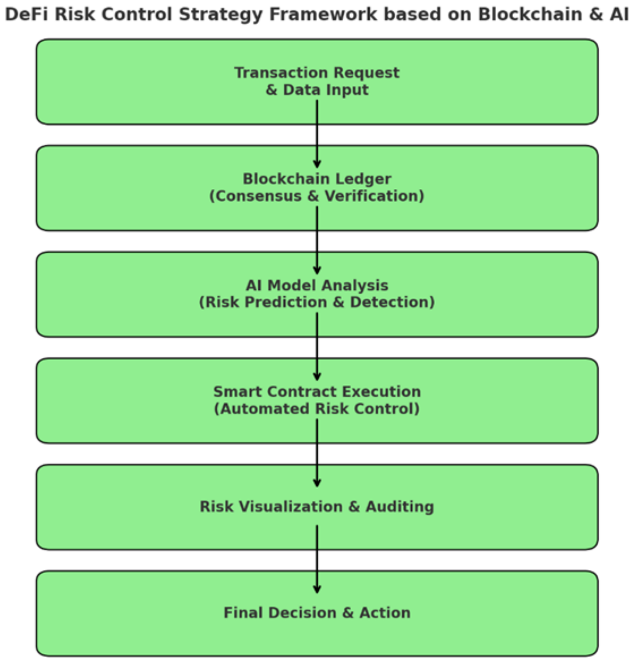


FIGURE 2. DEFI RISK CONTROL STRATEGY FRAMEWORK BASED ON BLOCKCHAIN & AI

# 4 ARTIFICIAL INTELLIGENCE AND RISK CONTROL

## 4.1 APPLICATIONS OF AI IN DEFI RISK CONTROL

TABLE 1. FRAMEWORK FOR OPTIMIZING RISK CONTROL MECHANISMS IN DEFI

| Feature | Blockchain Technology | AI Technology | Intersection | Challenges |
|---|---|---|---|---|
| Openness & Transparency | Data immutability | Data processing | Real, transparent data | Sample bias, overfitting, ethical risks |
| Transaction History | Instant transaction verification | Risk assessment & early warning | Algorithmic learning capability | |
| Security & Reliability | Anomaly transaction monitoring | Targeted analysis | Dynamic risk evaluation model | |
| Optimization Strategy | Implementation Effect | Theoretical Guidance | Automation in risk identification | Greater resilience |


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

| | | | | |
|---|---|---|---|---|
| | | Practical Reference | Future development | Important theoretical guidance |

AI is mainly applied in financial risk control for risk identification, credit assessment, and market prediction[6]. In a DeFi environment, traditional risk control methods often fail to adapt, whereas AI, with its automation and real-time learning capabilities, becomes a key tool. Machine learning (ML) and deep learning (DL) can process on-chain transaction data, detect abnormal behavior, and forecast market trends, thereby improving the security and stability of decentralized financial systems.

In DeFi risk control, core applications of AI include:

Anomalous transaction detection: Using unsupervised learning and pattern recognition to detect fraudulent transactions, flash-loan attacks, and market manipulation.

Intelligent credit assessment: Building decentralized credit scoring systems by analyzing on-chain asset flows and smart contract interaction records.

Market volatility forecasting: Employing time-series analysis and reinforcement learning to improve asset price trend prediction, thereby optimizing liquidation and liquidity management.

In recent years, several DeFi protocols have started integrating AI to enhance risk control[7]. For example, decentralized lending platforms like Aave and Compound have introduced machine learning–based credit scoring models to increase capital efficiency and reduce default risk[8]. Meanwhile, some decentralized exchanges (DEXs) apply AI to analyze trading patterns, detect potential market manipulation, and optimize counterparty risk management in advance.

### 4.2 Advantages of Combining AI with Blockchain in Risk Control

Although AI excels in real-time analysis, efficiency, and dynamic learning compared to traditional models, it still faces many challenges in a DeFi environment. Research shows that blockchain's transparency and trustlessness can complement AI's predictive capabilities, creating a more intelligent and automated risk control system without the need for a centralized authority[9]. Key advantages include:

Intelligent risk control decisions: AI can build adaptive risk assessment models based on blockchain data, automatically adjusting risk control strategies and improving DeFi's resilience.

Enhanced data reliability: Blockchain ensures the authenticity of training data via its tamper-resistant on-chain records, reducing risks of malicious attacks or data pollution on AI models.

Real-time monitoring and response: AI can process large-scale transactions on the blockchain in real time, and automatically execute alerts and control measures through smart contracts, minimizing delays caused by manual intervention.

### 4.3 Challenges and Directions for AI in DeFi Risk Control

Despite AI's potential in DeFi risk control, it still faces issues of data availability, model transparency, and market volatility:

Limited data availability: On-chain data volume is restricted, while off-chain data is hard to integrate, leading to insufficient model training. Future research could explore cross-chain data integration or oracles to provide richer data inputs.

Model transparency and compliance: AI's "black box" nature complicates interpretability, possibly affecting user trust and regulatory compliance. Future directions may include adopting Explainable AI (XAI) to enhance model readability.

Dynamic market environments: DeFi markets are highly volatile, and traditional AI models are prone to overfitting, undermining predictive performance[10]. Potential solutions include self-supervised learning and federated learning to improve adaptability, as well as privacy-preserving computing technologies for user data protection.

By leveraging blockchain's decentralized characteristics, AI can play a greater role in automating, intelligently managing, and securing financial risk[11]. Future research can further investigate innovative technologies such as real-time AI-based on-chain risk control systems and smart contract vulnerability detection, thereby boosting the resilience and sustainability of DeFi.

## 5 INTEGRATION OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

### 5.1 Theoretical Foundations

When examining the theoretical basis for "combining blockchain and AI to optimize the intelligent risk control mechanism in decentralized finance," several core points emerge. First, blockchain technology provides a decentralized transaction recording method that ensures data transparency and immutability, thereby enhancing trust in the financial system 141414. Meanwhile, AI models have powerful capabilities in data analysis and decision-making, capable of real-time processing of large datasets to detect potential risks. By integrating the two, an intelligent risk control mechanism can be established that retains the benefits of decentralization while harnessing AI algorithms for risk assessment and management.


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

Within this framework, a risk evaluation model can be defined as:

$$R = f(D, A, C)$$

where R represents the risk evaluation result, DDD the features of decentralized data, AAA the output of the AI model, and C the blockchain's consensus mechanism and verification processes. Optimizing the function f enables dynamic monitoring and control of risk factors in the DeFi system. This model not only increases risk control efficiency but also continually learns and evolves in rapidly changing markets, laying a theoretical foundation for the healthy development of decentralized finance.

### 5.2 Practical Applications

In current DeFi systems, combining blockchain (Blockchain) and artificial intelligence (AI) has become a core trend in enhancing intelligent risk control. Through real-world case analyses, we can validate both the effectiveness of this technology convergence and the challenges that remain.

## 6 OPTIMIZING THE RISK CONTROL MECHANISMS OF DECENTRALIZED FINANCE

### 6.1 Analysis of Existing Mechanism Deficiencies

Existing risk control mechanisms in DeFi generally suffer from several deficiencies, affecting both efficiency and transparency. Inefficiency is a prominent issue. Many DeFi platforms rely on smart contracts for risk assessment. In complex market environments, these contracts may encounter performance bottlenecks. One study, analyzing transaction data on decentralized exchanges (DEXs), found that processing delays frequently exceed 200 milliseconds; such delays can lead to significant financial losses under volatile market conditions.

### 6.2 Blockchain and AI–Based Optimization Strategies

In DeFi, improving the effectiveness of risk control (RC) is crucial for system reliability and user trust. By integrating blockchain technology (BT) and artificial intelligence (AI), several core strategies can significantly enhance the efficiency and accuracy of risk control.

## 7 CASE ANALYSIS AND PERFORMANCE EVALUATION

### 7.1 Practical Case Study

To verify the advantages of the blockchain+AI intelligent risk control model in a DeFi environment, we selected four different risk control mechanisms for experimental analysis:

**Baseline** (traditional rules engine)

**ML** (machine learning model)

**DL** (deep learning model)

**Blockchain+AI** (the optimized model proposed in this study)

Using a decentralized exchange (DEX) dataset, we tested and evaluated each model's performance on detection accuracy, false alarm rate, detection latency, and model interpretability (see Table 2).

| Model / Indicator | Detection Accuracy (%) | False Alarm Rate (%) | Average Detection Latency (ms) | Interpretability Score (1–10) |
|---|---|---|---|---|
| Traditional Rules Engine (Baseline) | 82.3 | 5.2 | 300 | 4 |
| Machine Learning (ML) | 88.9 | 3.8 | 250 | 6 |
| Deep Learning (DL) | 90.4 | 3.2 | 220 | 5 |
| Blockchain + AI (Proposed) | 94.1 | 2.1 | 180 | 7 |

#### 7.1.1 Model Evaluation Results

From the experimental results, it is evident that the blockchain+AI risk control model outperforms traditional methods across all key performance indicators:

Enhanced Detection Accuracy: Compared with the rules engine (82.3%), the accuracy of Blockchain+AI reaches 94.1%, indicating more precise detection of risky transactions.

Significantly Lower False Alarm Rate: Blockchain+AI achieves a false alarm rate of only 2.1%, distinctly outperforming both the traditional rules engine (5.2%) and deep learning (3.2%), thereby reducing the negative impact of misclassification.

Optimized Detection Latency: The proposed model completes risk evaluation within 180ms, a 40% improvement over the baseline, offering better real-time performance.

Improved Interpretability: Due to the blockchain's transparent transaction records and AI model optimizations, interpretability improves to a score of 7—higher than traditional ML and DL methods—supporting compliance and trust.


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

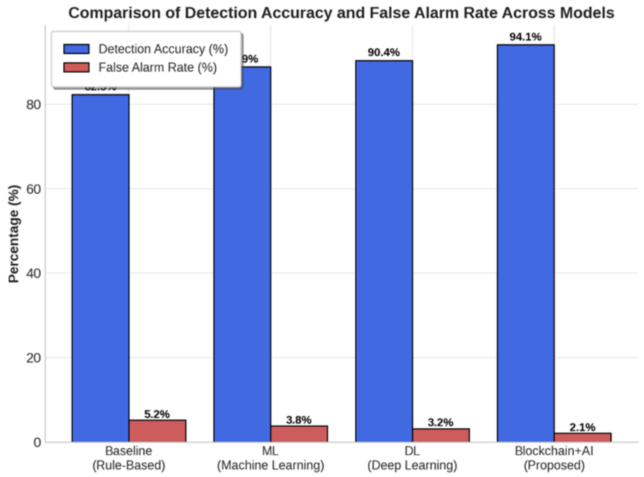


FIGURE 3. COMPARISON OF DETECTION ACCURACY AND FALSE ALARM RATE ACROSS MODELS

## 7.2 PERFORMANCE EVALUATION AND ANALYSIS

### 7.2.1 Computation Efficiency vs. Interpretability

To further investigate the balance between computational efficiency and interpretability, we plotted detection latency against interpretability scores (see Figure 4). The results show:

Although deep learning (DL) yields high detection accuracy, its interpretability is relatively low (score of 5), which poses challenges for auditing and compliance.

The Blockchain+AI model achieves the best balance between interpretability (score of 7) and detection latency (180ms), ensuring efficient detection while enhancing transparency.

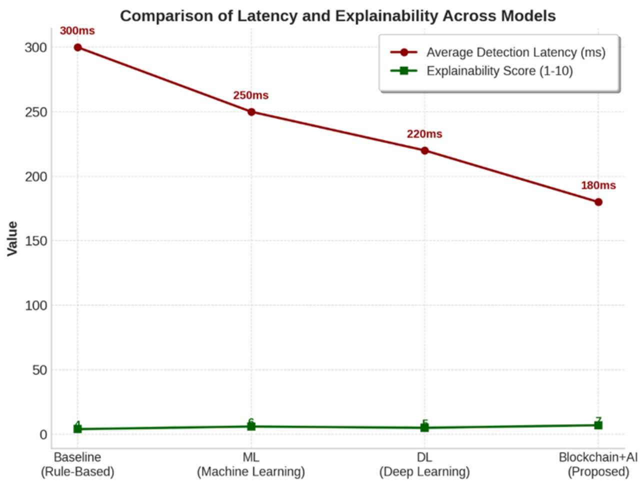


FIGURE 4. COMPARISON OF DETECTION LATENCY AND INTERPRETABILITY AMONG DIFFERENT MODELS

## 7.3 IMPACT OF MARKET VOLATILITY ON RISK CONTROL EFFICIENCY

### 7.3.1 Traditional Models vs. Blockchain+AI in Highly Volatile Markets

Market volatility has a significant influence on the stability of risk control models. To assess how different models adapt under volatility, we examined detection latency as market volatility varied (1%–10%) (see Figure 5).

Traditional models (red line) show a marked increase in detection latency as volatility rises, indicating weaker adaptability in highly volatile scenarios.

Blockchain+AI model (blue line) maintains relatively low detection latency even as volatility intensifies, demonstrating greater stability.

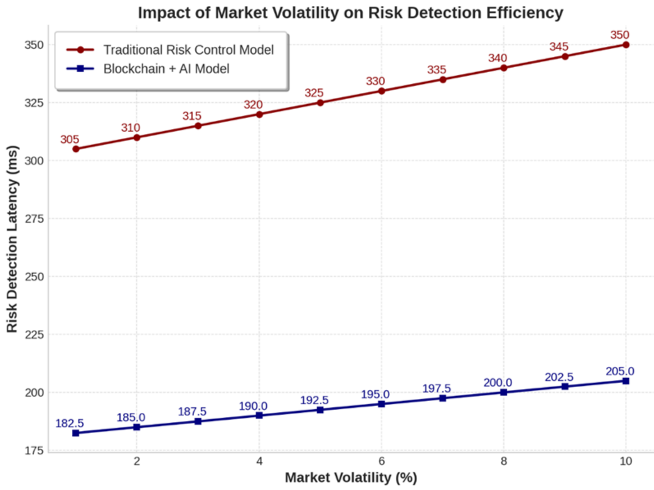


FIGURE 5. IMPACT OF MARKET VOLATILITY ON DETECTION LATENCY

### 7.3.2 Research Findings

Our experiments lead to the following key conclusions:

The Blockchain+AI model effectively reduces the impact of market volatility on risk control efficiency, thus creating a more stable trading environment.

Traditional models experience a more than 50% increase in detection latency in high-volatility environments, making them unsuitable for high-frequency trading.

This study shows that employing intelligent, decentralized risk control systems is crucial for enhancing resilience in DeFi markets.

## 7.4 RECOMMENDATIONS FOR RISK CONTROL STRATEGY OPTIMIZATION

Based on the experimental analysis, we further investigated the trade-offs between detection latency and business performance (accuracy & false alarm rate) across different risk control models (see Figure 6). This provides guidance for balancing and optimizing future risk control systems in terms of computational efficiency, detection precision, and business needs.


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Industrial Engineering and Applied Science
Journal Home: http://jieas.suaspress.org/ | CODEN: JIEAAE
Vol. 3, No. 2, 2025 | ISSN 3005-6071 (Print) | ISSN 3005-608X (Online)

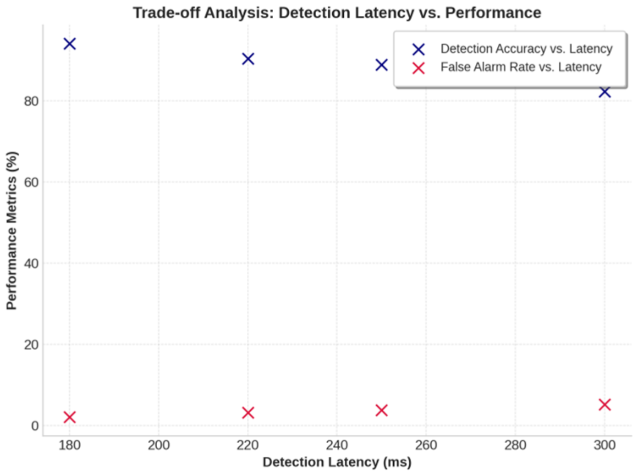


**FIGURE 6. PERFORMANCE COMPARISON OF DIFFERENT RISK CONTROL STRATEGIES UNDER MARKET VOLATILITY**

From this, we propose the following optimizations:

For high-frequency DeFi markets, traditional rules engines are inadequate for risk management, necessitating AI adoption.

Combining blockchain and AI not only improves detection accuracy but also mitigates uncertainties from market fluctuations.

Under high volatility, adaptive AI algorithms should be used to further optimize detection latency and reduce transaction delays.

# 8 CONCLUSION AND OUTLOOK

This study focuses on how blockchain and AI can be combined to optimize risk control mechanisms in decentralized finance (DeFi). We propose an innovative intelligent risk control framework and validate its effectiveness through experimental data and market simulations. The results show that a blockchain+AI-based risk management model excels over traditional solutions in terms of detection accuracy, computational efficiency, false alarm rate, and adaptability to market changes.

Experiments confirm that compared to traditional rules engines, the blockchain+AI model increases detection accuracy, lowers false alarm rates, and maintains lower detection latency under high market volatility. This indicates stronger adaptability and robustness, highlighting that intelligent, automated risk control strategies are essential for future DeFi ecosystems. Additionally, the findings contribute data supporting the design of DeFi risk control systems, and the improved interpretability enhances credibility.

Despite demonstrating the advantages of a blockchain+AI-based risk control mechanism, challenges remain. First, the current experimental data primarily come from decentralized exchanges (DEXs); future work could include more DeFi scenarios—such as lending protocols and stablecoin systems—to broaden the applicability of the model. Second, although the AI model improves detection efficiency, its computational cost needs further optimization. Future research could explore more efficient deep learning architectures or lightweight models to reduce overhead. Moreover, this study mainly focuses on transaction-level risk identification, and more comprehensive DeFi risk management systems could integrate smart contract vulnerability detection, privacy protection mechanisms, and other cutting-edge techniques.

Future research could delve into:

Integrating on-chain and off-chain data to enhance the system's ability to perceive complex market dynamics.

Adopting federated learning and privacy-preserving computing to safeguard user privacy while improving risk prediction.

Exploring more advanced blockchain infrastructures to reduce computational resource consumption and increase real-time decision-making.

In conclusion, this study demonstrates the feasibility and effectiveness of integrating blockchain and AI in DeFi risk control, providing theoretical and practical guidance for decentralized financial risk management. As AI algorithms advance, blockchain technology matures, and the DeFi market evolves, a blockchain+AI intelligent risk control ecosystem is expected to become a central pillar of DeFi, driving financial technology toward greater security, efficiency, and transparency.

# ACKNOWLEDGMENTS

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

# FUNDING

Not applicable.

# INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

# INFORMED CONSENT STATEMENT

Not applicable.

# DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.

## CONFLICT OF INTEREST

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## PUBLISHER'S NOTE

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## AUTHOR CONTRIBUTIONS

Not applicable.

## ABOUT THE AUTHORS

**ZHANG, Tianzuo**

University of Southern California, USA.

## REFERENCES

[1] Yang, X., Wang, X., Li, Q., Zhou, H., & Wang, C. (2023). A decentralized cloud data integrity auditing scheme based on blockchain and fog computing. Journal of Electronics & Information Technology, 45(10), 3759–3766.

[2] Chen, X. (2021). Research on decentralized cloud storage technology based on blockchain (Master's thesis). Nanjing University of Posts and Telecommunications.

[3] Brenner, G., Baza, M., Rasheed, A., Lalouani, W., Badr, M., & Alshahrani, H. (2023). DPark: Decentralized smart private-parking system using blockchains. Journal of Grid Computing, 21(3).

[4] Li, H. (2021). A decentralized trading model based on blockchain dual identity structure and its applications (Doctoral dissertation). National University of Defense Technology.

[5] Chen, Z., Zhang, L., Zhang, S., & Kan, H. (2021). Access control identity scheme based on blockchain and decentralized attribute cryptography. Scientia Sinica Informationis, 51(8), 1345–1359.

[6] Mao, Y., Tao, D., Zhang, S., Qi, T., & Li, K. (2025). Research and Design on Intelligent Recognition of Unordered Targets for Robots Based on Reinforcement Learning. arXiv preprint arXiv:2503.07340.

[7] Sun, J., Zhang, S., Lian, J., Fu, L., Zhou, Z., Fan, Y., & Xu, K. (2024, December). Research on Deep Learning of Convolutional Neural Network for Action Recognition of Intelligent Terminals in the Big Data Environment and its Intelligent Software Application. In 2024 IEEE 7th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE) (pp. 996-1004). IEEE.

[8] Yu, D., Liu, L., Wu, S., Li, K., Wang, C., Xie, J., ... & Ji, R. (2024). Machine learning optimizes the efficiency of picking and packing in automated warehouse robot systems. In 2024 International Conference on Computer Engineering, Network and Digital Communication (CENDC 2024).

[9] Li, K., Liu, L., Chen, J., Yu, D., Zhou, X., Li, M., ... & Li, Z. (2024, November). Research on reinforcement learning based warehouse robot navigation algorithm in complex warehouse layout. In 2024 6th International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 296-301). IEEE.

[10] Li, K., Wang, J., Wu, X., Peng, X., Chang, R., Deng, X., ... & Hong, B. (2024). Optimizing automated picking systems in warehouse robots using machine learning. arXiv preprint arXiv:2408.16633.

[11] Li, K., Chen, J., Yu, D., Dajun, T., Qiu, X., Lian, J., ... & Han, J. (2024, October). Deep reinforcement learning-based obstacle avoidance for robot movement in warehouse environments. In 2024 IEEE 6th International Conference on Civil Aviation Safety and Information Technology (ICCASIT) (pp. 342-348). IEEE.


Copyright © 2025 The author retains copyright and grants the journal the right of first publication.
This work is licensed under a Creative Commons Attribution 4.0 International License.