European International Journal of Multidisciplinary Research and Management Studies (ISSN: 2750-8587)

Received: 01 April 2026 | Accepted: 15 April 2026 | Published: 30 April 2026

RESEARCH ARTICLE

Intelligent Neural Network Framework for Distributed Digital Ledgers with Live Scam Detection and Risk Forecasting

Terekab Ngiraked

Department of Artificial Intelligence and Analytics, Pacific Institute of Digital Research, Palau

VOLUME: Vol.06 Issue 04 2026

PAGE: 135-142

Abstract

The rapid expansion of distributed digital ledger technologies, particularly blockchain-based systems, has introduced new paradigms in decentralized finance, data integrity, and autonomous transaction systems. However, the increasing sophistication of cyber fraud, financial manipulation, and real-time scam strategies has exposed critical vulnerabilities in ledger ecosystems. This research proposes an intelligent neural network framework integrated with distributed digital ledger systems to enable live scam detection and predictive risk forecasting.

The study synthesizes advancements in machine learning, risk evaluation methodologies, and intelligent decision systems to construct a hybrid analytical architecture. The framework leverages deep neural networks for anomaly detection, probabilistic risk scoring, and adaptive learning mechanisms capable of evolving with transactional behaviors. Drawing from established methodologies such as fuzzy analytic hierarchy processes (Hu Wei et al., 2005), clustering-based expert weighting systems (Lihua He et al., 2014), and multi-factor risk evaluation models (Qiang Sun et al., 2012), the proposed system integrates structured decision intelligence with real-time computational learning.

Furthermore, reliability modeling techniques inspired by complex distribution systems (Weixing Li et al.) and cooperative game-based assessment frameworks (Yan Xu & Xin Chen, 2015) are incorporated to enhance system robustness. The study also builds upon recent advancements in deep learning-based financial fraud prediction systems (Kodela et al., 2026), which demonstrate the effectiveness of neural architectures in real-time risk environments.

The proposed framework introduces a dual-layer architecture: a blockchain integrity layer ensuring secure distributed consensus, and an intelligence layer responsible for continuous monitoring, anomaly detection, and predictive analytics. Experimental simulations indicate that neural-enhanced ledger systems significantly improve fraud detection accuracy, reduce false positives, and enable proactive risk mitigation.

The findings suggest that integrating deep learning with distributed ledger infrastructures offers a transformative approach to financial cybersecurity, enabling adaptive, scalable, and self-learning risk management systems suitable for next-generation digital economies.

KEYWORDS

Neural Networks, Distributed Digital Ledger, Blockchain Security, Scam Detection, Risk Forecasting, Deep Learning, Financial Fraud Detection, Anomaly Detection, Fuzzy Logic Systems, Intelligent Risk Management.

INTRODUCTION

The emergence of distributed digital ledger technologies has significantly transformed the landscape of digital transactions, financial systems, and data management infrastructures. By enabling decentralized verification, immutability, and transparency, blockchain and related ledger systems have reduced dependency on centralized authorities while improving trust mechanisms across digital ecosystems. However, as adoption has expanded across industries such as banking, supply chain, healthcare, and smart grids, the complexity and scale of cyber threats have also increased proportionally.

One of the most pressing challenges in distributed ledger environments is the detection and prevention of fraudulent activities in real time. Traditional rule-based security systems are no longer sufficient to address evolving scam techniques that exploit system latency, transaction anonymity, and smart contract vulnerabilities. This necessitates the development of intelligent systems capable of adaptive learning and predictive analysis.

In parallel, advancements in neural network architectures and machine learning methodologies have demonstrated strong potential in addressing complex pattern recognition and anomaly detection tasks. Deep learning systems are particularly effective in extracting latent patterns from high-dimensional transactional data, making them suitable for financial risk prediction and fraud detection in distributed environments.

Research in risk assessment methodologies provides foundational insights for building intelligent detection systems. For instance, fuzzy analytic hierarchy processes have been widely used to evaluate uncertain and multi-criteria decision problems in security systems (Hu Wei et al., 2005). Similarly, clustering-based approaches for determining expert weights in decision-making systems highlight the importance of adaptive weighting mechanisms in complex environments (Lihua He et al., 2014). These approaches contribute to the theoretical foundation of intelligent risk modeling.

Furthermore, multi-factor risk evaluation frameworks developed for smart grids emphasize the importance of multidimensional risk assessment in complex systems (Qiang Sun et al., 2012). Such models provide valuable analogies for distributed ledger environments, where risk factors are heterogeneous and dynamically evolving.

The integration of intelligent computational systems into distributed infrastructures has also been explored in reliability evaluation of complex network systems (Weixing Li et al.). These studies demonstrate the importance of system resilience and fault tolerance in decentralized environments, which are essential characteristics of blockchain-based architectures.

Recent advancements in cooperative game theory and cloud-based evaluation models for system status assessment (Yan Xu & Xin Chen, 2015) further extend the applicability of hybrid analytical frameworks in distributed systems. These models provide mechanisms for collaborative decision-making and adaptive system evaluation, which are critical in decentralized ledger ecosystems.

More recently, deep learning-enhanced financial risk prediction models have shown significant promise in detecting fraudulent activities in real-time financial environments (Kodela et al., 2026). These models utilize neural architectures capable of learning evolving fraud patterns, thereby improving predictive accuracy and reducing detection latency. This research serves as a key foundation for integrating neural intelligence into distributed ledger systems.

Despite these advancements, existing systems still face several limitations. First, most blockchain security mechanisms operate reactively rather than proactively, identifying fraud only after it has occurred. Second, traditional risk assessment models lack real-time adaptability and fail to capture dynamic behavioral shifts in transaction patterns. Third, integration between distributed ledger systems and artificial intelligence models remains limited, resulting in fragmented security architectures.

To address these challenges, this research proposes an intelligent neural network framework designed specifically for distributed digital ledger environments. The primary objective is to enable real-time scam detection and predictive risk forecasting through a hybrid architecture combining blockchain integrity mechanisms with adaptive neural intelligence.

The scope of this study includes the design of a dual-layer system architecture, integration of multi-criteria decision-making models, and evaluation of deep learning-based

anomaly detection mechanisms. The significance of this research lies in its potential to enhance cybersecurity, improve financial system resilience, and support autonomous risk governance in decentralized digital ecosystems.

LITERATURE REVIEW

The evolution of intelligent risk assessment systems has been shaped by contributions across multiple domains, including power systems, financial analytics, decision science, and machine learning. The integration of these domains provides a multidisciplinary foundation for developing advanced distributed ledger security frameworks.

Early work in security risk assessment using fuzzy analytic hierarchy processes demonstrated the effectiveness of handling uncertainty in complex decision environments. Hu Wei et al. (2005) proposed a fuzzy-based hierarchical model for evaluating information security risks, emphasizing the role of subjective judgment and uncertainty modeling. This approach laid the groundwork for later developments in intelligent risk evaluation systems by introducing structured yet flexible decision frameworks.

Similarly, research on smart grid systems highlights the importance of multi-dimensional risk evaluation in large-scale distributed infrastructures. Kang Chang et al. (2009) analyzed the fundamental characteristics and technical processes of smart grid systems in China, emphasizing system complexity, decentralization, and real-time operational requirements. These characteristics closely resemble distributed ledger systems, where scalability and reliability are critical.

Further advancements in risk evaluation methodologies were introduced through multi-factorial and multi-dimensional models for smart grid risk assessment (Qiang Sun et al., 2012). This work demonstrated that risk cannot be assessed using single-dimensional metrics and must incorporate multiple interacting variables. Such insights are directly applicable to blockchain ecosystems, where transaction risk depends on network behavior, node reliability, and consensus mechanisms.

In the domain of decision science, clustering-based approaches for determining expert weights in multi-attribute group decision-making systems (Lihua He et al., 2014) introduced adaptive weighting strategies that improve decision accuracy. These methods are relevant for distributed ledger systems, where consensus and validation require dynamic weighting of node trustworthiness.

Additionally, subjective and objective weighting models for multi-objective decision-making (Dongmei Song et al., 2015) provide a hybrid approach to balancing human expertise and computational analytics. This duality is essential in designing intelligent blockchain governance systems that combine automated detection with expert oversight.

Reliability evaluation of complex radial distribution systems (Weixing Li et al.) contributes to understanding system robustness in interconnected networks. The methodologies used in this study emphasize fault tolerance, redundancy, and system stability—key principles for distributed ledger architectures.

Transformer status assessment using cooperative game theory and cloud models (Yan Xu & Xin Chen, 2015) introduces collaborative evaluation techniques that enhance system monitoring and predictive maintenance. These models are particularly relevant for distributed systems requiring collective intelligence for anomaly detection and system health evaluation.

Recent advancements in deep learning applications for financial risk prediction have significantly transformed fraud detection methodologies. Kodela et al. (2026) propose a deep learning-enhanced cloud accounting model capable of identifying real-time fraud and financial risks using adaptive neural architectures. Their findings demonstrate that neural networks outperform traditional statistical methods in identifying nonlinear fraud patterns and evolving cyber threats.

Recent advancements in Artificial Intelligence have expanded beyond predictive analytics toward intelligent digital twin ecosystems capable of supporting real-time monitoring and autonomous decision-making. Philip (2024) introduced the concept of Project Management 5.0, highlighting that AI-enabled Digital Twins facilitate continuous system synchronization, predictive analytics, adaptive resource optimization, and intelligent operational control. These capabilities complement distributed ledger security by enabling proactive monitoring of transaction networks and improving the efficiency of fraud detection and risk forecasting. The integration of Digital Twin concepts with neural intelligence therefore provides an additional foundation for developing scalable and adaptive blockchain security

frameworks.

This study directly informs the development of intelligent ledger frameworks by highlighting the importance of continuous learning, real-time analytics, and cloud-integrated intelligence systems. The integration of such models into blockchain environments enables proactive detection of suspicious transactions and adaptive risk scoring.

Despite the extensive research in individual domains, there remains a significant gap in the integration of neural networks with distributed ledger technologies for unified risk management. Existing literature primarily focuses on either blockchain security or machine learning-based fraud detection independently, rather than a cohesive hybrid system.

This research addresses this gap by proposing a unified intelligent framework that combines fuzzy logic, decision theory, and deep neural networks within a distributed ledger environment. The goal is to create a scalable, adaptive, and real-time risk detection system capable of evolving with emerging cyber threats.

METHODOLOGY

Research Design Overview

The proposed research adopts a hybrid systems engineering and computational intelligence design to develop an intelligent neural network framework integrated with distributed digital ledger infrastructure. The core objective is to enable real-time scam detection and predictive risk forecasting through continuous learning mechanisms embedded within blockchain transactions.

The system design is grounded in four integrated paradigms:

1. Distributed ledger architecture (blockchain-based immutability and consensus)
2. Deep neural network-based anomaly detection
3. Multi-criteria risk evaluation models
4. Adaptive predictive forecasting mechanisms

This hybridization ensures that transactional integrity, behavioral analysis, and predictive intelligence operate as a unified system rather than isolated modules.

The methodological foundation is influenced by risk modeling techniques such as fuzzy analytic hierarchy processes (Hu Wei et al., 2005), multi-factor decision frameworks (Qiang Sun et al., 2012), and cooperative decision systems (Yan Xu & Xin Chen, 2015). Additionally, neural predictive modeling principles are aligned with deep learning fraud detection systems (Kodela et al., 2026), which demonstrate strong applicability in real-time financial environments.

The proposed framework can also benefit from Digital Twin principles that maintain synchronized virtual representations of distributed ledger environments. As explained by Philip (2024), AI-driven Digital Twins support continuous monitoring, predictive decision support, and adaptive operational optimization. Integrating these concepts with the intelligent neural network architecture can further enhance live scam detection, system resilience, and predictive risk forecasting within decentralized financial ecosystems.

System Architecture Design

The proposed framework consists of two primary layers:

5.2.1 Distributed Ledger Layer

This layer is responsible for:

- Transaction recording
- Node validation
- Consensus maintenance
- Cryptographic security enforcement

Each transaction is represented as a structured data block containing:

- Transaction ID
- Sender/receiver metadata
- Timestamp
- Transaction value
- Behavioral signature vector
- Risk metadata (generated by AI layer)

The ledger follows a decentralized architecture where nodes validate transactions using consensus algorithms (e.g., Proof-of-Stake or hybrid consensus models). The key objective is to ensure immutability while enabling integration with external analytical systems.

The distributed nature of this layer aligns with reliability principles observed in complex systems (Weixing Li et al.), where redundancy and fault tolerance enhance system

stability.

Intelligent Neural Network Layer

This layer performs real-time analytics and includes:

- Feature extraction module
- Deep neural anomaly detector
- Risk scoring engine
- Predictive forecasting unit

The neural network operates on streaming transactional data, converting raw ledger entries into structured feature embeddings.

Feature Input Vector Includes:

- Transaction frequency patterns
- Node trust scores
- Historical fraud indicators
- Temporal transaction deviations
- Network graph relationships
- Value distribution anomalies

A hybrid neural architecture is used:

- Recurrent Neural Networks (RNNs) for sequential pattern modeling
- Convolutional Neural Networks (CNNs) for feature pattern extraction
- Attention mechanisms for identifying high-risk transaction nodes

This design ensures both temporal and structural learning capabilities.

Risk Evaluation Model

The risk evaluation module integrates classical decision science with neural inference.

Fuzzy Risk Scoring Layer

Inspired by fuzzy analytic hierarchy processes (Hu Wei et al., 2005), uncertainty in transaction evaluation is modeled using fuzzy membership functions.

Each transaction is assigned:

- Low-risk membership (μL)
- Medium-risk membership (μM)
- High-risk membership (μH)

These values are computed based on:

- Transaction anomalies
- Node credibility
- Historical behavior deviations

This allows uncertainty handling in ambiguous fraud scenarios.

Multi-Factor Weighting System

Drawing from multi-attribute decision-making models (Lihua He et al., 2014; Dongmei Song et al., 2015), the system assigns dynamic weights to risk indicators:

Risk Score (R):

$R = \Sigma (Wi \times Fi)$

Where:

- Wi = adaptive weight of feature i
- Fi = normalized risk feature

Weights are continuously updated using clustering-based behavioral segmentation, allowing dynamic adaptation to evolving fraud patterns.

Neural Fraud Detection Model

The deep learning module is the core intelligence engine.

Model Structure

The architecture consists of:

1. Input Layer (feature embeddings)
2. Temporal learning layer (LSTM-based memory unit)
3. Convolutional feature extractor
4. Attention-based risk prioritization layer
5. Output layer (risk probability score)

Training Process

The model is trained using:

- Historical transaction datasets
- Synthetic fraud injection data
- Anomaly simulation environments

Loss function:

$L = \alpha(L_{classification}) + \beta(L_{forecasting}) + \gamma(L_{anomaly})$

Where:

- Classification loss reduces fraud detection error
- Forecasting loss improves predictive accuracy
- Anomaly loss enhances outlier sensitivity

The model continuously retrains using online learning mechanisms to adapt to evolving scam behaviors.

Predictive Risk Forecasting Module

This module forecasts future fraudulent activity using:

- Time-series modeling
- Behavioral trajectory analysis
- Graph-based dependency modeling

The system constructs a transaction graph:

- Nodes = users/entities
- Edges = transactions
- Edge weights = transaction risk probability

Graph neural networks (GNNs) are used to detect:

- Fraud rings
- Coordinated attack patterns
- Suspicious node clustering

This aligns with reliability evaluation approaches in distributed systems (Weixing Li et al.) and predictive modeling strategies in neural financial systems (Kodela et al., 2026).

Real-Time Scam Detection Mechanism

The real-time detection pipeline includes:

1. Transaction ingestion
2. Feature extraction
3. Neural risk scoring
4. Threshold-based classification
5. Ledger validation decision

A transaction is classified as:

- Approved (low risk)
- Flagged (medium risk, requires review)
- Rejected (high risk fraud)

Decision thresholds are dynamically adjusted using reinforcement learning techniques.

System Optimization Strategy

Optimization is achieved through:

- Gradient-based neural optimization
- Adaptive weighting refinement
- Consensus-layer feedback loops
- Node trust recalibration

Game-theoretic principles (Yan Xu & Xin Chen, 2015) are used to balance competing node validations and prevent adversarial manipulation.

Evaluation Metrics

The system is evaluated using:

- Precision and recall (fraud detection accuracy)
- F1-score (classification balance)
- False positive rate (system efficiency)
- Detection latency (real-time capability)
- Forecast accuracy (predictive performance)

RESULTS

The experimental simulation of the proposed intelligent neural ledger framework demonstrates significant improvements in fraud detection accuracy, predictive capability, and system responsiveness compared to conventional rule-based blockchain security systems.

The neural network-based detection module achieved a high fraud identification rate, with consistent performance across varied transaction datasets. The integration of temporal learning (LSTM layers) and structural analysis (graph-based modeling) significantly enhanced the system's ability to detect both isolated fraud attempts and coordinated scam networks. In particular, the attention mechanism improved detection sensitivity toward high-risk nodes, reducing missed anomalies in complex transaction environments.

The fuzzy risk evaluation layer contributed to improved handling of uncertain and borderline transactions. By

assigning probabilistic risk memberships, the system reduced rigid classification errors commonly observed in deterministic models. This resulted in improved classification stability in ambiguous transaction scenarios.

The predictive forecasting module demonstrated strong capability in identifying emerging fraud patterns before full manifestation. Graph neural network analysis successfully detected clustered fraudulent behaviors, indicating coordinated attack structures. This early-warning capability is particularly valuable in decentralized environments where fraud propagation can occur rapidly.

When benchmarked against traditional risk assessment systems, the proposed framework showed:

- Higher detection accuracy
- Lower false positive rates
- Improved adaptability to evolving fraud patterns
- Faster real-time decision-making capability

The integration of adaptive weighting mechanisms (inspired by clustering-based decision models) improved system responsiveness to behavioral shifts in transaction networks. Additionally, reinforcement learning-based threshold tuning enhanced system flexibility under dynamic network conditions.

Overall, the results confirm that combining deep neural architectures with distributed ledger systems creates a robust hybrid framework capable of addressing both current and emerging cybersecurity threats in digital financial ecosystems.

DISCUSSION

The findings of this study highlight the transformative potential of integrating neural networks with distributed ledger technologies for intelligent fraud detection and risk forecasting. The results indicate that traditional blockchain systems, while secure in terms of data integrity, lack sufficient intelligence for proactive threat mitigation. The proposed framework addresses this limitation by embedding adaptive learning mechanisms directly into the transaction validation process.

A key theoretical implication is the convergence of distributed systems theory with deep learning-based predictive analytics. This convergence enables the transition from static security models to dynamic, self-learning cybersecurity architectures. The inclusion of fuzzy logic-based risk modeling further enhances system robustness by addressing uncertainty, which is a critical challenge in real-world financial systems.

The application of multi-factor decision-making models improves interpretability and adaptability. By incorporating clustering-based weight adjustments and subjective-objective hybrid evaluation techniques, the system aligns closely with real-world decision-making complexities. This is particularly important in decentralized environments where trust is distributed across multiple nodes.

However, several limitations must be acknowledged. First, the computational complexity of integrating neural networks with blockchain validation processes may introduce latency in large-scale deployments. Second, the reliance on high-quality training data may limit performance in environments with sparse or noisy transaction histories. Third, adversarial attacks targeting neural models remain a potential vulnerability, particularly in open distributed networks.

Despite these limitations, the system demonstrates strong practical applicability in financial fraud detection, decentralized finance platforms, and smart contract auditing systems. The predictive capabilities of the framework also suggest potential use cases in regulatory compliance and financial risk monitoring.

Comparatively, the study aligns with deep learning-enhanced financial risk prediction models (Kodela et al., 2026), which emphasize real-time fraud detection through neural architectures. However, this research extends those principles by embedding predictive intelligence directly into distributed ledger systems rather than treating it as an external analytical layer.

The discussion also reinforces the importance of hybrid modeling approaches that combine statistical decision systems, fuzzy logic, and neural networks. Such integration is essential for building resilient, adaptive, and scalable cybersecurity infrastructures in modern digital economies.

CONCLUSION

This research presented an intelligent neural network framework integrated with distributed digital ledger systems for real-time scam detection and risk forecasting. The proposed architecture successfully combines blockchain-based transactional integrity with advanced deep learning-based anomaly detection and predictive analytics.

The study demonstrates that neural-enhanced distributed ledgers significantly improve fraud detection accuracy, reduce false positives, and enable proactive risk identification. By incorporating fuzzy logic systems, multi-criteria decision models, and graph-based neural architectures, the framework achieves a high level of adaptability and robustness in dynamic financial environments.

The research contributes to the field in three major ways. First, it introduces a hybrid architectural model that integrates blockchain and neural intelligence into a unified system. Second, it enhances real-time fraud detection through adaptive learning mechanisms and behavioral modeling. Third, it provides a predictive forecasting capability that enables early detection of emerging scam patterns.

Future research can focus on optimizing computational efficiency, improving adversarial robustness, and expanding scalability for global financial networks. Additionally, integration with quantum-resistant cryptographic mechanisms and federated learning systems may further strengthen the framework's applicability in next-generation digital ecosystems.

Overall, the proposed framework represents a significant advancement in intelligent cybersecurity systems, offering a scalable and adaptive solution for securing distributed financial infrastructures.

REFERENCES

1. Kang Chang, Feng Xue, Weidong Yang. Review on the basic characteristics and its technical process of smart grid in China [J]. Automation of Electric Power Systems, 2009, 33 (17): 10–15.
2. Lihua He, Yueqi Wang, Lianying Zhang. A method of determining the experts' weights of multi-attribute group decisionmaking based on clustering analysis [J]. Operations Research and Management Science, 2014, 23 (6): 65–71.
3. Hu Wei, Li Tieke, Cui Jianshung. Information security risk assessment based on fuzzy analytic hierarchy process [J]. Network security technology and application, 2005, (6): 32–35.
4. Kodela, S., Kurada, S. B., Mogili, V. B., & Duggirala, J. (2026, March). Deep Learning-Enhanced Cloud Accounting Model for Real-Time Fraud and Financial Risk Prediction. In 2026 Innovations in Machine, Engineering, and Digital Conference (IMED) (pp. 1-6).
5. Weixing Li, Peng Wang, Zhimin Li, et al. Reliability Evaluation of Complex Radial Distribution Systems
6. Dongmei Song, Chunxiao Liu, Chen Shen, et al. Multiple objective and attribution decision making based on the subjective and objective weighting [J]. Journal of Shandong University (Engineering Science), 2015, 45 (4): 1–9.
7. Qiang Sun, Yifu Zhang, Dong Han, et al. Multifactorial and multidimensional risk evaluation of smart grid [J]. Power System Technology, 2012 36 (9): 51–55.
8. Philip, P. G. (2024). Digital Twinning, Artificial Intelligence, and Project Management 5.0: The Future of Intelligent Project Delivery . The American Journal of Interdisciplinary Innovations and Research, 6(12), 63–80. Retrieved from https://theamericanjournals.com/index.php/tajiir/article/view/digital-twinning-ai-project-management-5-0
9. Yan Xu, Xin Chen. Transformer status assessment based on cooperative game and cloud model [J]. Electric Power Automation Equipment, 2015, 35 (3): 88–93.