Literature Review: AI-Powered Fraud Detection in Blockchain Networks

1. Introduction

The integration of Artificial Intelligence (AI) with blockchain technology is revolutionizing fraud detection across decentralized networks. This review synthesizes insights from recent research on how AI models enhance the detection of illicit activities in cryptocurrency transactions and blockchain infrastructures.

---

2. AI Techniques Used

2.1 Supervised Learning

- **Algorithms**: Random Forest, Logistic Regression, Gradient Boosting, LightGBM, Decision Tree, Support Vector Machine
- **Use Cases**: Classification of blacklisted Ethereum addresses, financial fraud detection in transactions

2.2 Unsupervised & Semi-supervised Learning

- **Techniques**: K-Means Clustering, Autoencoders, GANs, Semi-supervised learning
- **Applications**: Anomaly detection, generation of synthetic training data for rare fraudulent activities

2.3 Deep Learning

- **Models**: RNNs, LSTMs, Graph Neural Networks (GNNs), Multilayer Perceptrons
- **Use Cases**: Detecting temporal fraud patterns, analyzing transaction graphs, simulating behavioral fraud scenarios

2.4 Explainable & Federated AI

- **Goals**: Ensure transparency and privacy preservation
- **Techniques**: XAI models, federated learning, off-chain AI computation

---

3. Fraud Types Detected

- Ponzi and Pyramid schemes
- Pump-and-Dump activities
- Rug Pulls in DeFi
- Phishing, Double-Spending, Sybil, and 51% attacks
- Smart contract vulnerabilities: reentrancy, overflow/underflow

---

4. Feature Engineering

4.1 On-Chain Features

- Transaction frequency, volume, hash, block attributes
- Smart contract structures and execution behavior

4.2 Off-Chain Features

- Social media sentiment, community buzz, phishing indicators

4.3 Address-Based Features

- Wallet balance, transaction history, age, unique interactions

4.4 Graph-Based Features

- Pagerank, path lengths, connected component analysis

5. System Architecture and Models

- Integration of AI with smart contracts on permissioned/public blockchains
- Use of LightGBM for scalable fraud detection
- Synthetic data generation using GANs and VAE for model training
- Federated learning and off-chain processing for privacy and latency optimization

6. Challenges

- **Data Imbalance**: Handled using SMOTE, ADASYN, undersampling
- **Concept Drift**: Requires dynamic retraining
- **Scalability**: Optimized through off-chain computation
- **Interpretability**: Addressed with Explainable AI
- **Data Diversity & Anonymity**: Limits in labeling and feature extraction

7. Performance and Results

- Models achieved accuracy > 97% in classifying fraudulent activities
- LightGBM showed high AUC-ROC and F1-scores with large datasets
- Real-time systems processed up to 1200 TPS with minimal latency

8. Future Directions

- Cross-chain fraud detection

- Broader application domains (IoT, healthcare)
- Compliance with global regulatory frameworks
- Open-source collaborative datasets and model sharing

9. Conclusion

The synergy between AI and blockchain enables robust, scalable, and adaptive fraud detection mechanisms. By leveraging advanced ML and DL models, organizations can combat evolving threats in decentralized financial systems while maintaining transparency, efficiency, and compliance.

Visualization Concepts

A. AI Model vs Fraud Type Matrix

AI Technique	Fraud Types Detected
LightGBM	Ponzi, Phishing, Rug Pulls
GNNs	Transaction Graph Anomalies
LSTM/RNN	Temporal Fraud Patterns
GANs	Synthetic Data Generation
Clustering	Sybil Attacks, Unusual Patterns
Sentiment Analysis	Pump-and-Dump via Social Media

B. Architecture Flow Diagram

1. Data Ingestion: On-chain + Off-chain sources
2. Feature Engineering: Local, global, textual, graph
3. Model Training: LightGBM, RNN, GNN, etc.
4. Real-Time Monitoring: Smart contract + AI agent
5. Alerting: Notify users, trigger regulatory checks

C. Timeline for AI-Blockchain Evolution

- 2020: Heuristic-based detection
- 2022: ML classifiers on historical data
- 2024: Real-time AI with LightGBM and RNNs
- 2025: Federated and explainable models in production

D. Challenges Radar Chart

- Data Imbalance
- Concept Drift

- Interpretability
- Privacy
- Scalability
- Regulatory Compliance