INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

ANALYZING CRYPTO FRAUD DETECTION MODELS: A REVIEW OF CURRENT APPROACHES AND LIMITATIONS

[1]Sweta Kahurke, [2]Harsha Jain, [3]Shifra Sheikh, [4]Srushti Pillare, [5]Vishakha Kandrikar

[1]Professor, [2345]Student
[12345]Department of Artificial Intelligence,
[12345]JD College of Engineering and Management, Nagpur, India

Abstract : This review paper presents a comprehensive analysis of current approaches to crypto fraud detection, examining both their methodological strengths and their inherent limitations. As blockchain technologies continue to evolve, so do the sophisticated techniques employed by malicious actors to perpetrate financial crimes. We systematically categorize and evaluate existing detection models in four primary domains: transaction graph analysis, machine learning-based approaches, hybrid detection systems, and anomaly detection frameworks. Our analysis reveals that while graph-based methods excel at identifying structural patterns in transaction networks, they often struggle with computational scalability. Machine learning approaches demonstrate promising accuracy, but face challenges with interpretability and adaptation to emerging fraud patterns. In addition, we identify critical research gaps, including inadequate standardization of evaluation metrics, limited cross-chain applicability, and insufficient attention to privacy-preserving detection techniques. The paper concludes by proposing a research roadmap that emphasizes the development of explainable AI models, real-time detection capabilities, and cross-chain compatibility frameworks. These advancements will be essential to address the evolving landscape of cryptocurrency fraud and strengthen the security infrastructure of digital asset ecosystems. Our findings provide valuable insights for researchers, regulatory bodies, and blockchain security practitioners working toward more robust fraud prevention systems.

IndexTerms **- Crypto Fraud Detection, Blockchain Security, Machine Learning, Graph Neural Networks, Anomaly Detection, Federated Learning.**

I. INTRODUCTION

Cryptocurrency markets have grown dramatically in recent years, creating new opportunities for investors, but also attracting fraudulent activities. As digital currencies like Bitcoin and Ethereum become more mainstream, detecting and preventing fraud has become a critical concern for users, exchanges, and regulators alike. Traditional financial fraud detection methods often prove inadequate in the cryptocurrency space due to the unique characteristics of blockchain technology, including pseudonymity, decentralization, and global accessibility. This research examines current approaches to crypto fraud detection, focusing on their effectiveness and limitations. By understanding the strengths and weaknesses of existing models, we aim to identify promising directions for improvement. Our work is motivated by the need to protect cryptocurrency users from financial harm while maintaining the innovative benefits that blockchain technology offers. As regulatory frameworks continue to develop around digital assets, robust fraud detection systems will play an essential role in building trust and stability in cryptocurrency markets. The increasing financial impact of cryptocurrency fraud has made it a critical area of research in both academia and industry.

II. BACKGROUND ON CRYPTOCURRENCY

2.1 Blockchain Technology and Distributed Ledgers

Blockchain technology forms the foundation of most cryptocurrencies, functioning as a distributed ledger system that records transactions across multiple computers. Unlike traditional centralized databases, blockchains store information in blocks that are cryptographically linked, creating an immutable chain of transaction records. Each block typically contains a timestamp, transaction data, and a cryptographic hash of the previous block, ensuring the integrity of the entire chain.

The distributed nature of blockchain technology means that the ledger is simultaneously maintained across a network of computers (nodes), eliminating the need for a central authority. Decentralization in blockchain networks is maintained through consensus protocols, which ensure that all participating nodes reach agreement on which transactions are valid and can be added to the ledger. The two most common consensus protocols are:

2.1.1 Proof of Work (PoW)

In Proof of Work, miners carry out computationally demanding tasks to solve cryptographic puzzles. The miner who finds the correct solution first is granted permission to validate and record the next block of transactions on the blockchain. This process demands significant computational resources and energy consumption.

2.1.2 Proof of Stake (PoS)

Validators are chosen depending on how much cryptocurrency they commit as a stake in the network. Since this method doesn't rely on energy-intensive computations, it offers a much more energy-efficient alternative to Proof of Work.

2.2 Major Cryptocurrencies and Their Technologies

2.2.1 Bitcoin (BTC)

Introduced in 2009 by the pseudonymous Satoshi Nakamoto, Bitcoin pioneered the cryptocurrency movement. Bitcoin employs a Proof-of-Work consensus model and features a maximum supply limit of 21 million units, making it a deflationary digital asset.The Bitcoin network emphasizes security and decentralization, although its transaction throughput is limited to around seven transactions per second. Bitcoin includes a simplified scripting system, intentionally restricted in functionality to minimize security risks, which supports only basic forms of smart contract execution.

2.2.2 Ethereum (ETH)

Introduced in 2015, Ethereum brought a new layer of functionality to blockchain by enabling smart contracts: programmable agreements that execute automatically based on predefined conditions.Ethereum supports a Turing-complete programming environment, enabling developers to design decentralised applications (dApps) and implement advanced logic through programmable smart contracts. Initially using PoW, Ethereum completed a transition to PoS in 2022 with "The Merge" upgrade, significantly reducing its environmental impact. Ether, the primary token on the Ethereum network, acts not only as a digital currency but also as a utility for covering computational costs, known as gas fees, during network transactions.

Other Notable Cryptocurrencies: Ripple (XRP), Cardano (ADA), Solana (SOL), Binance Coin (BNB)

2.3 The Cryptocurrency Ecosystem

2.3.1 Exchanges

Cryptocurrency exchanges serve as the primary marketplaces where users can buy, sell, and trade digital assets.These platforms fall into several categories:

- Centralized Exchanges (CEXs): Operate as traditional financial intermediaries, maintaining custody of user funds and facilitating order matching. Examples include Coinbase, Binance, and Kraken. These platforms typically offer high liquidity and user-friendly interfaces but require users to trust the exchange with their assets.
- decentralised Exchanges (DEXs): Execute trades directly between users through smart contracts without a central intermediary. Examples include Uniswap, SushiSwap, and dYdX. DEXs align more closely with cryptocurrency's decentralization philosophy but often have lower liquidity and more complex user interfaces.
- Hybrid Exchanges: Combine elements of both centralized and decentralised models, attempting to balance security, trustlessness, and user experience.

2.3.2 Wallets

Cryptocurrency wallets are software applications or hardware devices that store the private keys needed to access and manage digital assets. The main types include:

- Hot Wallets: Connected to the internet for convenient access but with higher security risks. These include web wallets, desktop applications, and mobile apps.
- Cold Wallets: Offline storage solutions that offer enhanced security by keeping private keys disconnected from the internet.
- Custodial Wallets: Third-party services that manage private keys on behalf of users, typically provided by exchanges or financial institutions.
- Non-custodial Wallets: Allow users to maintain full control of their private keys and, consequently, their assets.

III. TYPES OF CRYPTOCURRENCY FRAUD

The cryptocurrency ecosystem has given rise to numerous sophisticated fraud schemes that exploit the technical complexity, regulatory uncertainty, and pseudonymous nature of blockchain transactions. This section examines the major categories of cryptocurrency fraud and their evolving methodologies.

3.1 Traditional Fraud Schemes in the Cryptocurrency Context

3.1.1 Ponzi and Pyramid Schemes

Cryptocurrency Ponzi schemes maintain the fundamental structure of traditional Ponzi operations but leverage blockchain technology to appear more legitimate. These schemes typically promise unrealistically high returns through purported investment strategies, mining operations, or trading algorithms. In reality, they use funds from new investors to pay existing participants.

3.1.2 Pump and Dump Schemes

Pump and dump operations have found fertile ground in cryptocurrency markets, especially with low-capitalization altcoins, where price manipulation requires less capital.

- Accumulation Phase: Orchestrators quietly purchase large quantities of a cryptocurrency with low trading volume and market capitalization.
- Promotion Phase: Coordinated misinformation campaigns spread across social media platforms, messaging apps, and forums to create artificial excitement about the token.
- Dump Phase: As retail investors buy in response to the hype, driving up prices, the orchestrators sell their holdings at inflated prices.

3.1.3 Exit Scams

Exit scams occur when cryptocurrency projects or platforms suddenly disappear, taking user funds with them. These scams take several forms:

- Initial Coin Offering (ICO) Exit Scams: Project developers raise funds through token sales but abandon the project before delivering on promises, absconding with investor capital.
- Exchange Exit Scams: Cryptocurrency exchanges suddenly shut down operations and disappear with customer deposits.
- Rug Pulls: Typically occurring in decentralised finance (DeFi), developers abandon a project after creating liquidity pools with seemingly legitimate tokens, then withdraw all funds, leaving investors with worthless assets.

3.2 Cryptocurrency-Specific Fraud Mechanisms

3.2.1 Smart Contract Vulnerabilities and Exploits

Smart contract vulnerabilities represent a unique attack vector in the cryptocurrency ecosystem. These include:

- Flash Loan Attacks: Attackers borrow substantial amounts of cryptocurrency without collateral (through flash loans), manipulate market prices or exploit protocol vulnerabilities, and then repay the loan within the same transaction block, extracting profit from the price discrepancy.
- Re-entrancy Attacks: Exploiting smart contract code to withdraw funds repeatedly before the contract updates its balance. The DAO hack of 2016, which resulted in the theft of approximately \$60 million in Ether, exemplifies this vulnerability.

3.2.2 Cryptojacking

Cryptojacking refers to the illicit exploitation of someone's computing power to carry out cryptocurrency mining without their knowledge or consent. This fraud type has evolved in several directions:

- Browser-Based Cryptojacking: Malicious scripts embedded in websites use visitors' computers to mine cryptocurrencies during their visit.
- Malware Deployment: More persistent forms of cryptojacking involve malware installation that continues mining operations even after users leave the compromised website.
- Cloud Resource Theft: Attackers gain access to cloud computing accounts and deploy mining software, generating substantial costs for the account owners while directing mining rewards to the attackers.

3.2.3 Identity-Based Cryptocurrency Fraud

The pseudonymous nature of cryptocurrency transactions has enabled various identity-based fraud schemes:

- Impersonation Scams: Fraudsters create fake social media profiles mimicking cryptocurrency influencers, exchange executives, or project founders to trick followers into sending funds.
- Blockchain Address Manipulation: Malware that replaces cryptocurrency addresses in users' clipboards with addresses controlled by attackers when users attempt to make transactions.
- SIM Swapping: Attackers gain control of victims' phone numbers through social engineering of mobile carriers, then use this access to reset passwords for cryptocurrency exchange accounts and withdraw funds.

IV. CASE STUDIES OF MAJOR CRYPTO FRAUDS

While theoretical models provide the foundation for cryptocurrency fraud prevention, examining high-profile incidents offers valuable insights into practical detection challenges. This section analyzes four significant cryptocurrency fraud cases, highlighting the vulnerabilities that enabled each incident.

4.1 Mt. Gox: Transaction Malleability Exploitation

The Mt. Gox exchange collapse in 2014 involved approximately 850,000 stolen Bitcoin (valued at 450 million at the time). Attackers exploited "transaction malleability," altering transaction identifiers after submission but before confirmation. This created confusion in the exchange's accounting systems, causing multiple payments for single withdrawal requests.

The case demonstrates critical failures in transaction verification protocols, as the exchange relied exclusively on transaction IDs rather than implementing multi-signature verification or independent transaction ledgers.

4.2 Bitfinex: Multi-Signature Wallet Compromise

The 2016 Bitfinex hack resulted in the theft of approximately 120,000 Bitcoin (valued at 72 million) despite multi-signature security measures. Attackers compromised the implementation by gaining access to private keys held by BitGo, the third-party security provider, effectively circumventing the additional security layer.

This incident led to significant improvements in multi-signature implementations, including segregated authorization workflows and tiered transaction approval thresholds. Modern detection systems now incorporate risk scoring that considers transaction size, destination address reputation, and historical behavior patterns.

4.3 Ronin Network: Bridge Protocol Exploitation

The 2022 Ronin Network exploit resulted in the theft of approximately 620 million in Ethereum and USDC. Attackers compromised five of the nine validator nodes that secured the Ronin bridge, authorizing fraudulent withdrawals. The breach went undetected for six days before discovery.

This case highlights vulnerabilities in cross-chain bridge architectures and insufficient monitoring. Modern bridge protocols have subsequently implemented time-locks for large transactions, validator rotation protocols, and behavioral analysis of cross-chain transfer patterns.

4.4 FTX Collapse: Misappropriation and Governance Failures

The 2022 collapse of FTX resulted from systematic misappropriation of customer funds rather than an external attack. FTX had secretly transferred customer assets to Alameda Research, where they were used for high-risk trading activities and personal purchases.

This case demonstrates the limitations of fraud detection when faced with deliberate obfuscation by insiders. Modern exchange monitoring now increasingly tracks the ratio of on-chain reserves to customer liabilities and changes in cold wallet balances, while regulatory frameworks are evolving to require segregation of customer assets.

V. EXISTING FRAUD DETECTION TECHNIQUES

Machine learning techniques have demonstrated significant effectiveness in crypto fraud detection by identifying complex patterns not easily captured by rule-based systems. In supervised learning applications, multiple studies have evaluated classification algorithms including Random Forests, Support Vector Machines, and ensemble methods for detecting fraudulent Bitcoin transactions using features derived from transaction graphs. These approaches have achieved accuracy rates exceeding 93% in controlled studies.

Deep learning models have shown particular promise in capturing complex relationships in transaction data. Graph neural network models for anti-money laundering in cryptocurrency transactions have achieved significant improvements over traditional machine learning methods by effectively modeling transaction networks. Recurrent Neural Networks and Long Short-Term Memory networks have proven effective at capturing the temporal evolution of transaction behaviors to identify suspicious patterns.

Unsupervised learning techniques have proven valuable given the limited availability of labeled fraud data. Methods such as Local Outlier Factor algorithms have successfully identified unusual transaction patterns in the Ethereum network with high precision. Semi-supervised approaches using Generative Adversarial Networks have demonstrated effectiveness while requiring fewer labeled examples, addressing a key challenge in crypto fraud detection.

The transparent nature of blockchain data enables sophisticated network analysis techniques that reveal patterns not apparent at the individual transaction level. Graph-based analysis has emerged as a powerful approach, with disentangled prototypical autoencoders specifically targeting phishing scams in cryptocurrency transactions. Graph convolutional networks effectively capture both local and global structural information in transaction networks, improving the detection of sophisticated fraud patterns involving multiple addresses.

Behavioral analysis focuses on user activity patterns rather than individual transactions. By developing user behavior profiles based on transaction frequency and temporal patterns, these systems can identify deviations that might indicate fraudulent activity. For platforms supporting smart contracts, code analysis provides another detection vector, identifying suspicious implementation patterns and execution behaviors that may indicate Ponzi schemes or other fraudulent operations.

Hybrid detection systems that combine multiple techniques have shown improved effectiveness in real-world applications. Frameworks that integrate ensemble stacking models with transaction graph analysis achieve better performance in detecting fraudulent Bitcoin transactions than either approach alone. Real-time hybrid systems that apply lightweight rule-based filtering followed by more computationally intensive machine learning analysis for suspicious transactions balance performance and scalability requirements.

VI. CHALLENGES IN CRYPTO FRAUD DETECTION

Crypto fraud detection faces significant challenges due to the pseudonymous nature of blockchain transactions. While transactions are recorded publicly on the blockchain, the actual identities behind wallet addresses remain hidden, complicating traditional identity verification methods. This pseudonymity provides fraudsters with a veil of anonymity, making it difficult for investigators to trace funds back to their human operators. Additionally, the lack of standardized regulations across different jurisdictions creates significant gaps that fraudsters exploit. The decentralised and global nature of cryptocurrencies means

transactions can easily cross borders, putting them beyond the reach of any single regulatory authority and creating jurisdictional complications for law enforcement and regulatory bodies.

Data quality and availability present substantial obstacles for researchers and fraud detection systems. Historical transaction data can be inconsistent across different blockchains, with varying levels of detail and formatting. Many crucial off-chain contextual data points, such as user behavior patterns and identity information, are often unavailable or incomplete. Moreover, the massive volume of transaction data creates computational challenges, requiring significant resources for effective real-time processing. The imbalanced nature of fraud datasets, where legitimate transactions vastly outnumber fraudulent ones—further complicates the training of machine learning models, often resulting in biased or underperforming systems. These data challenges are compounded by privacy concerns that limit what information can be collected and shared among detection systems.

The dynamic nature of cryptocurrency fraud presents perhaps the most persistent challenge to detection efforts. Fraudsters continuously adapt their techniques to evade detection, developing sophisticated methods that can quickly render existing detection models obsolete. The emergence of new cryptocurrencies, tokens, and blockchain platforms creates an ever-expanding attack surface that detection systems must monitor. Cross-chain transactions and the use of privacy coins further complicate tracking efforts, as funds can be moved across different blockchains or through channels specifically designed to enhance anonymity. This rapidly evolving landscape necessitates adaptive detection methods that can learn and evolve alongside fraudulent techniques. Current research highlights the need for more flexible models that can respond to previously unseen fraud patterns while maintaining accuracy and minimizing false positives, which remain a significant concern in operational environments.

VII. EMERGING TRENDS AND FUTURE DIRECTION

The dynamic nature of cryptocurrency transactions, combined with increasing decentralization, presents unique challenges in fraud detection. As fraudsters adopt more complex and stealthy tactics, emerging trends in artificial intelligence and blockchain analytics are paving the way for smarter, more adaptive detection systems. This section highlights some of the most promising trends that are expected to shape the future of crypto fraud detection.

7.1 Federated Learning for Privacy-Preserving Detection

One of the most significant challenges in building effective fraud detection models is accessing large volumes of labeled data without compromising user privacy. Federated Learning (FL) offers a solution by enabling decentralised model training across multiple data sources, such as exchanges or wallets without sharing raw data. This allows organizations to collaboratively improve detection accuracy while preserving data confidentiality. Recent research emphasizes its potential for scalable and secure fraud detection, though challenges such as communication overhead and model synchronization remain areas for further study.

7.2 Real-Time Transaction Monitoring

Traditional fraud detection systems often rely on post-analysis, which may delay response and allow fraudulent activities to go unnoticed until damage is done. The future of fraud detection lies in real-time analysis, powered by stream-processing frameworks and lightweight ML models. Such proactive systems are crucial for preventing high-speed fraud patterns in both centralized exchanges and decentralised platforms.

7.3 Explainable AI (XAI) for Trust and Transparency

With regulatory scrutiny increasing around automated decision-making in financial services, the adoption of Explainable AI is gaining momentum. Explainable models help investigators and compliance teams understand why a transaction was flagged, making decisions more transparent and auditable. Tools like SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) are being integrated into fraud detection pipelines to enhance interpretability without sacrificing accuracy.

7.4 Cross-Chain Fraud Analysis

Fraudsters often exploit the siloed nature of blockchain ecosystems by moving assets across different chains to obscure transaction trails. Emerging research focuses on cross-chain fraud detection that correlates activities across multiple blockchain networks. By developing interoperable analytics tools and standardized data models, it becomes possible to track suspicious behavior even when assets move between chains through bridges or decentralised exchanges.

7.5 Smart Contract Security and DeFi Fraud Detection

The rise of decentralised finance (DeFi) has introduced new vectors for fraud, including rug pulls, flash loan attacks, and contract manipulation. Future detection efforts are increasingly focusing on smart contract auditing using techniques such as symbolic execution, formal verification, and runtime monitoring. These tools help identify vulnerabilities before contracts are deployed and can monitor suspicious behaviors during execution, especially in liquidity pools and staking contracts.

VIII. CONCLUSIONS

Cryptocurrency has revolutionized digital finance by introducing decentralised, borderless, and permissionless transactions. However, these features, while innovative, also create fertile ground for various types of fraud, including phishing, Ponzi schemes, wash trading, and money laundering. As the global adoption of cryptocurrencies continues to surge, the need for robust, accurate, and adaptable fraud detection systems becomes increasingly critical.

This paper presented a comprehensive review of the current models used in crypto fraud detection. We began by discussing the significance of fraud detection in the crypto landscape and highlighted how the decentralised and pseudonymous nature of blockchain platforms makes traditional detection methods less effective. We then categorized the types of fraud commonly observed in the cryptocurrency ecosystem and analyzed how they exploit both technological vulnerabilities and social engineering tactics.

To bridge these gaps, we explored several emerging trends shaping the future of fraud detection. Among them, federated learning stood out as a promising direction for privacy-preserving collaborative model training, especially across exchanges and financial institutions. The adoption of explainable AI (XAI) is another major development, helping increase the transparency and trustworthiness of automated fraud decisions. In addition, real-time fraud detection systems leveraging streaming data and adaptive learning algorithms are being actively researched to counter time-sensitive scams. Furthermore, cross-chain analytics and smart contract auditing are emerging as crucial tools to detect and prevent frauds that span multiple blockchains or exploit decentralised finance (DeFi) protocols.

Ultimately, this review underscores that while significant progress has been made in developing advanced fraud detection systems for cryptocurrencies, the field remains dynamic and requires constant innovation. Future efforts must focus on building scalable, interpretable, and interoperable solutions that can operate in decentralised environments, comply with emerging regulations, and adapt to the ever-changing nature of fraudulent behavior.

IX. Acknowledgment

The authors would like to express their sincere gratitude to the Department of Artificial Intelligence, JD College of Engineering and Management, Nagpur, for their guidance and support throughout this research. We also thank our professor for valuable insights and encouragement during the completion of this paper.

References

[1] A. A. Ahmed and O. O. Alabi, "Secure and Scalable Blockchain-Based Federated Learning for crypto fraud detection: A Systematic Review," in IEEE Access, vol. 12, pp. 102219-102241, 2024, doi: 10.1109/ACCESS.2024.3429205.

[2] J. Kang and S. -J. Buu, "Graph Anomaly Detection With Disentangled Prototypical Autoencoder for Phishing Scam Detection in Cryptocurrency Transactions," in IEEE Access, vol. 12, pp. 91075-91088, 2024, doi: 10.1109/ACCESS.2024.3419152.

[3] J. Nicholls, A. Kuppa and N. -A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," in IEEE Access, vol. 9, pp. 163965-163986, 2021, doi: 10.1109/ACCESS.2021.3134076.

[4] Y. K. Sanjalawe and S. R. Al-E'mari, "Abnormal Transactions Detection in the Ethereum Network Using Semi-Supervised Generative Adversarial Networks," in IEEE Access, vol. 11, pp. 98516-98531, 2023, doi: 10.1109/ACCESS.2023.3313630.

[5] L. Ju, T. Zhang, S. Toor and A. Hellander, "Accelerating Fair Federated Learning: Adaptive Federated Adam," in IEEE Transactions on Machine Learning in Communications and Networking, vol. 2, pp. 1017-1032, 2024, doi: 10.1109/TMLCN.2024.3423648.

[6] A. Ehsan et al., "Enhanced Anomaly Detection in Ethereum: Unveiling and Classifying Threats With Machine Learning," in IEEE Access, vol. 12, pp. 176440-176456, 2024, doi: 10.1109/ACCESS.2024.3504300.

[7] A. H. H. Kabla et al., "Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review," in IEEE Access, vol. 10, pp. 71632-71655, 2022, doi: 10.1109/ACCESS.2022.3188637.

[8] D. Mistry, M. F. Mridha, M. Safran, S. Alfarhood, A. K. Saha and D. Che, "Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning," in IEEE Access, vol. 11, pp. 79315-79329, 2023, doi: 10.1109/ACCESS.2023.3299331.

[9] E. Badawi and G. -V. Jourdan, "Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review," in IEEE Access, vol. 8, pp. 200021-200037, 2020, doi: 10.1109/ACCESS.2020.3034816.

[10] N. Nayyer, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh and M. Jamil, "A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities," in IEEE Access, vol. 11, pp. 90916-90938, 2023, doi: 10.1109/ACCESS.2023.3308298.

[11] Q. Umer, J. -W. Li, M. R. Ashraf, R. N. Bashir and H. Ghous, "Ensemble Deep Learning-Based Prediction of Fraudulent Cryptocurrency Transactions," in IEEE Access, vol. 11, pp. 95213-95224, 2023, doi: 10.1109/ACCESS.2023.3310576.

[12] S. Ferretti, G. D'Angelo and V. Ghini, "Enhancing Anti-Money Laundering Frameworks: An Application of Graph Neural Networks in Cryptocurrency Transaction Classification," in IEEE Access, vol. 13, pp. 50201-50215, 2025, doi: 10.1109/ACCESS.2025.3552240.

[13] T. Awosika, R. M. Shukla and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," in IEEE Access, vol. 12, pp. 64551-64560, 2024, doi: 10.1109/ACCESS.2024.3394528.

[14] M. M. Islam and H. P. IN, "A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2372-2386, 1 July-Aug. 2023, doi: 10.1109/TSC.2022.3226120.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.