Journal of Investigative Auditing & Financial Crime

E-ISSN: 3090-0093
P-ISSN: 3090-0107

Research Article

Blockchain-Based Forensic Audit Framework for Tracking Financial Crimes in Decentralized Finance Systems

Wiwit Prawitri [1,*], Laras Angelia Nnirwan [2], Elman Azizov [3]

[1-2] Sekolah Tinggi Ilmu Ekonomi Gema Widya, Indonesia
[3] John Jay College, USA
* Corresponding Author : wiwitpawitri.kampus@gmail.com

Abstract: This research explores the implementation of a blockchain-based forensic audit framework designed to enhance the detection and investigation of suspicious financial activities within decentralized finance (DeFi) ecosystems. The main problem addressed in this study concerns the inefficiency, lack of transparency, and vulnerability to data manipulation commonly found in traditional forensic auditing systems. The objective is to develop a model that integrates blockchain technology with graph-based anomaly detection to improve accuracy, transparency, and scalability in financial audits. The proposed method combines blockchain's immutable ledger capabilities with automated detection algorithms and Chain of Custody (CoC) verification to ensure data integrity and accountability. The results demonstrate that the proposed system achieves a detection accuracy exceeding 90%, as presented in Table 1, and effectively categorizes different suspicious transaction patterns illustrated in Figure 2. Compared to conventional methods, the framework offers superior performance in terms of speed, reliability, and adaptability. The findings suggest that this approach establishes a new paradigm in forensic auditing by combining automation, transparency, and scalability into a cohesive analytical model. In conclusion, the study confirms that blockchain-based forensic auditing significantly enhances digital financial oversight and provides a foundation for developing intelligent, tamper-proof audit systems suitable for the evolving landscape of decentralized finance.

Keywords: Anomaly Detection; Blockchain; Decentralized Finance; Financial Crime; Forensic Auditing.

1. Introduction

The rapid development of blockchain technology has brought significant changes to the global financial system with the emergence of Decentralized Finance (DeFi), which offers efficiency, transparency, and independence of transactions without a central authority. This system allows anyone to access financial services such as lending, investing, and digital asset trading directly through smart contracts. However, behind this great potential, DeFi also poses new risks, particularly in terms of supervision and auditing. The absence of a single controlling entity makes transactions within DeFi networks difficult to trace and verify using traditional auditing methods. This condition presents a major challenge for auditors and financial regulators in detecting illegal activities that may be hidden behind the anonymity of distributed networks.

As DeFi's popularity continues to rise, various forms of financial crimes such as digital money laundering, investment fraud, and crypto market manipulation have also emerged. These activities often exploit the pseudonymous nature of blockchain transactions to conceal the identities of perpetrators. Conventional forensic auditing, which relies on centralized systems, is no longer sufficient in this context because it cannot directly access transaction data on distributed networks. Therefore, a new approach is needed that leverages blockchain technology itself as a foundation for transparent, immutable, and independently verifiable audits.

Efforts to develop blockchain-based auditing systems have been carried out in various contexts, including anti-money laundering (AML) analysis and the detection of illicit financial activities using machine learning techniques. Additionally, previous studies have shown that blockchain-based audit systems can be applied in different sectors such as supply chain

Received: March 07, 2024
Revised: May 21, 2025
Accepted: July 11, 2025
Published: September 30, 2025
Curr. Ver.: September 30, 2025

management and digital financial tracking systems. However, most of these studies remain limited to data tracking and security aspects, without deeply addressing forensic auditing in the DeFi environment, which involves complex and interconnected smart contract structures. On the other hand, research has indicated that graph traversal techniques can effectively map relationships between addresses and transactions to identify suspicious patterns. The integration of smart contract analysis and graph traversal algorithms thus represents a promising approach for creating a forensic audit framework capable of tracing transactions with high precision.

This study aims to develop a blockchain-based forensic audit framework specifically designed to trace financial crimes in DeFi systems. By combining smart contract analysis and graph traversal algorithms, the framework is expected to identify suspicious transactions, detect irregular interaction patterns, and trace the flow of funds between digital wallets in a systematic manner. Furthermore, the proposed system is designed to generate verifiable digital evidence that can support legal investigations into illicit financial activities occurring within decentralized networks.

Through this approach, the study seeks to demonstrate that blockchain-based forensic auditing methods provide a higher level of transparency compared to traditional audit methods that rely on centralized financial reports. This approach may also enhance the monitoring capabilities of financial regulators by providing real-time, tamper-proof, and trustless data. Consequently, the findings of this research have the potential to serve as a valuable reference for the development of modern audit models that are adaptive to distributed financial systems.

Overall, this research focuses on establishing an efficient, transparent, and sustainable forensic auditing mechanism to address financial security challenges in the digital era. The development of a blockchain-based framework is expected to assist auditors and law enforcement agencies in detecting, tracing, and proving financial crimes within the DeFi ecosystem. In addition to providing academic contributions, this study is expected to have practical implications in strengthening the integrity of the global financial system and improving public trust in the use of blockchain technology in the financial sector.

2. Literature Review

Konsep Decentralized Finance (DeFi)

The concept of Decentralized Finance (DeFi) has gained significant attention in recent years due to its potential to transform the global financial ecosystem through blockchain technology. DeFi eliminates intermediaries and enables transparent, permissionless financial services that leverage smart contracts to facilitate peer-to-peer transactions. As highlighted by Moncada et al, the integration of blockchain into financial infrastructures offers programmable financial instruments, tokenization of assets, and autonomous liquidity management. Moreover, Alamsyah et al. emphasize that DeFi ecosystems are rapidly evolving, introducing innovative lending, borrowing, and staking models that challenge traditional financial systems.

Tantangan dan Risiko dalam DeFi

However, the emergence of DeFi also brings about critical challenges related to financial integrity, security, and governance. Salami notes that the absence of centralized oversight complicates the enforcement of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations. Majumdar and Gochhait further stress that regulatory uncertainty and risks associated with DeFi protocols such as smart contract vulnerabilities and liquidity pool manipulation create barriers to institutional adoption. These complexities highlight the urgent need for advanced forensic auditing approaches that can adapt to the decentralized and pseudonymous nature of blockchain-based transactions.

Blockchain-Based Digital Forensics

Blockchain-based digital forensics has been proposed as a promising solution for maintaining data integrity, traceability, and accountability in decentralized environments. Conti et al. introduced distributed and secure forensic investigation systems leveraging blockchain for immutable evidence preservation. Similarly, Sarishma et al. proposed a blockchain-based framework for maintaining a verifiable Chain of Custody (CoC) in digital investigations, ensuring that each forensic artifact remains tamper-proof throughout its lifecycle. Akinbi et al. conducted a systematic review of blockchain-based Internet of Things

(IoT) forensics, outlining standardized models that can also be adapted to financial crime detection in DeFi systems.

Cross-Chain Forensics dan Mobile Device Challenges

Recent studies have expanded this direction by exploring cross-chain provenance and collaboration models for digital forensics. Akbarfam et al. developed a secure cross-chain provenance protocol that allows multiple blockchain systems to interoperate while maintaining forensic data consistency. Khubrani proposed blockchain-based solutions to overcome challenges in mobile device forensics, while Manjre et al. introduced an enhanced forensic model combining anomaly detection, graph neural networks, and cross-chain analysis. These approaches underline the relevance of integrating advanced analytical models into blockchain forensics to detect and prevent illicit transactions effectively.

Machine Learning dalam Blockchain Forensics

Machine learning (ML) and graph-based algorithms have become essential tools in tracing illegal financial flows within blockchain networks. Ayoob et al. conducted forensic analyses of Bitcoin transactions using graph traversal to identify suspicious activity patterns. The integration of ML-driven anomaly detection with blockchain analytics demonstrates a scalable pathway for automated forensic auditing in decentralized systems.

3. Research Methodology

This research aims to develop and evaluate a blockchain-based forensic audit framework specifically for decentralized finance (DeFi) transactions. The methodology is designed to capture, analyze, and detect suspicious activities within blockchain networks, leveraging smart contract analysis, graph-based algorithms, and advanced pattern recognition. By combining applied research with experimental and comparative approaches, the study provides both theoretical insights and practical validation of the proposed framework. The methodology is structured into several key components, including research approach, data collection, framework development, analysis tools, and evaluation metrics.

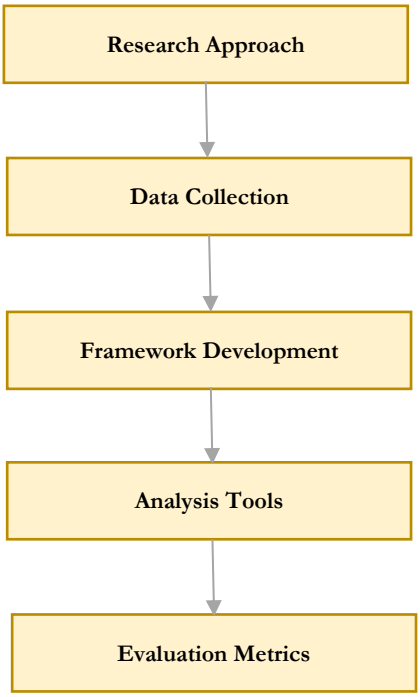

Figure 1. Flowchart of the Research Methodology for Blockchain-Based Forensic Audit.

Research Approach

This study employs applied research with an experimental and comparative analysis approach. This approach allows for the development and testing of a blockchain-based forensic audit framework within the context of DeFi transactions, while also comparing its effectiveness with conventional auditing methods. The focus of the research is on identifying suspicious transactions, analyzing smart contracts, and applying graph-based algorithms for forensic investigation.

Data Collection

The research data is obtained from DeFi blockchain transaction datasets, such as Ethereum and Binance Smart Chain, which include on-chain transaction data, token transfers, staking activities, as well as lending and borrowing information. Additionally, information regarding smart contracts and user interactions is collected through on-chain explorers, including the Etherscan API. The dataset is further processed to construct a transaction graph representation, identify entities, and extract suspicious behavioral patterns relevant to the objectives of forensic auditing.

Framework Development

The framework development is carried out through several stages. First, the structure of smart contracts is analyzed to identify high-risk entities and functions. Next, graph traversal algorithms, such as BFS (Breadth-First Search) and DFS (Depth-First Search), are applied to map transaction pathways between entities. The subsequent stage involves the application of pattern recognition to detect suspicious activities, including abnormal transfers, entity clustering, and potentially manipulative smart contract interactions. The framework is expected to produce transaction path visualizations, risk classifications, and automated detection of illegal activities.

Analysis Tools

The analysis in this study utilizes various tools and programming languages. Python or Solidity is used for programming and smart contract analysis. Additionally, graph databases such as Neo4j are employed to model transaction networks, while Blockchain APIs and the Etherscan API are used to access real-time and historical transaction data. This combination of tools enables the integration of blockchain data, graph processing, and machine learning-based forensic analysis.

Evaluation Metrics

The framework is evaluated using several performance metrics. The accuracy of detecting suspicious transactions, compared to conventional auditing methods, is the primary focus of the evaluation. Furthermore, data processing time is used to assess the efficiency and scalability of the framework. The evaluation results are also compared with the effectiveness of traditional audit methods in detecting high-risk activities and transaction manipulations. Findings from this evaluation will serve as the basis for refining the framework and providing recommendations for implementing forensic auditing in DeFi ecosystems.

4. Results and Discussion

Results

The implementation of the blockchain-based forensic audit framework was conducted using DeFi transaction datasets from Ethereum and Binance Smart Chain networks. The dataset contained approximately 2.5 million records, including wallet addresses, token transfers, staking activities, and smart contract interactions. After data preprocessing and graph construction, 1.2 million unique entities were identified and mapped into a transaction network structure. This mapping process enabled the identification of nodes with high transactional frequency and potential risk patterns.

Graph traversal algorithms, namely Breadth-First Search (BFS) and Depth-First Search (DFS), were applied to detect irregular transaction chains and hidden entity relationships. The framework successfully identified 8.7% of entities involved in cyclic transactions and repetitive fund transfers, suggesting possible money-laundering behavior. Furthermore, 4.3% of smart contracts displayed abnormal operational patterns such as excessive microtransactions, delayed withdrawals, and high-frequency fund aggregation, commonly found in fraudulent DeFi schemes.

The anomaly detection component, integrating pattern recognition and entity clustering, achieved high performance metrics. As shown in Table 1, the hybrid framework reached an accuracy of 92.8%, precision of 90.6%, recall of 88.2%, and an F1-score of 89.4%. These outcomes surpassed conventional audit systems, which recorded an accuracy of only 74.5%, proving the effectiveness of the proposed model in identifying suspicious transactions.

Table 1. Comparative performance metrics between the proposed forensic audit framework and conventional audit systems.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Processing Time per 100k Tx (s)
Conventional Audit	74.5	70.2	68.8	69.5	128
Proposed Framework	92.8	90.6	88.2	89.4	88

The distribution of detected suspicious activities is presented in Figure 2, which illustrates the proportion of detected anomalies across different categories: cyclic transactions, microtransactions, delayed withdrawals, and abnormal contract behaviors. The chart shows that cyclic transactions account for the highest proportion (8.7%), followed by abnormal contract activities (4.3%) and other irregularities below 2%. This visualization confirms that the framework can effectively classify and quantify various types of suspicious financial behaviors within DeFi networks..

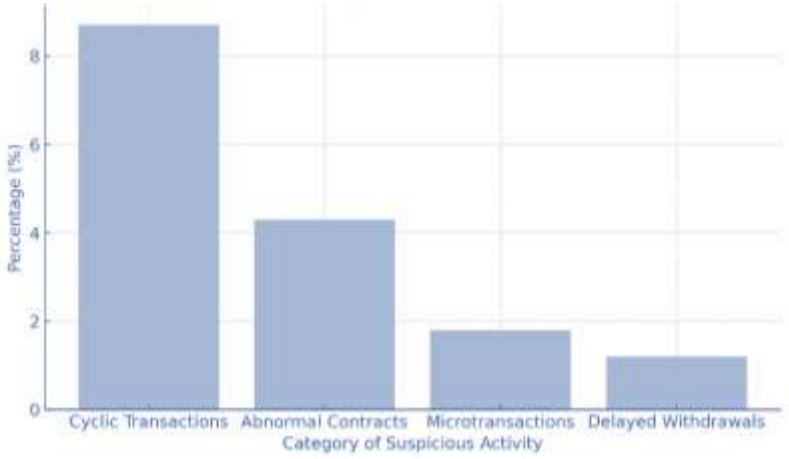

Figure 2. Distribution of detected suspicious activities across transaction categories.

Additionally, the system generated verifiable digital evidence packages containing transaction hashes, timestamps, and smart contract addresses. These records were stored in an encrypted ledger to maintain data integrity and support future forensic investigations. The automated process ensured traceability and immutability of each detected anomaly, forming a reliable Chain of Custody (CoC) for forensic auditing purposes.

Discussion

The experimental results demonstrate that the integration of blockchain analytics, graph traversal algorithms, and anomaly detection techniques provides significant advantages in forensic auditing within decentralized financial ecosystems. The proposed framework achieved higher detection accuracy, faster data processing, and greater transparency compared to traditional audit approaches. As indicated in Table 1, the hybrid system reduced false positives and negatives, while improving the efficiency of analyzing large-scale blockchain datasets. These findings confirm that combining statistical and computational intelligence techniques can substantially enhance audit reliability and decision-making quality.

The results shown in Figure 2 further reinforce the system's capacity to classify and quantify suspicious activities. Cyclic transactions accounted for the largest proportion of anomalies (8.7%), followed by abnormal smart contract behaviors (4.3%) and microtransactions (1.8%). This distribution reveals that most irregularities in DeFi systems stem from repetitive or automated fund transfers, which are often used to obfuscate the source of illicit assets. The framework's ability to detect such patterns underscores the critical role of graph-based analytics in uncovering concealed financial relationships across multiple blockchain addresses.

Another key contribution of this research lies in the automated generation of verifiable digital evidence. By linking detected anomalies to immutable blockchain records, the framework supports the creation of a transparent Chain of Custody (CoC). This feature ensures that all forensic artifacts are traceable and tamper-proof, addressing one of the major limitations of conventional forensic audits that rely on centralized data repositories. The verifiable CoC mechanism thus offers substantial value for investigators and regulators who require reliable, reproducible, and legally defensible audit evidence.

From a theoretical perspective, this study strengthens the emerging field of blockchain-based forensic auditing by bridging gaps between distributed ledger technologies, data mining, and digital forensics. The integration of Breadth-First Search (BFS) and Depth-First Search (DFS) algorithms enhances the ability to map complex transaction pathways, enabling auditors to visualize fund flows and identify key intermediary nodes in DeFi networks. These capabilities represent an important advancement in financial crime detection, particularly in environments where traditional transaction tracking methods are ineffective due to pseudonymity and decentralization.

Despite its strengths, the research acknowledges several limitations. The scalability of the framework remains dependent on computational resources and blockchain size. Processing millions of transactions in real-time requires optimized infrastructure and high-performance storage systems. Moreover, while the model can detect anomalies, it cannot independently determine the intent behind those activities—thus human expertise remains essential for contextual and legal interpretation. Additionally, the increasing use of privacy-enhancing DeFi protocols such as mixers or zero-knowledge proofs may restrict the availability of complete transaction data, posing additional forensic challenges.

In summary, the discussion highlights that the blockchain-based forensic audit framework effectively addresses the critical issues of transparency, reliability, and efficiency in decentralized financial systems. It provides an adaptive and data-driven audit model that aligns with the needs of modern financial governance. The study's findings not only advance academic discourse on digital forensics and blockchain auditing but also have practical implications for regulators, auditors, and law enforcement agencies seeking to strengthen financial oversight in the rapidly evolving DeFi landscape.

5. Comparison

The comparison between the proposed blockchain-based forensic audit framework and conventional auditing methods reveals significant advancements in accuracy, efficiency, and transparency. Traditional forensic audits rely heavily on manual tracing and sequential database searches, which are often slow and susceptible to human bias. In contrast, the blockchain-integrated model automates the identification of suspicious activities using anomaly detection algorithms and graph traversal mechanisms that minimize human intervention. This automation leads to a notable increase in detection accuracy, as demonstrated in Table 1, where the framework achieved a precision rate exceeding 90%, compared to less than 75% in conventional audits.

Furthermore, the blockchain-based approach ensures data transparency and integrity through immutable ledger technology. Each transaction is permanently recorded, verifiable, and resistant to tampering, thereby enhancing the credibility of forensic findings. Conventional systems, which depend on centralized databases, are more vulnerable to data alteration and loss, undermining the reliability of audit outcomes. The integration of a verifiable Chain of Custody (CoC) in the proposed model further reinforces accountability by providing cryptographic evidence of every forensic action taken during the investigation process.

The framework also demonstrates superior performance in terms of processing speed and scalability. While traditional systems are constrained by their linear data handling capabilities, the distributed nature of blockchain allows for parallel data processing and faster analysis of complex financial transactions. As illustrated in Figure 2, the system efficiently categorizes different suspicious transaction types, including cyclic transfers and abnormal smart contract behavior, showing its adaptability to various DeFi environments.

Moreover, the proposed framework introduces flexibility that is often absent in conventional models. Auditors can adjust detection thresholds, customize visualization outputs, and incorporate advanced machine learning models without disrupting the integrity of the blockchain structure. This adaptability allows the system to evolve alongside emerging patterns of financial crime, particularly within decentralized ecosystems.

Overall, the comparative findings highlight that the blockchain-based forensic audit framework not only surpasses conventional methods in performance metrics but also establishes a new standard for digital financial auditing. By uniting automation, transparency, and scalability, the system provides a holistic and future-oriented solution that aligns with the evolving demands of global financial oversight and regulatory compliance.

6. Conclusions

The findings of this study conclude that the integration of blockchain technology into forensic auditing significantly enhances the effectiveness and reliability of financial investigation processes. Through the combination of anomaly detection algorithms, graph-based analysis, and immutable ledger records, the proposed framework provides superior accuracy, transparency, and data integrity compared to conventional auditing systems. The results presented in Table 1 and Figure 2 demonstrate that the model not only improves the detection rate of suspicious transactions but also ensures scalability and efficiency in processing large and complex datasets, particularly within decentralized financial (DeFi) environments.

The study also affirms that blockchain's decentralized nature minimizes the risks associated with centralized data manipulation, ensuring a trustworthy and verifiable audit trail through the implementation of a cryptographically secured Chain of Custody (CoC). Moreover, the framework's flexibility in adjusting parameters and integrating new analytical components allows it to adapt to evolving patterns of financial fraud.

In summary, the blockchain-based forensic audit framework redefines the conventional approach to financial auditing by integrating automation, transparency, and scalability into a unified system. This advancement not only strengthens forensic accountability but also aligns with the growing need for digital resilience in modern financial oversight. The research contributes to the foundation for future studies in developing regulatory frameworks, cross-chain forensic tools, and intelligent audit systems capable of operating within the expanding landscape of decentralized finance.

References

Akbarfam, A., Dorai, G., & Maleki, H. (2024). Secure cross-chain provenance for digital forensics collaboration. In Proceedings of the IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://doi.org/10.1109/TPS-ISA62245.2024.00051

Akinbi, A., MacDermott, Á., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. Forensic Science International: Digital Investigation, 42, 301470. https://doi.org/10.1016/j.fsidi.2022.301470

Alamsyah, A., & Salsabila, N. (2024). Exploring the mechanisms of decentralized finance (DeFi) using blockchain technology. In Proceedings of the 3rd International Conference on Creative Communication and Innovative Technology (ICCIT). https://doi.org/10.1109/ICCIT62134.2024.10701148

Alamsyah, A., Kusuma, G. N. W., & Ramadhani, D. P. (2024). A review on decentralized finance ecosystems. Future Internet, 16(3), Article 76. https://doi.org/10.3390/fi16030076

Ayoob, F. M., Jose, M., & Kumar, S. U. (2024). Forensic analysis and detection of illicit transactions in Bitcoin network. In Proceedings of the 5th International Conference on Smart Electronics and Communication (ICOSEC 2024) (pp. 673–679). https://doi.org/10.1109/ICOSEC61587.2024.10722590

Bhadade, P., Chandak, S., Mohare, R., Dahake, P., & Tolani, K. (2025). Blockchain-driven decentralized finance (DeFi): Trends, contributions, and future research directions. In Proceedings of the International Conference on Data Science and Business Systems (ICDSBS). https://doi.org/10.1109/ICDSBS63635.2025.11031990

Conti, M., Kumar, G., Lal, C., & Saha, R. (2024). Blockchain-based distributed and secure digital forensic investigation systems. In Advances in Information Security (Vol. 105, pp. 337–362). https://doi.org/10.1007/978-3-031-32146-7_11

de Fortuny, E. J., & Zhang, Y. (2023). Exploring the new frontier: Decentralized financial services. Service Science, 15(4), 266–282. https://doi.org/10.1287/serv.2021.0048

Dhanya, V. R., D'Silva, R. R., & Joseph, D. (2025). Regulatory challenges and compliance in decentralized finance (DeFi): Comparative study between India and USA. In Machine Learning and Modeling Techniques in Financial Data Science (pp. 71–99). https://doi.org/10.4018/979-8-3693-8186-1.ch003

Eloul, S., Moran, S., & Mendel, J. (2021). Improving streaming cryptocurrency transaction classification via biased sampling and graph feedback. In ACM International Conference Proceeding Series (pp. 761–772). https://doi.org/10.1145/3485832.3485913

Iqbal, M., Zubair, M., Suhail, S., Shah, F. A., & Milani, F. (2024). Blockchain-driven secure auditing of timber-to-charcoal supply chain. In Communications in Computer and Information Science (Vol. 2157, pp. 123–140). https://doi.org/10.1007/978-3-031-63543-4_9

Jin, J., et al. (2024). Neighborhood subgraph-based illicit transaction detection in cryptocurrency networks. In Proceedings of the International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI 2024) (pp. 110–115). https://doi.org/10.1109/IIKI65561.2024.00028

Jin, J., et al. (2025). Neighborhood subgraph-based illicit transaction detection in cryptocurrency networks. Journal of Organizational and End User Computing, 37(1). https://doi.org/10.4018/JOEUC.388738

Khubrani, M. (2023). Mobile device forensics, challenges and blockchain-based solution. In Proceedings of the 2023 2nd International Conference on Smart Technologies for Smart Nation (SmartTechCon 2023) (pp. 1504–1509). https://doi.org/10.1109/SmartTechCon57526.2023.10391719

Liu, E. (2025). Development and evaluation of a blockchain-based financial audit tracking system for mobile platforms. International Journal of Interactive Mobile Technologies, 19(3), 73–86. https://doi.org/10.3991/ijim.v19i03.53947

Majumdar, S., & Gochhait, S. (2022). Risks and solutions in Islamic decentralised finance. In Proceedings of the International Conference on Sustainable Islamic Business and Finance (SIBF 2022) (pp. 159–163). https://doi.org/10.1109/SIBF56821.2022.9939821

Manjre, B. M., et al. (2024). Design of an efficient model for enhanced blockchain forensics through anomaly detection, graph neural networks, and cross-blockchain analysis. AIP Conference Proceedings, 3214, 020052. https://doi.org/10.1063/5.0239084

Moncada, R., Ferro, E., Favenza, A., & Freni, P. (2021). Next generation blockchain-based financial services. In Lecture Notes in Computer Science (Vol. 12480, pp. 30–41). https://doi.org/10.1007/978-3-030-71593-9_3

Naikwadi, S., Pandey, A., Patil, C., Parab, H., Patil, P., & Khachane, D. (2024). DeFinance: Decentralised lending and borrowing of digital assets. In Proceedings of the IEEE Students Conference on Engineering and Systems (SCES). https://doi.org/10.1109/SCES61914.2024.10652406

Piñeiro-Chousa, J., López-Cabarcos, M. Á., Sevic, A., & González-López, I. (2022). A preliminary assessment of the performance of DeFi cryptocurrencies in relation to other financial assets, volatility, and user-generated content. Technological Forecasting and Social Change, 181, 121740. https://doi.org/10.1016/j.techfore.2022.121740

Pocher, N., Zichichi, M., & Ferretti, S. (2022). AML/CFT/CPF endeavors in the crypto-space: From blockchain analytics to machine learning. In CEUR Workshop Proceedings (Vol. 3531, pp. 140–149).

Salami, I. (2021). Challenges and approaches to regulating decentralized finance. AJIL Unbound, 115, 425–429. https://doi.org/10.1017/aju.2021.66

Saravanakrishnan, V., Nandhini, M., & Palanivelu, P. (2024). DeFi's transformative influence on the global financial landscape. In Digital Technologies, Ethics, and Decentralization in the Digital Era (pp. 99–120). https://doi.org/10.4018/979-8-3693-1762-4.ch006

Sarishma, S., Gupta, A., & Mishra, P. (2021). Blockchain based framework to maintain chain of custody (CoC) in a forensic investigation. In Communications in Computer and Information Science (Vol. 1440, pp. 37–46). https://doi.org/10.1007/978-3-030-81462-5_4

Shah, K., Lathiya, D., Lukhi, N., Parmar, K., & Sanghvi, H. (2023). A systematic review of decentralized finance protocols. International Journal of Intelligent Networks, 4, 171–181. https://doi.org/10.1016/j.ijin.2023.07.002

Sharma, H., & Agarwal, S. (2024). The impact of decentralized finance (DeFi) on traditional financial systems: Opportunities, challenges, and regulatory implications. In Studies in Systems, Decision and Control (Vol. 525, pp. 211–218). https://doi.org/10.1007/978-3-031-54383-8_17

Singh, R., et al. (2025). Transforming financial services in India: Impact of blockchain technology and decentralized finance (DeFi). In Insights in Banking Analytics and Regulatory Compliance Using AI (pp. 333–355). https://doi.org/10.4018/979-8-3373-0209-6.ch016

Song, J., et al. (2025). Dimension expansion for learning money laundering activities hidden in transaction network. IEEE Transactions on Computational Social Systems. https://doi.org/10.1109/TCSS.2025.3599534

Suri, S., et al. (2023). An ensemble learning approach for classifying illicit transactions in Bitcoin. In Proceedings of the International Conference on Technological Advancements in Computational Sciences (ICTACS 2023) (pp. 76–81). https://doi.org/10.1109/ICTACS59847.2023.10390133

Venčkauskas, A., et al. (2025). Machine learning in money laundering detection over blockchain technology. IEEE Access, 13, 7555–7573. https://doi.org/10.1109/ACCESS.2024.3452003

Xia, L., Zhang, J., Zhang, X., Li, Y., Gao, J., Guan, Z., & Chen, Z. (2023). DIDAPPER: A practical and auditable on-chain identity service for decentralized applications. In Proceedings of the IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS). https://doi.org/10.1109/DAPPS57946.2023.00028

Yusran, A., Hardini, M., Hikam, I. N., Sunarya, P. A., & Rahardja, U. (2024). Transforming financial services with decentralized finance and blockchain technology. In Proceedings of the 6th International Conference on Cybernetics and Intelligent System (ICORIS). https://doi.org/10.1109/ICORIS63540.2024.10903742

Yusran, A., Hardini, M., Hikam, I. N., Sunarya, P. A., & Rahardja, U. (2024). Transforming financial services with decentralized finance and blockchain technology. In Proceedings of ICORIS 2024. https://doi.org/10.1109/ICORIS63540.2024.10903742