International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com

AI and Blockchain in Forensic Auditing: A Review of Tools for Investigating Financial Crimes in the U.S.

Olivia Larkwor Nartey[1], Evelyn Agyei[2], Barnabas Anim[3], Mary Magdalene Yeboah[4]

[1]Virginia Polytechnic Institute & State University, USA
[2]Valparaiso University, Valparaiso, IN, USA
[3]University of Bradford, Bradford, West Yorkshire, UK
[4]University of Ghana Business School, Ghana

ABSTRACT

The increasing complexity of financial crimes in the United States has created a pressing need for more advanced, efficient, and accurate forensic auditing methods. Artificial Intelligence (AI) has emerged as a transformative tool in this area. AI helps detect, analyze, and prevent financial fraud. It automates data analysis, recognizes hidden patterns, and enhances decision-making in forensic audits.

This study adopts a qualitative systematic literature review (SLR) approach. It examines the role of advanced technologies in forensic auditing and their application in investigating financial crimes in the United States.

The paper draws from current literature, case studies, and industry reports. It examines major AI-powered tools, including machine learning algorithms, natural language processing (NLP), neural networks, and predictive analytics systems. These tools are deployed by U.S. auditing firms and regulatory bodies.

The review highlights several benefits of these technologies. They improve the accuracy and timeliness of fraud detection. They help reduce audit fatigue. Additionally, they strengthen compliance with regulatory standards such as the Sarbanes–Oxley Act (SOX) and the Dodd-Frank Act.

The paper concludes that advanced technologies cannot entirely replace human judgment in forensic auditing. Instead, it serves as a powerful complement that significantly enhances the ability to uncover and prevent financial crimes in the U.S. financial system.

KEYWORDS: Artificial Intelligence (AI), forensic auditing**,** Machine learning, fraud detection, Blockchain

INTRODUCTION

Financial crimes pose a significant threat to the integrity and stability of the U.S. financial system. From corporate fraud and tax evasion to money laundering and cyber-enabled embezzlement, these crimes not only cause substantial economic losses but also erode public trust in financial institutions (Ogunti O, 2025). Traditional forensic auditing methods, though effective to an extent, are increasingly challenged by the vast volumes of digital financial data and the growing sophistication of criminal schemes. As a result, auditors and regulators have turned to advanced technologies to strengthen forensic investigations and improve the speed and reliability of fraud detection (Kokina & Davenport, 2017).

AI in forensic auditing refers to the integration of intelligent computational systems capable of learning from data, identifying irregularities, and supporting human auditors in complex decision-making processes. Machine learning algorithms can analyze historical transaction patterns to flag anomalies. Meanwhile, natural language processing (NLP) enables the examination of unstructured data such as emails, financial statements, and communication records for deceptive language or hidden connections (Hendrix and Lang, 2024). Neural networks and deep learning models further enhance pattern recognition, enabling auditors to detect subtle fraud indicators that may go unnoticed in manual reviews (Issa et al., 2016).

In the U.S., major accounting firms, including Deloitte, PwC, KPMG, and EY, have begun integrating AI tools into their forensic audit processes (Leocádio et al., 2024). Likewise, federal agencies, including the Securities and Exchange Commission (SEC) and the Financial Crimes Enforcement Network (FinCEN), employ AI-driven analytics to monitor suspicious transactions and compliance breaches. For example, the SEC's "Advanced Relational Trading Enforcement Metric Investigation System (ARTEMIS)" uses AI to detect insider trading patterns from millions of market transactions, while banks increasingly rely on AI-based anti-money laundering (AML) systems to meet regulatory requirements (Bertrand et al 2021).

Despite these advances, the adoption of AI in forensic auditing presents both opportunities and challenges. Concerns about data security, transparency of AI algorithms, and ethical implications of automated decision-making continue to shape the debate around its use (Felzmann et al, 2020). Moreover, the effectiveness of AI systems depends largely on the quality of data input and the expertise of forensic auditors who interpret the results (Appelbaum et al., 2017). Therefore, understanding the tools, applications, and limitations of AI in forensic auditing is essential for advancing financial crime investigations and ensuring accountability in the digital economy.

In the context of forensic auditing, blockchain enhances data integrity and transparency by providing a verifiable record of every financial transaction. Each entry on the blockchain serves as an auditable trail, allowing forensic investigators to trace the flow of funds, verify the legitimacy of transactions, and detect inconsistencies that may indicate fraud or manipulation. For instance, when a transaction is recorded on a blockchain, its digital signature ensures that both the source and destination of funds can be authenticated without ambiguity. This capability significantly reduces the risk of document forgery and unauthorized alterations, which are common in traditional accounting systems (Kshetri, 2018).

When combined, AI and blockchain create a synergistic forensic ecosystem. AI provides intelligent analytics while blockchain ensures the authenticity and immutability of the underlying financial data (Alaka et al 2025). Together, these technologies empower forensic auditors to operate with unprecedented speed, accuracy, and trustworthiness. AI-driven analytics can be trained directly on blockchain-verified datasets, reducing data bias and enhancing audit credibility. Likewise, blockchain can record the decision-making steps of AI models, providing a transparent trail of algorithmic actions for accountability and regulatory compliance (Dai & Vasarhelyi, 2017)

While AI focuses on analysis and pattern recognition, blockchain technology addresses another key forensic concern, evidence integrity and traceability. Blockchain operates as a decentralized, cryptographically secured ledger that records transactions in an immutable sequence of blocks. Each transaction is timestamped, verified by consensus among network participants, and linked to previous records, making retroactive alteration nearly impossible (Crosby et al., 2016). In forensic auditing, blockchain provides an incorruptible audit trail, ensuring that all financial entries are verifiable and tamper evident. This capability is invaluable for establishing a chain of custody over digital evidence, verifying the authenticity of records, and enabling auditors to reconstruct financial histories with precision (Kshetri, 2018).

Moreover, blockchain facilitates real-time collaboration among auditors, regulators, and financial institutions through permissioned ledgers. These systems allow authorized participants to access consistent and verifiable records while maintaining confidentiality through cryptographic controls (Androulaki et al., 2018). Smart contracts self-executing code embedded in blockchain for further automated audit triggers, compliance verification, and fraud detection. For instance, a smart contract can automatically flag, or halt suspicious transactions once pre-set risk thresholds are exceeded. Such automation enhances transparency and reduces opportunities for manipulation or concealment (Gaikwad, 2024).

The integration of AI and blockchain marks a fundamental transformation in forensic auditing practices. AI contributes predictive and diagnostic intelligence, while blockchain guarantees the authenticity and immutability of the underlying data. The U.S. SEC promotes cryptocurrency and AI financial regulation to protect investors and encourage innovation and competition (RootData, 2025). The SEC recognizes AI and blockchain as key enablers for automated trading, risk management, and regulatory oversight. FinCEN also plays a leading role in combating money laundering and ensuring compliance in digital assets through advanced blockchain analytics (Rodriguez Valencia et al., 2025; Alaka et al 2025).

Despite growing interest, empirical research exploring the combined impact of AI and blockchain in forensic auditing remains limited. Most existing studies examine AI and blockchain technologies separately. This leaves a gap in understanding how their integration can jointly improve fraud detection, evidence management, and compliance assurance (Alaka et al 2025). Consequently, this study aims to review current literature and assess the tools, benefits, and challenges of applying AI and blockchain in forensic auditing of financial crimes within the U.S. context. The analysis seeks to provide insights for practitioners, policymakers, and scholars on how these technologies can strengthen investigative accuracy. It also aims to highlight their role in enhancing ethical accountability and institutional resilience against financial misconduct.

LITERATURE REVIEW

The growing complexity of financial crimes in the United States has prompted forensic auditors to adopt Artificial Intelligence (AI) tools to enhance fraud detection and investigative efficiency. Literature widely agrees that AI technologies, particularly machine learning (ML), natural language processing (NLP), and network analytics, have transformed traditional auditing from manual, sample-based methods into automated, data-driven processes capable of analyzing large and diverse datasets (Alaka et al 2025).

The emergence of Artificial Intelligence has reshaped the landscape of forensic auditing by transforming how auditors detect, investigate, and prevent financial crimes. Over the past decade, a growing body of academic and professional literature has examined how these technologies can enhance transparency, automate the detection of fraud, and ensure the integrity of financial data (Omowole et al 2022). This literature review explores key themes in AI and blockchain applications in forensic auditing, focusing on empirical studies and theoretical frameworks. It further examines emerging research on their integration within the U.S. financial regulatory environment.

Artificial Intelligence in Forensic Auditing

AI has been widely recognized as a transformative force in auditing and accounting. Appelbaum et al. 2017 argue that AI and big data analytics have revolutionized audit engagements. This allows auditors to analyze massive datasets beyond the capabilities of traditional sampling methods. AI-driven systems can detect complex fraud schemes by recognizing unusual data patterns, classifying risky transactions, and predicting potential anomalies before they result in financial loss.

Machine learning (ML), a subset of AI, plays a central role in forensic analytics. ML algorithms learn from historical data to classify transactions as normal or suspicious based on predefined risk indicators. For instance, unsupervised learning techniques can identify outliers without prior labeling, making them suitable for detecting previously unknown fraud schemes (Issa et al., 2016). Neural networks and deep learning models enhance this process by detecting subtle relationships across large, unstructured datasets. Example includes payment histories, invoices, and vendor relationships (Goodfellow et al., 2016).

Furthermore, natural language processing (NLP) enables forensic auditors to analyze qualitative data sources emails, contracts, and reports, for deceptive language or collusion. Batool et al. (2025) note that NLP can help identify emotional tone, hidden intent, or inconsistencies in communication among executives, thus supplementing traditional audit evidence. According to Christina Ho (2025), Public Company Accounting Oversight Board (PCAOB) and major U.S. audit firms increasingly advocate integrating such technologies for continuous auditing and predictive fraud detection (Ho C, 2025).

However, scholars also highlight challenges in applying AI to forensic auditing. One major concern is the "black box" problem. AI systems often produce accurate predictions without transparent reasoning. Ribeiro et al., 2016) argue that the lack of model interpretability can hinder auditors' ability to explain findings in legal or regulatory contexts. Moreover, AI models depend heavily on the quality of training data; biased or incomplete datasets can lead to false positives, misclassification, or missed fraud cases. Consequently, researchers recommend the adoption of Explainable AI (XAI) frameworks that combine algorithmic transparency with human judgment (Kokina & Davenport, 2017).

Supervised models such as decision trees, random forests, and neural networks are employed to predict fraudulent activity based on historical patterns, while unsupervised techniques like clustering and anomaly detection uncover irregularities in unlabeled data (Chandola et al., 2009; Goodfellow et al., 2016). These approaches have proven valuable in detecting emerging fraud schemes that traditional rule-based systems often miss. Hybrid ML models that combine both supervised and unsupervised methods are increasingly common in fraud risk assessment (Akoglu et al., 2015).

Natural language processing (NLP) plays a critical role in examining unstructured data sources such as emails, reports, and contracts for linguistic cues of deception, unusual sentiment, or undisclosed relationships (Loughran & McDonald, 2011; Alaka et al 2025). With advances in deep learning, NLP models can now detect subtle inconsistencies in textual narratives, thereby enhancing the reliability of forensic document analysis. Similarly, graph analytics and network modeling have become vital tools for identifying hidden relationships and suspicious connections among entities, particularly in anti-money laundering (AML) investigations (Akoglu et al., 2015).

AI-powered transaction monitoring systems are also transforming AML compliance in U.S. financial institutions. By integrating ML-based risk scoring and anomaly detection, these systems improve the accuracy of suspicious activity reporting and reduce false positives that previously burdened human investigators (Mousavian & Miah (2025).

However, literature cautions that challenges remain, including algorithmic transparency, model governance, and data privacy concerns (Felzmann et al., 2020).

Explainable AI (XAI) frameworks such as LIME and SHAP are increasingly emphasized to ensure that AI-generated audit findings are interpretable and legally defensible (Ribeiro et al., 2016; Mousavian & Miah, 2025). LIME helps forensic auditors by providing clear, local explanations for individual AI predictions. It approximates complex models around specific transactions or cases with simpler, interpretable models, enabling auditors to understand why a particular transaction was flagged. This localized transparency supports the validation of fraud alerts and anomaly detection, helping auditors trust the AI outputs and make informed decisions based on concrete rationale.

In forensic auditing, SHAP quantifies each feature's contribution to a fraud prediction, highlighting key drivers behind suspicious activities across datasets. This global and local interpretability helps auditors identify systematic fraud patterns, assess model fairness, and ensure compliance with accountability standards. This enhances the overall effectiveness and trustworthiness of AI-assisted audits (Ahmed et al., 2024). Scholars stress that forensic auditing requires human oversight and that AI tools should augment, not replace, professional judgement. Continuous training and cross-disciplinary collaboration between auditors, data scientists, and regulators are therefore essential for ethical and effective implementation (Issa et al., 2016).

Blockchain In Forensic Auditing

While AI focuses on fraud detection and pattern recognition, blockchain addresses the need for data authenticity and audit trail integrity. Blockchain technology operates as a decentralized ledger, recording transactions across a network of computers in an immutable and cryptographically secure format. Every transaction, once verified, becomes part of a permanent record that cannot be retroactively altered (Crosby et al., 2016). This property makes blockchain an ideal tool for maintaining forensic evidence and ensuring data credibility during investigations.

Blockchain has potential in ensuring data provenance and the ability to trace the origin and modification history of financial records. Dai and Vasarhelyi (2017) emphasize that blockchain's immutable nature enhances the reliability of audit evidence. This allows auditors to confirm that financial data has not been tampered with. Similarly, Kshetri (2018) notes that blockchain-based auditing systems can automate compliance and verification processes, reducing the need for intermediaries and enhancing efficiency.

Another important development is the use of smart contracts; self-executing programs embedded in blockchain networks. Smart contracts can enforce predefined audit and compliance rules, automatically flagging transactions that violate financial regulations or internal policies (Androulaki et al., 2018). For instance, within anti-money laundering (AML) frameworks, smart contracts can restrict high-risk transactions and generate real-time alerts for auditors. This automation improves detection speed while minimizing human error (Nita, B. 2025).

Moreover, blockchain facilitates continuous auditing by providing auditors with real-time access to verified transactions. In traditional systems, auditors rely on periodic sampling, which may overlook fraud occurring between audit cycles. Blockchain eliminates this gap by ensuring that every transaction is automatically logged and accessible to authorized parties. This feature also supports collaboration between financial institutions, regulators, and auditors through permissioned blockchains, which restrict access to verified participants (Tapscott & Tapscott, 2018). Such collaboration enhances the transparency and timeliness of financial crime investigations, particularly within U.S. institutions under the Securities and Exchange Commission (SEC) and Financial Crimes Enforcement Network (FinCEN) oversight.

Nonetheless, the adoption of blockchain in forensic auditing is not without limitations. Zhang et al.,2019 observe that scalability and interoperability remain major technical hurdles. As the number of transactions grows, blockchain networks can experience performance bottlenecks, increasing costs and processing time. Additionally, legal frameworks in the U.S. have yet to fully recognize blockchain-based evidence, raising concerns about admissibility in court proceedings (Wang, X., et al., 2024). Data privacy regulations, such as the California Consumer Privacy Act (CCPA), also present challenges in reconciling

blockchain's immutability with individuals' "right to be forgotten (Alza Jr, 2021).
Overall, the reviewed literature concludes that AI significantly strengthens forensic auditing by enhancing accuracy, scalability, and speed in detecting financial crimes. Yet, issues of explainability, bias, and governance persist. This underscores the need for transparent models, ethical standards, and specialized auditor training to realize AI's full potential in safeguarding the U.S. financial system.

TECHNOLOGICAL IMPLICATIONS IN FORENSIC AUDITING

This study explored the role of advanced technologies in forensic auditing, focusing on their applications in investigating financial crimes in the United States. The systematic review of literature demonstrates that AI technologies particularly machine learning (ML), natural language processing (NLP), and graph analytics have become transformative elements in the detection and prevention of financial fraud. These tools allow forensic auditors to analyze massive volumes of structured and unstructured data with speed and precision unattainable by traditional audit techniques (Appelbaum et al., 2017).
AI-driven solutions significantly enhance the efficiency, accuracy, and predictive capability of forensic auditing. Machine learning algorithms can identify hidden anomalies and patterns in transactional data, while NLP models extract meaningful insights from textual evidence such as contracts and communications. Graph-based systems, on the other hand, reveal complex financial networks often used in money laundering or insider trading. Collectively, these technologies contribute to more robust fraud detection and financial crime prevention frameworks.
The integration of Artificial Intelligence (AI) and Blockchain Technology represents a transformation in the field of forensic auditing, particularly in the United States where financial crimes are becoming increasingly sophisticated. AI contributes through intelligent data analysis, predictive fraud detection, and automation of complex auditing tasks, while blockchain offers immutability, traceability, and verifiable digital audit trails. Moreover, AI-driven forensic enable auditors to detect anomalies and suspicious transactions in real time, reducing their dependency on traditional sampling techniques. These systems identify hidden fraud patterns that human auditors might overlook due to data overload or bias (Appelbaum et al., 2017; Issa et al., 2016). Predictive AI models can flag irregularities before they escalate, supporting proactive fraud prevention rather than reactive investigation. On the other hand, blockchain technology reinforces forensic integrity by ensuring that financial records cannot be tampered with once entered the distributed ledger. This immutability makes blockchain a reliable source of digital evidence for both auditors and regulators. And so blockchain not only prevents document manipulation but also allows auditors to verify the origin and legitimacy of each transaction with cryptographic assurance. The transparency of distributed ledgers further strengthens public confidence in financial reporting, especially when used in conjunction with smart contracts that automatically enforce compliance and internal control rules (Dai & Vasahelyi, 2017).
Perhaps the most promising finding is the synergistic potential of integrating AI and blockchain. Together, these technologies create a secure and intelligent auditing ecosystem where AI analyzes blockchain-verified data to uncover patterns of fraud with a high degree of accuracy. In turn, blockchain provides an immutable record of AI's analytic processes, ensuring accountability and auditability of automated decision-making (Kokina & Davenport, 2017). This integration represents a powerful response to persistent challenges in forensic auditing, such as manipulation of financial evidence, cross-border money laundering, and lack of transparency in audit trails.
Nevertheless, despite these advances, significant barriers remain. Ethical and legal concerns such as algorithmic bias, explainability, privacy rights, and admissibility of digital evidence pose real obstacles to

full adoption. Technical challenges like system interoperability, high implementation costs, and lack of specialized auditor training further slow progress (Zhang et al., 2019). Again, the regulatory landscape in the U.S., governed by bodies like the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB), has yet to develop comprehensive standards for AI- and blockchain-based audits.

However, the study also highlights critical limitations and ethical challenges. Many AI models operate as "black boxes," offering little interpretability in legal and regulatory contexts. Data quality issues, algorithmic bias, and privacy concerns remain major obstacles to full-scale implementation. Moreover, the literature emphasizes that AI cannot entirely replace human judgment. Expertise, skepticism, and contextual understanding of auditors remain essential to ensure that AI-driven results are properly validated and ethically applied. The evidence supports that AI and blockchain are not merely technological trends but transformational tools capable of reshaping the foundations of forensic auditing. Their combined use enhances fraud detection accuracy, improves audit transparency, and strengthens regulatory compliance. However, to fully realize these benefits, the U.S. auditing ecosystem must establish clear governance frameworks, promote auditor education, and foster cross-industry collaboration to ensure ethical and effective deployment.

RECOMMENDATIONS

Based on the findings and the current state of research, the following recommendations are proposed to strengthen the adoption and governance of AI and blockchain in forensic auditing in the U.S.:

1. Develop Regulatory and Legal Frameworks for AI and Blockchain Auditing

The U.S. auditing and regulatory bodies, including the SEC, PCAOB and FinCEN should collaborate to design comprehensive legal standards for the use of AI and blockchain in forensic investigations. These frameworks should define:

a. How blockchain records can be admitted as legal evidence in court.
b. How AI-generated findings should be documented and validated.
c. Ethical principles governing algorithmic transparency, data privacy, and accountability.

Establishing such standards would promote consistency, reduce legal ambiguity, and ensure that AI and blockchain evidence meet the same probative thresholds as traditional audit documentation (Hongdan et al, 2023).

2. Promote Auditor Training and Digital Forensic Competencies

Forensic auditors must acquire new technical skills to operate and interpret AI and blockchain systems effectively. Universities, professional bodies, and audit firms should integrate data analytics, machine learning, cybersecurity, and blockchain validation into their curricula and training programs. Professional organizations such as the American Institute of Certified Public Accountants (AICPA) should mandate continuous professional education (CPE) courses focusing on emerging technologies in forensic auditing. This investment in human capital will reduce the skills gap and enhance the credibility of technology-assisted investigations (Alaka et al 2025, Turning Numbers, 2025).

3. Encourage Adoption of Explainable and Ethical AI

Given the "black box" nature of some AI algorithms, forensic auditing must prioritize Explainable Artificial Intelligence (XAI) models. XAI provides transparency into how algorithms reach their conclusions, which is crucial for courtroom admissibility and auditor accountability (Hermosilla, et al., 2025).

Regulators should require that all AI systems used in forensic audits produce an interpretable, auditable decision log (Alaka et al., 2025). This ensures that machine-assisted judgments are transparent, unbiased, and verifiable, protecting both auditors and accused entities from potential errors or bias.

4. Leverage Blockchain for Continuous and Real-Time Auditing

Organizations and audit firms should utilize blockchain's capabilities to implement continuous auditing systems, which allow real-time verification of transactions as they occur. This approach minimizes the time gap between fraudulent activity and detection, significantly improving response time in financial crime investigations (Dai & Vasarhelyi, 2017). Blockchain-enabled smart contracts can also automate compliance checks and trigger alerts when transactions deviate from approved patterns, creating an autonomous internal control system that supports human auditors (Zaruba et al.,2024).

5. Foster Collaboration Between Regulators, Technology Firms, and Academia

Collaboration is essential to ensure that forensic auditing technology evolves responsibly. Regulators should partner with technology companies, academic researchers, and auditing firms to test AI and blockchain systems in sandbox environments.

Such partnerships will promote shared learning, accelerate innovation, and help regulators stay ahead of emerging financial crime tactics. The creation of a National Forensic Technology Consortium could provide a centralized platform for research, standard setting, and knowledge exchange among stakeholders (Norta et al.,2025).

6. Address Privacy, Security, and Interoperability Concerns

While blockchain's transparency enhances audit trust, it can conflict with privacy laws such as the California Consumer Privacy Act (CCPA). Developers must adopt privacy-preserving cryptographic techniques, for example, zero-knowledge proofs and permissioned blockchains to ensure compliance while maintaining data integrity.

Additionally, interoperability standards should be established so that AI and blockchain systems across different audit firms and regulators can exchange data securely and efficiently (Zhou & Böhme, 2025).

7. Provide Government Incentives and Support for Adoption

Government agencies should offer tax incentives, grants, and pilot funding to encourage small and medium sized audit firms to adopt AI and blockchain tools. This will prevent technological monopolization by large firms and promote equitable access to forensic innovation across the industry. Public private partnerships could further support national initiatives aimed at modernizing forensic auditing infrastructure (Sadu, 2017).

CONCLUSION

In summary, the convergence of AI and blockchain technologies represents a revolutionary frontier in forensic auditing. Their joint application can deter financial crime, improve evidentiary reliability, and restore public confidence in corporate governance. However, technology alone cannot replace human judgment; it must instead serve as an intelligent partner to auditors, one that amplifies human expertise, ethical reasoning, and accountability.

The future of forensic auditing will therefore depend not only on technological innovation but also on the responsible integration of human and artificial intelligence to uphold justice, transparency, and trust in financial systems.

References

1. Ahmed Salih, Zahra Raisi, Ilaria Boscolo Galazzo & Petia Radeva (2024): A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME.

2. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 29(3), 626-688.
3. Alaka, E., Akindayo, A. E., Ilemore, O., & Emmanuel, I. (2025). The integration of artificial intelligence in forensic auditing and its implications for real-time fraud detection in global financial institutions. International Journal of Innovative Science and Research Technology, 10(9), 1688-1707. https://doi.org/10.38124/ijisrt/25sep1334
4. Alza Jr., G. (2021). Blockchain & CCPA. Santa Clara Law Digital Commons.
5. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference.
6. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27.
7. Bertrand, A., Maxwell, W., & Vamparys, X. (2021). Do AI-based anti-money laundering (AML) systems violate European fundamental rights? International Data Privacy Law, 11(3), 276–293. https://doi.org/10.1093/idpl/ipab010
8. Batool, I., Wakeel, S., & bin Asad, D. (2025). The Future of Auditing: How Artificial Intelligence and Blockchain Technology Are Revolutionizing the Industry. *Review of Applied Management and Social Sciences*, *8*(1), 531-546.
9. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6–10.
10. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21.
11. Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. Science and Engineering Ethics, 26(6), 3333-3361.
12. Gaikwad, M. M. (2024). Development of blockchain based smart contracts for digital forensic. International Journal of Novel Research and Development, 9(6), 364-374.
13. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
14. Hashem, R. E. E. D., Mubarak, A. I., & Abu-Musa, A. A. E. (2023). The impact of blockchain technology on audit process quality: An empirical study on the banking sector. International Journal of Auditing and Accounting Studies, 5(1), 87-118. https://doi.org/10.47509/IJAAS.2023.v05i01.04
15. Hendrix, D., & Lang, H. (2024). The use of AI in real-time transaction monitoring and anomaly detection. SSRN. https://ssrn.com/abstract=5393794
16. Hermosilla, P., Berríos, S., & Allende-Cid, H. (2025). Explainable AI for forensic analysis: A comparative study of SHAP and LIME in intrusion detection models. Applied Sciences, 15(13), 7329. https://doi.org/10.3390/app15137329
17. Ho, C. (2025). AI and the pursuit of audit quality: A regulatory perspective. Speech presented at the PCAOB. https://pcaobus.org/news-events/speeches/speech-detail/ai-and-the-pursuit-of-audit-quality--a-regulatory-perspective
18. Hongdan, H., Radha, K., Mordi, C., Botchie, D., & Shiwakoti, R. (2023). Accounting and auditing with blockchain technology and artificial intelligence. International Journal of Accounting Information Systems, 48(3), 100598. https://doi.org/10.1016/j.accinf.2022.100598
19. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in

Accounting, 13(2), 1–20. Journal of Artificial Intelligence Research. DOI:10.1002/aisy.202400304
20. Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122.
21. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89.
22. Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Generation Computer Systems, 120, 13-25.
23. Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. *Administrative Sciences*, *14*(10), 238.
24. Loughran, T., & McDonald, B. (2011). When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks. The Journal of Finance, 66(1), 35-65.
25. Mousavian, S., & Miah, S. J. (2025). Review of artificial intelligence-based applications for anti-money laundering. Knowledge and Information Systems.
26. Murtaza, B. I., Wakeel, S., & Asad, D. B. (2025). The future of auditing: How artificial intelligence and blockchain technology are revolutionizing the industry. Review of applied Management and Social Sciences, 8(1), 531-546. https://doi.org/10.47067/ramss.v8i1.499
27. Batool, I., Wakeel, S., & bin Asad, D. (2025). The Future of Auditing: How Artificial Intelligence and Blockchain Technology Are Revolutionizing the Industry. *Review of Applied Management and Social Sciences*, *8*(1), 531-546.
28. Nita, B. (2025). Blockchain Technology in Anti-Money Laundering: Challenges and Opportunities in the V4 Countries and Ukraine.
29. Norta, A., Udokwu, C., Voicu-Dorobanțu, R., Ogunyemi, A. A., Sturua, N., & Crass, S. (2025). Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience.
30. Ogunti, O. (2025). The economic and national security implications of money laundering and fraud in the US. International Journal of Public Policy and Administration, 7(1), 68-83.
31. Omowole, B. M., Adewusi, S. A., Chiekezie, N., & Eyo-Udo, R. (2022). Blockchain-enhanced financial transparency. American Journal of Social Science and Economics Innovation, 9(1), 59-77.
32. Qader, K. S., & Cek, K. (2024). Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey. Heliyon, 10(9), e30166.
33. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.
34. Rodríguez Valencia, L., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. D. V., ... & Levi Alfaroviz, A. (2025). A Systematic Review of Artificial Intelligence Applied to Compliance: Fraud Detection in Cryptocurrency Transactions. *Journal of Risk and Financial Management*, *18*(11), 612.
35. RootData. (2025). The U.S. SEC promotes cryptocurrency and AI financial regulation to protect investors and encourage innovation and competition with a principle of minimal intervention. https://www.rootdata.com/news/361192
36. Sadu, I. (2017). Digital Forensics in the Audit of Public Private Partnerships–A Case Study. Forensic Research & Criminology International Journal, 4(6).
37. Turning Numbers. (2025). Key skills every forensic accountant should have. https://www.turningnumbers.com/blog/key-skills-every-forensic-accountant-should-have

38. Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: Exploring its evidentiary significance and the procedural implications of integrating this technology into the U.S. judicial system. Frontiers in Blockchain, 7, 1306058.
39. ZARUBA SMITH, S. A. M. U. E. L., & GARCIA, A. (2024). Blockchain Smart Contracts, Part 4: How to Audit. *ISACA Journal*, (2).
40. Zhang, R., George, A., Kim, J., Johnson, V., & Ramesh, B. (2019). Benefits of blockchain initiatives for value-based care: Proposed framework. Journal of Medical Internet Research, 21(9), e13595.
41. Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), 1-34. https://doi.org/10.1145/3316481
42. Zhou, E., & Böhme, R. (2025). A privacy preserving and auditable blockchain framework for securities trading. *Frontiers in Blockchain, 8*, Article 754321.