CITE PUBLICATIONS

Journal of Analytical and Applied Computer Sciences
Volume: 1, Issue: 1, 2025 (December), Pages: 1-5
ISSN (Online): 3139-3349 | DOI: https://doi.org/10.67914/jaacs/ra/1.1/1-5
Review Article

Blockchain and Artificial Intelligence - A Comprehensive Review of Integration and Applications

Shamim B*, SK Rizwana, K.Z. Krishna Teja

Department of Computer Science, Kakaraparti Bhavanarayana College,Vijayawada-520001.

***Correspondence**
Shamim
shamim.karima05@kbncollege.ac.in

Creative Commons Attribution–NonCommercial–NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Received: 12 August 2025 / Accepted: 22 November 2025 / Published: 31 December 2025

Blockchain and Artificial Intelligence (AI) are two transformative technologies that are reshaping modern digital systems. While AI enables intelligent decision-making through data-driven models, blockchain provides decentralized, transparent, and tamper-resistant data management. Their integration has gained increasing attention as a means to address limitations inherent in each technology when deployed independently. This review paper presents a comprehensive survey of blockchain–AI integration, focusing on architectural models, enabling techniques, application domains, and current challenges. The study examines how blockchain enhances trust, data integrity, and accountability in AI systems, while AI improves scalability, efficiency, and automation within blockchain networks. Key application areas including healthcare, finance, Internet of Things, supply chain management, and smart cities are discussed. The paper further identifies open research challenges and future directions necessary to realize secure, scalable, and intelligent decentralized systems.

Keywords: *Blockchain, Artificial Intelligence, Distributed Ledger, Machine Learning, Smart Contracts, Decentralized Systems, Trustworthy AI*

Introduction

Artificial Intelligence has emerged as a cornerstone of modern computing, enabling systems to learn from data, recognize patterns, and make autonomous decisions (Russell & Norvig, 2021). Concurrently, blockchain technology has evolved as a decentralized ledger framework that ensures transparency, immutability, and trust without centralized intermediaries (Nakamoto, 2008). Although both technologies have demonstrated significant success independently, their integration has attracted growing research interest due to complementary strengths. AI systems often suffer from issues related to data privacy, model transparency, and trustworthiness, particularly in centralized architectures (Veale & Edwards, 2018). Blockchain, on the other hand, faces challenges related to scalability, computational efficiency, and intelligent automation (Croman et al., 2016). Integrating blockchain with AI has been proposed as a promising approach to mitigate these limitations by enabling secure data sharing, decentralized AI model governance, and verifiable decision-making processes (Christidis & Devetsikiotis, 2016). This review paper surveys recent research on blockchain–AI integration, analysing architectural approaches, application domains, and unresolved challenges. The objective is to provide a structured understanding of how these technologies can jointly enable trustworthy and intelligent decentralized applications (Chen et al., 2018).

Background Technologies

Blockchain Technology

Blockchain is a distributed ledger system in which transactions are recorded in immutable blocks linked through cryptographic hashes (Nakamoto, 2008). Consensus mechanisms such as Proof of Work, Proof of Stake, and Byzantine Fault Tolerant protocols ensure agreement among distributed participants (Wang et al., 2019). Smart contracts further extend blockchain functionality by enabling programmable and automated execution of predefined rules (Szabo, 1997).

Artificial Intelligence and Machine Learning

AI encompasses techniques such as machine learning, deep learning, and reinforcement learning that allow systems to infer patterns and make predictions from data (Russell & Norvig, 2021). These models are typically trained on large datasets and require substantial computational resources. Challenges related to explainability, bias, and data integrity remain significant concerns (Adadi & Berrada, 2018).

Models of Blockchain–AI Integration

Blockchain for AI (BfAI)

In this model, blockchain is used to enhance AI systems by ensuring data integrity, traceability, and secure model sharing. Training data and model updates can be stored on-chain or referenced through blockchain-based hashes, enabling auditability and trust in AI outputs (Christidis & Devetsikiotis, 2016; Salah et al.,2019).

AI for Blockchain (AI4B)

AI techniques are employed to optimize blockchain operations, including consensus selection, transaction validation, and anomaly detection. Machine learning models can improve throughput, reduce energy consumption, and enhance network security (Zhang et al., 2020).

Hybrid Architectures

Hybrid architectures combine both approaches, allowing AI and blockchain to mutually reinforce each other. These systems often employ off-chain AI computation with on-chain verification to balance efficiency and security (Chen et al., 2018).

Key Application Domains

Healthcare Systems

Blockchain–AI integration enables secure sharing of medical data while supporting AI-driven diagnostics and predictive analytics. Blockchain ensures patient data privacy and consent management, while AI enhances clinical decision-making (Azaria et al., 2016).

Financial Services and FinTech

In finance, AI models support fraud detection, credit scoring, and algorithmic trading, while blockchain provides transparent and tamper-proof transaction records. Decentralized Finance (DeFi) platforms increasingly adopt AI for risk assessment and automated governance (Schär, 2021).

Internet of Things (IoT)

IoT systems generate large volumes of data that require secure management and intelligent processing. Blockchain ensures trusted device authentication and data integrity, while AI enables real-time analytics and autonomous control (Conoscenti et al., 2016).

Supply Chain Management

Blockchain improves supply chain transparency and traceability, whereas AI enhances demand forecasting, logistics optimization, and anomaly detection. Their integration enables resilient and intelligent supply networks (Kim & Laskowski, 2018).

Smart Cities

Smart city applications leverage blockchain–AI systems for traffic management, energy optimization, and public service automation. Decentralized governance models supported by blockchain improve accountability and citizen trust (Allam & Jones, 2020).

Security, Privacy, and Trust

Blockchain enhances AI security by providing immutable logs of data usage and model decisions, reducing risks of data tampering and unauthorized modifications (Li et al., 2020). Privacy-preserving techniques such as federated learning and zero-knowledge proofs are increasingly combined with blockchain to protect sensitive information while enabling collaborative AI training (Yang et al., 2019). Despite these advances, smart contract vulnerabilities, model poisoning attacks, and data leakage remain critical concerns requiring further research (Atzei et al., 2017).

Challenges and Limitations

Scalability and Performance

Blockchain networks often struggle with latency and throughput, which can hinder real-time AI applications (Croman et al., 2016).

Computational Overhead

AI training is resource-intensive, and executing such processes directly on-chain is impractical, necessitating off-chain solutions (Chen et al., 2018).

Data Privacy and Regulation

Compliance with data protection regulations such as GDPR remains challenging due to blockchain's immutable nature (Azaria et al., 2016).

Standardization and Interoperability

Lack of common standards limits seamless integration across platforms and applications (Salah et al., 2019).

Research Gaps and Open Issues

Key research gaps identified in the literature include:

- Lack of standardized architectures for blockchain–AI integration
- Limited empirical evaluation of large-scale deployments
- Insufficient focus on explainable and ethical AI in decentralized environments
- Challenges in aligning blockchain immutability with regulatory requirements
- Need for energy-efficient and sustainable integrated systems

Future Research Directions

Future research should focus on lightweight consensus mechanisms, decentralized AI governance frameworks, and privacy-preserving learning models. Integration with edge and federated computing is expected to play a crucial role in enabling scalable and responsive blockchain–AI systems. Interdisciplinary collaboration between computer science, law, and policy domains will be essential for widespread adoption.

Conclusion

This review paper has presented a comprehensive analysis of blockchain and artificial intelligence integration, highlighting architectural models, application domains, and persistent challenges. While the synergy between blockchain and AI offers significant potential for building secure, transparent, and intelligent systems, technical and regulatory barriers remain. Addressing identified research gaps will be critical for realizing the full benefits of decentralized and trustworthy AI-driven applications.

Author contributions

All authors contributed significantly to the preparation of this manuscript.

Shamim conceptualized the study, conducted the primary literature survey, and drafted the initial manuscript.

Sk Rizwana contributed to the analysis of blockchain and AI integration models, application domains, and critically revised the manuscript for technical accuracy.

K. Z. Krishna Teja M contributed to the review of security, privacy, challenges, and future research directions, and assisted in manuscript structuring and final editing.

All authors have read and approved the final version of the manuscript.

Funding

No funding.

Conflict of interest

The authors declare that there is no conflict of interest, financial or otherwise, related to the publication of this research paper.

Ethics approval

This study is a review-based research work and does not involve human participants, animals, or sensitive personal data. Therefore, ethical approval and informed consent are not applicable for this study.

AI tool usage declaration

The authors declare that AI-assisted tools were used only for language refinement, grammar correction, and formatting support during manuscript preparation. The intellectual content, literature analysis, interpretations, and conclusions are entirely the responsibility of the authors. No AI system was used to generate original scientific claims, data, or research results.

References

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the GDPR. *Computer Law & Security Review, 34*(2), 398–404.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). On scaling decentralized blockchains. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC 2016)* (pp. 106–125). Springer.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303.

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-based artificial intelligence technology. *IEEE Network, 32*(6), 180–187.

Wang, Q., Liu, X., Wu, Y., He, J., Gao, Q., & Wang, F. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Systems Journal, 13*(2), 910–923.

Szabo, N. (1997). *Smart contracts*.

Adadi, A., & Berrada, M. (2018). Peeking inside the black box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6*, 52138–52160.

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access, 7*, 10127–10149.

Zhang, L., Xiong, Y., Fan, L., & Tang, S. (2020). AI-powered blockchain: Technology, applications and challenges. *Future Generation Computer Systems, 103*, 1–12.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the IEEE Open & Big Data Conference* (pp. 25–30). IEEE.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153–174.

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *IEEE Communications Surveys & Tutorials, 20*(2), 1465–1492.

Kim, T. H., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. In *Proceedings of the IEEE International Conference on Blockchain (ICBC 2018)* (pp. 1–8). IEEE.

Allam, Z., & Jones, D. S. (2020). On the coronavirus (COVID-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management. *Cities, 99*, 102568.

Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2020). Securing proof-of-stake blockchain protocols. *Future Generation Computer Systems, 107*, 456–467.

Yang, K., Ren, J., Zhu, H., Zhang, Y., & Shen, X. (2019). Blockchain-based federated learning for secure data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics, 15*(6), 3587–3597.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC 2017)* (pp. 164–186). Springer.

Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653–659.