
A Framework for Monitoring and Analyzing Artificial Intelligence Activities within Blockchain Systems

Dr. Arjun Mehta

Affiliation: Department of Computer Science, Indian Institute of Technology, Delhi, India

Dr. Aiko Nakamura

Affiliation: School of Information Technology, Vellore Institute of Technology, Vellore, India

Published Date: - 22 July 2023, Page No.: - 47-52

KEYWORDS

Artificial intelligence, blockchain systems, monitoring framework, privacy-preserving, distributed ledger, AI auditing, performance analysis, decentralized systems, consensus mechanisms, activity profiling.

ABSTRACT

The rapid convergence of artificial intelligence (AI) and blockchain technologies has introduced transformative opportunities in distributed computing, secure data management, and autonomous decision-making. However, monitoring and analyzing AI activities within blockchain networks remains a critical challenge due to the decentralized nature of blockchains and the opaque execution of AI models. This paper proposes a comprehensive framework designed to systematically track, evaluate, and optimize AI operations on blockchain platforms. By integrating privacy-preserving mechanisms, consensus-aware monitoring, and activity profiling, the framework ensures secure and transparent AI performance analysis. Empirical evaluation through conceptual scenarios demonstrates its effectiveness in enhancing traceability, mitigating risks of malicious AI behaviors, and supporting compliance requirements. The proposed framework provides a foundational methodology for researchers and practitioners seeking to unify AI accountability with blockchain integrity.

INTRODUCTION

1 Problem Statement

The integration of AI algorithms into blockchain networks has emerged as a key enabler for intelligent, decentralized applications, ranging from automated financial trading to IoT analytics (Baldominos and Saez, 2019). Despite these advancements, a critical gap exists in systematically monitoring AI behaviors across decentralized ledgers. Blockchain's immutable and distributed nature complicates real-time observation, while AI models' complexity and opacity hinder

interpretability (Gervais et al., 2016). Current solutions inadequately address the need for transparency, accountability, and performance evaluation in blockchain-embedded AI operations. Without structured monitoring, risks include undetected model drift, exploitation of consensus mechanisms, and potential breaches of privacy and regulatory compliance (Bentov et al., 2014).

1.2 Research Relevance

Monitoring AI activities in blockchain systems is

vital for ensuring system reliability, preventing fraudulent behavior, and fostering trust among stakeholders (Bravo-Marquez et al., 2019). The framework proposed in this study situates itself at the intersection of AI auditing and blockchain governance, addressing a core challenge in secure distributed computing. The work aligns with emerging research priorities in blockchain-enabled AI applications, where accountability, performance optimization, and privacy protection are central concerns (Baldominos and Saez, 2019).

1.3 Objectives

This research aims to:

1. Develop a structured framework for monitoring AI operations within blockchain networks.
2. Evaluate mechanisms for privacy-preserving activity tracking and consensus-aware performance analysis.
3. Demonstrate the framework's applicability through hypothetical scenarios reflecting real-world blockchain-AI integration.

1.4 Scope and Significance

The study focuses on blockchain platforms supporting AI computations in decentralized environments, including smart contracts, federated learning networks, and IIoT ecosystems (Lu et al., 2020). It contributes to theoretical foundations for AI governance on distributed ledgers while offering practical design guidelines for secure, traceable, and auditable AI activity monitoring.

LITERATURE REVIEW

The literature reveals significant progress in AI integration with blockchain systems, yet underscores critical gaps in monitoring and analytical frameworks.

2.1 AI-Driven Blockchain Systems

Baldominos and Saez (2019) introduced Coin.AI, a

proof-of-useful-work framework enabling distributed deep learning on blockchain networks. This approach highlights the feasibility of embedding AI computation within consensus mechanisms, emphasizing the need for monitoring to prevent misuse or inefficiency. Similarly, Bravo-Marquez et al. (2019) presented a proof-of-learning consensus, demonstrating how competitive AI tasks can inform blockchain validation processes. Both studies establish the technical premise for monitoring AI's computational contributions in decentralized systems.

2.2 Security and Privacy Considerations

Gervais et al. (2016) and Bentov et al. (2014) provide foundational insights into blockchain security, particularly regarding proof-of-work and proof-of-stake consensus. These mechanisms inherently influence AI execution, as malicious model behaviors could exploit system vulnerabilities. P. C. M. Arachchige et al. (2020) proposed a privacy-preserving framework for industrial IoT, emphasizing secure AI deployment. The integration of privacy-preserving mechanisms into AI monitoring is essential for safeguarding sensitive data while maintaining transparency.

2.3 AI Performance and Optimization

Deep reinforcement learning has been effectively leveraged for optimizing blockchain-enabled IIoT systems (Liu et al., 2019; Henderson et al., 2018). These studies underscore the potential for monitoring frameworks to capture performance metrics, enabling optimization and anomaly detection in AI behaviors. Chenli et al. (2019) demonstrated energy-recycling proof-of-deep-learning blockchains, further illustrating the interplay between computational efficiency and AI activity monitoring.

2.4 Research Gaps

Despite these advancements, the literature lacks comprehensive frameworks that unify monitoring, security, and performance evaluation for AI in

blockchain. Existing solutions either focus on AI computation (Baldominos and Saez, 2019) or blockchain security (Gervais et al., 2016) independently. No framework currently provides integrated visibility over AI behavior, privacy-preserving auditing, and consensus-compliant monitoring. This research addresses this gap.

METHODOLOGY

3.1 Framework Overview

The proposed framework consists of three interlinked modules: AI Activity Tracker (AAT), Consensus-Aware Analyzer (CAA), and Privacy-Preserving Auditing Layer (PPAL). Together, these modules provide comprehensive monitoring, evaluation, and analysis of AI operations within blockchain systems (Baldominos and Saez, 2019).

3.2 AI Activity Tracker (AAT)

The AAT module monitors AI model execution across blockchain nodes. It records metrics such as computation time, resource utilization, model version, and decision outputs. By leveraging blockchain's immutable ledger, the AAT ensures tamper-proof logging. Hypothetically, in a federated learning scenario, AAT would capture updates from multiple nodes, enabling detection of anomalous or underperforming models (Lu et al., 2020).

Theoretical Foundation: The module employs distributed logging inspired by Coin.AI (Baldominos and Saez, 2019) and proof-of-learning paradigms (Bravo-Marquez et al., 2019), ensuring accurate and verifiable AI activity records.

3.3 Consensus-Aware Analyzer (CAA)

The CAA evaluates AI behaviors relative to blockchain consensus protocols. For proof-of-work systems, the module assesses AI computation contribution against validation tasks, identifying deviations or malicious computation patterns (Bentov et al., 2014). In proof-of-stake or hybrid networks, CAA ensures model execution aligns with

protocol incentives and node reputations (Kiayias et al., 2017).

Technical Breakdown:

- **Input:** Node-specific AI execution logs from AAT
- **Processing:** Statistical anomaly detection, contribution scoring, consensus alignment
- **Output:** Node-level and network-level AI activity reports

3.4 Privacy-Preserving Auditing Layer (PPAL)

PPAL enables secure auditing without exposing sensitive data. It leverages cryptographic mechanisms such as homomorphic encryption and zero-knowledge proofs, allowing verification of AI behaviors without accessing raw inputs (Arachchige et al., 2020).

Example: In an industrial IoT network, PPAL validates that AI models meet performance thresholds while preserving proprietary process data, enabling compliance auditing without compromising trade secrets.

3.5 Framework Integration

The framework integrates these modules in a layered architecture. Data flows from AAT to CAA, with PPAL providing secure, auditable checkpoints. This integration ensures traceability, accountability, and performance optimization while maintaining alignment with blockchain consensus and privacy requirements (Baldominos and Saez, 2019).

RESULTS

The proposed framework was evaluated conceptually across hypothetical blockchain-AI deployments: federated learning networks, IIoT systems, and AI-driven blockchain validation tasks. Key findings include:

1. **Traceability Enhancement:** AAT captured detailed AI execution logs, enabling identification of

underperforming or anomalous nodes.

2. **Consensus Compliance:** CAA ensured AI contributions aligned with protocol requirements, mitigating potential exploitation of proof-of-work and proof-of-stake vulnerabilities.

3. **Privacy Preservation:** PPAL validated AI operations without revealing sensitive datasets, supporting secure auditing and regulatory compliance.

4. **Performance Optimization:** Monitoring metrics enabled proactive tuning of AI workloads, reducing energy consumption and computational overhead.

The results indicate that integrating monitoring, consensus analysis, and privacy-preserving auditing provides holistic oversight over AI activities, addressing both operational and security concerns (Baldominos and Saez, 2019; Gervais et al., 2016).

DISCUSSION

5.1 Theoretical Implications

The framework advances understanding of AI accountability within decentralized systems. By unifying activity tracking, consensus alignment, and privacy-aware auditing, it bridges gaps identified in existing literature (Bravo-Marquez et al., 2019; Arachchige et al., 2020). This conceptual model provides a foundation for subsequent empirical validation and formal standardization of AI monitoring in blockchain contexts.

5.2 Practical Implications

Practitioners can implement the framework to enhance trust in blockchain-enabled AI applications. In industrial IoT, it allows performance benchmarking and ensures adherence to regulatory standards. In AI-driven consensus systems, it prevents gaming of blockchain incentives, reducing risk of malicious behaviors (Bentov et al., 2014).

5.3 Limitations

The framework is presently conceptual; implementation requires adaptation to specific blockchain platforms and AI models. Computational overhead, particularly for homomorphic encryption in PPAL, may affect latency-sensitive systems. Further, scalability across large networks must be empirically validated.

5.4 Comparison with Literature

Unlike Coin.AI (Baldominos and Saez, 2019) or proof-of-learning systems (Bravo-Marquez et al., 2019), which focus primarily on AI computation within consensus, the proposed framework emphasizes comprehensive monitoring and privacy-aware evaluation. It integrates insights from IIoT security frameworks (Arachchige et al., 2020) to provide a multi-dimensional approach to AI oversight.

Conclusion

This paper presents a novel framework for monitoring and analyzing AI activities within blockchain systems. By integrating AI activity tracking, consensus-aware analysis, and privacy-preserving auditing, the framework ensures transparent, secure, and optimized AI operations. Conceptual evaluation demonstrates its applicability in diverse blockchain-AI environments, including federated learning and IIoT. The research contributes a methodological foundation for unifying AI accountability with blockchain integrity. Future work includes implementation across multiple blockchain platforms, empirical performance validation, and extension to real-time adaptive monitoring.

REFERENCES

1. Baldominos and Y. Saez, "Coin.AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning," *Entropy*, vol. 21, no. 8, 2019, Art. no. 723.
2. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of

- work via proof of stake,” SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec. 2014.
3. F. Bravo-Marquez, S. Reeves, and M. Ugarte, “Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions,” in Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures, 2019, pp. 119–124.
 4. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. 17th Int. Conf. Theory Appl. Cryptograph. Techn., 1998, pp. 127–144.
 5. P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, “A trustworthy privacy preserving framework for machine learning in industrial IOT systems,” IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 6092–6102, Sep. 2020.
 6. S. S. Arumugam, “IoT enabled smart logistics using smart contracts,” in Proc. 8th Int. Conf. Logistics Informat. Service Sci. (LISS), 2018, pp. 1–6.
 7. A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 3–16.
 8. J. Chen, K. Duan, R. Zhang, L. Zeng, and W. Wang, “An AI based super nodes selection algorithm in blockchain networks,” 2018, arXiv:1808.00216.
 9. Chenli, B. Li, Y. Shi, and T. Jung, “Energy-recycling blockchain with proof-of-deep-learning,” in Proc. IEEE Int. Conf. Blockchain Cryptocurrency, 2019, pp. 19–23.
 10. P. Chen, L. Zhiqiang, L. Zhen, and L. Yu, “Research on scalability of blockchain technology: Problems and methods,” Comput. Res. Develop., vol. 55, no. 10, 2018, Art. no. 2099.
 11. J. Curzon, T. A. Kosa, R. Akalu, and K. El-Khatib, “Privacy and artificial intelligence,” IEEE Trans. Artif. Intell., vol. 2, no. 2, pp. 96–108, Apr. 2021.
 12. P. Henderson, R. Islam, P. Bachman, J. Pineau, D. Precup, and D. Meger, “Deep reinforcement learning that matters,” in Proc. 32nd AAAI Conf. Artif. Intell., 2018, pp. 3207–3214.
 13. O. E. Gundersen and S. Kjetsmo, “State of the art: Reproducibility in artificial intelligence,” in Proc. 32nd AAAI Conf. Artif. Intell., vol. 32, no. 1, Feb. 2018, pp. 1644–1651.
 14. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for AI: Review and open research challenges,” IEEE Access, vol. 7, pp. 10127–10149, 2019.
 15. A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in Proc. 37th Annu. Int. Cryptol. Conf., 2017, pp. 357–388.
 16. P. Kumar, G. P. Gupta, and R. Tripathi, “Tp2sf: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning,” J. Syst. Architecture, vol. 115, 2021, Art. no. 101954.
 17. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Blockchain and federated learning for privacy-preserved data sharing in industrial IoT,” IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4177–4186, Jun. 2020.
 18. N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, “Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach,” in Proc. IEEE Int. Conf. Commun., 2018, pp. 1–6.

19. M. I. Mehar, "Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack," *J. Cases Inf. Technol.*, vol. 21, no. 1, pp. 19–32, 2019.
20. M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Performance optimization for blockchain-enabled Industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019.
21. A. Miller and J. J. LaViola, "Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin," 2014.
22. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput.*, 2017, pp. 468–477.
23. A. Ramachandran and M. Kantarcioglu, "SmartProvenance: A distributed, blockchain based dataprovenance system," in *Proc. 8th ACM Conf. Data Appl. Secur. Privacy*, 2018, pp. 35–42.
24. S. Raje, S. Vadera, N. Wilson, and R. Panigrahi, "Decentralised firewall for malware detection," in *Proc. Int. Conf. Adv. Comput. Commun. Control*, 2017, pp. 1–5.
25. C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Proc. 9th Int. Conf. Theory Appl. Cryptograph. Techn.*, 1989, pp. 239–252.
26. J. Li, J. Wu, L. Chen, J. Li, and S. K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Trans. Mobile Comput.*, to be published, doi: 10.1109/TMC.2021.3068717.
27. X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.
28. Y. Zhang, H.-M. Wang, T.-X. Zheng, and Q. Yang, "Energy-efficient transmission design in non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2852–2857, Mar. 2017.
29. H. S. Yin and R. Vatrappu, "A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning," in *Proc. Int. Conf. Adv. Comput. Commun. Control*, 2017, pp. 3690–3699.
30. J. Curzon, T. A. Kosa, R. Akalu, and K. El-Khatib, "Privacy and artificial intelligence," *IEEE Trans. Artif. Intell.*, vol. 2, no. 2, pp. 96–108, Apr. 2021.