A Framework for Cognitive Defense in Blockchain: A Case Study on AI-Based Protection Against Selfish Mining Attacks

| Conference paper | First Online: 26 April 2025

| pp 30–49 | Cite this conference paper

Agents and Artificial Intelligence

(ICAART 2024)

Ali Nikhalat-Jahromi, Ali Mohammad Saghiri & Mohammad Reza Meybodi

Part of the book series: Lecture Notes in Computer Science ((LNAI,volume 15591))

Included in the following conference series:
International Conference on Agents and Artificial Intelligence

Abstract

Blockchain is a revolutionary protocol that enables transactions to be both anonymous and

secure through a tamper-proof public ledger. Despite its significant potential, blockchain faces unresolved security challenges. Blockchain systems are highly dynamic and large-scale. Therefore, many management problems, such as defense mechanisms against a wide range of attacks, cannot be handled by humans because human reaction time is insufficient for many management tasks in blockchain systems. In other words, human reasoning is required in many situations, but we cannot use real humans as managers or system admins. Meanwhile, cognitive systems, designed to mimic human thinking processes through digitalized models, have seen widespread adoption. The core component, the cognitive engine, is responsible for implementing these functionalities. This paper proposes a novel framework that integrates cognitive systems into blockchain to defend against attacks. To our knowledge, no existing framework leverages cognitive systems for blockchain security. We specifically design a reinforcement learning (RL)-based defense mechanism to counter selfish mining attacks based on the cognitive defense framework. Simulation results demonstrate that our proposed cognitive framework significantly enhances blockchain security.

References

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

Google Scholar

2. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: Blockchain challenges and opportunities:

a survey. Int. J. Web Grid Serv. **14**, 352–375 (2018)

Article Google Scholar

3. Ressi, D., Romanello, R., Piazza, C., Rossi, S. AI-enhanced blockchain technology: a review of advancements and opportunities. J. Netw. Comput. Appl. pp. 103858 (2024)

Google Scholar

4. Revolution, B.: How the Technology Behind Bitcoin is Changing Money. Business and The World **324** (2016)

Google Scholar

5. Bennet, D., Maria, L., Sanjaya, Y., Zahra, A.: Blockchain technology: revolutionizing transactions in the digital age. ADI J. Recent Innov. **5**, 192–199 (2024)

Google Scholar

6. Rani, P., Sharma, P., Gupta, I.: Toward a greener future: a survey on sustainable blockchain applications and impact. J. Environ. Manage. **354**, 120273 (2024)

Article Google Scholar

7. Ray, R., Chowdhury, F., Hasan, M.: Blockchain applications in retail cybersecurity: enhancing supply chain integrity, secure transactions, and data protection. J. Business Manage. Stud. **6**, 206–214 (2024)

Article Google Scholar

8. Al-Nbhany, W., Zahary, A., Al-Shargabi, A. Blockchain-IoT healthcare applications and trends: a review. IEEE Access (2024)

Google Scholar

9. Dwivedi, K., Agrawal, A., Bhatia, A., Tiwari, K.: A Novel Classification of Attacks on lockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions. ArXiv Preprint ArXiv:2404.18090. (2024)

10. Santhosh, A., Subramanian, N.: Classify attacks based on blockchain components. In: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–6 (2024)

Google Scholar

11. Guru, A., Mohanta, B., Mohapatra, H., Al-Turjman, F., Altrjman, C., Yadav, A.: A survey on consensus protocols and attacks on blockchain technology. Appl. Sci. **13**, 2604 (2023)

Article Google Scholar

12. Giuliano, A., Hilal, W., Alsadi, N., Gadsden, S., Yawney, J.: A review of cognitive dynamic systems and cognitive IoT. In: 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1-7 (2022)

Google Scholar

13. Srivani, M., Murugappan, A., Mala, T.: Cognitive computing technological trends and future research directions in healthcare - A systematic literature review. Artif. Intell. Med. **138** pp. 102513 (2023). https://www.sciencedirect.com/science/article/pii/S0933365723000271

14. Khasawneh, M., Azab, A., Alrabaee, S., Sakkal, H., Bakhit, H.: Convergence of IoT and cognitive radio networks: a survey of applications, techniques, and challenges. IEEE Access. **11**, 71097–71112 (2023)

Article Google Scholar

15. Lin, R., Li, F., Wang, J., Hu, J., Zhang, Z., Wu, L.: A blockchain-based method to defend against massive SSDF attacks in cognitive Internet of Vehicles. IEEE Transactions On Vehicular Technology. (2023)

Google Scholar

16. Andrew, B., Richard S.S.: Reinforcement Learning: An Introduction. (The MIT Press) (2018)

Google Scholar

17. Shakya, A., Pillai, G., Chakrabarty, S.: Reinforcement learning algorithms: a brief survey. Expert Syst. Appl. **231**, 120495 (2023)

Article Google Scholar

18. Eyal, I., Sirer, E.: Majority is not enough: Bitcoin mining is vulnerable. Commun. ACM **61**, 95–102 (2018)

Article Google Scholar

19. Bai, Q., Xu, Y., Liu, N., Wang, X.: Blockchain mining with multiple selfish miners. IEEE Trans. Inform. Foren. Secur. **18**, 3116–3131 (2023)

Article Google Scholar

20. Bhutta, M., et al.: A survey on blockchain technology: evolution, architecture and security. Ieee Access. **9**, 61048–61073 (2021)

Article Google Scholar

21. Zaghloul, E., Li, T., Mutka, M., Ren, J.: Bitcoin and blockchain: security and privacy. IEEE Internet Things J. **7**, 10288–10313 (2020)

Article Google Scholar

22. Badertscher, C., Maurer, U., Tschudi, D., Zikas, V.: Bitcoin as a transaction ledger: a composable treatment. J. Cryptol. **37**, 18 (2024)

Article MathSciNet Google Scholar

23. Shahsavari, Y., Zhang, K., Talhi, C.: A theoretical model for block propagation analysis in bitcoin network. IEEE Trans. Eng. Manage. **69**, 1459–1476 (2020)

Article Google Scholar

24. Antonopoulos, A., Harding, D.: Mastering bitcoin. ("O'Reilly Media, Inc.",2023)

Google Scholar

25. Garay, J., Kiayias, A., Shen, Y.: Proof-of-work-based consensus in expected-constant time. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 96–125 (2024)

Google Scholar

26. Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016

ACM SIGSAC Conference on Computer And Communications Security, pp. 3–16 (2016)

Google Scholar

27. Porat, A., Pratap, A., Shah, P., Adkar, V.: Blockchain Consensus: An analysis of Proof-of-Work and its applications. (Stanford University: Stanford, CA, USA 2017)

Google Scholar

28. Garay, J., Kiayias, A., Panagiotakos, G.: Proofs of work for blockchain protocols. IACR Cryptol. EPrint Arch. **2017**, 775 (2017)

Google Scholar

29. Sriman, B., Ganesh Kumar, S., Shamili, P.: Blockchain technology: consensus protocol proof of work and proof of stake. In: Intelligent Computing and Applications: Proceedings of ICICA 2019, pp. 395–406 (2021)

Google Scholar

30. Nguyen, C., Hoang, D., Nguyen, D., Niyato, D., Nguyen, H., Dutkiewicz, E.: Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access. **7**, 85727–85745 (2019)

Article Google Scholar

31. Spasovski, J., Eklund, P.: Proof of stake blockchain: performance and scalability for groupware communications. In: Proceedings of the 9th International Conference on Management of Digital EcoSystems, pp. 251–258 (2017)

Google Scholar

32. Wang, T., Liew, S., Zhang, S.: When blockchain meets AI: optimal mining strategy achieved by machine learning. Int. J. Intell. Syst. **36**, 2183–2207 (2021)

Article Google Scholar

33. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and cryptocurrency technologies: a comprehensive introduction. (Princeton University Press,2016)

Google Scholar

34. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: Financial Cryptography And Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22-26, 2016, Revised Selected Papers 20, pp. 515–532 (2017)

Google Scholar

35. Mosakheil, J. Security threats classification in blockchains (2018)

Google Scholar

36. Nicolas, K., Wang, Y., Giakos, G., Wei, B., Shen, H.: Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. IEEE Access. **9**, 3838–3857 (2020)

Article Google Scholar

37. Begum, A., Tareq, A., Sultana, M., Sohel, M., Rahman, T., Sarwar, A.: Blockchain attacks analysis and a model to solve double spending attack. Int. J. Mach. Learn. Comput. **10**, 352–357 (2020)

Google Scholar

38. Chen, Y., Chen, H., Han, M., Liu, B., Chen, Q., Ren, T.: A novel computing power allocation algorithm for blockchain system in multiple mining pools under withholding attack. IEEE Access. **8**, 155630–155644 (2020)

Article Google Scholar

39. Li, W., Cao, M., Wang, Y., Tang, C., Lin, F.: Mining pool game model and nash equilibrium analysis for pow-based blockchain networks. IEEE Access. **8**, 101049–101060 (2020)

Article Google Scholar

40. Aggarwal, S., Kumar, N.: Attacks on blockchain. Adv. Comput. **121**, 399–410 (2021)

Google Scholar

41. Prashar, D.: Others Analysis on blockchain vulnerabilities and attacks on wallet. In: 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), pp. 1515–1521 (2021)

Google Scholar

42. Singh, S., Hosen, A., Yoon, B.: Blockchain security attacks, challenges, and solutions for the future distributed Iot network. Ieee Access. **9**, 13938–13959 (2021)

Article Google Scholar

43. Dai, Q., Zhang, B., Dong, S.: A DDoS-attack detection method oriented to the blockchain network layer. Secur. Commun. Netw. **2022**, 5692820 (2022)

Article Google Scholar

44. Sayeed, S., Marco-Gisbert, H., Caira, T.: Smart contract: attacks and protections. IEEE Access **8**, 24416–24427 (2020)

Article Google Scholar

45. Bhardwaj, A., Shah, S., Shankar, A., Alazab, M., Kumar, M., Gadekallu, T.: Penetration testing framework for smart contract blockchain. Peer-to-Peer Netw. Appl. **14**, 2635–2650 (2021)

Article Google Scholar

46. Hou, C., et al.: SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. *ArXiv Preprint* ArXiv:1912.01798. (2019)

47. Bar-Zur, R., Abu-Hanna, A., Eyal, I., Tamar, A.: WeRLman: to tackle whale (transactions), go deep (RL). In: Proceedings of the 15th ACM International Conference on Systems and Storage, pp. 148–148 (2022)

Google Scholar

48. Bar-Zur, R., Dori, D., Vardi, S., Eyal, I., Tamar, A.: Deep bribe: predicting the rise of bribery in blockchain mining with deep RL. In: 2023 IEEE Security And Privacy Workshops (SPW), pp. 29–37 (2023)

Google Scholar

49. Vernon, D. Artificial cognitive systems: A primer. (MIT Press,2014)

Google Scholar

50. De Brigard, F.: Cognitive systems and the changing brain. Philos. Explor. **20**, 224–241 (2017)

Article Google Scholar

51. Barfuss, W.: Dynamical systems as a level of cognitive analysis of multi-agent learning: Algorithmic foundations of temporal-difference learning dynamics. Neural Comput. Appl. **34**, 1653–1671 (2022)

Article Google Scholar

52. Mnih, V., et al.: Human-level control through deep reinforcement learning. Nature **518**, 529–533 (2015)

Google Scholar

53. Silver, D., et al.: Mastering the game of Go with deep neural networks and tree search. Nature **529**, 484–489 (2016)

Google Scholar

54. Ghalavand, M., Hatami, J., Setarehdan, S., Nosrati, F., Ghalavand, H., Nikhalat-Jahromi, A.: Comparison of the Effects of Interaction with Intentional Agent and Artificial Intelligence using fNIRS. ArXiv Preprint ArXiv:2402.17650. (2024)

55. Dellermann, D., Ebel, P., Söllner, M., Leimeister, J.: Hybrid intelligence. Bus. Inform. Syst. Eng. **61**, 637–643 (2019)

Article Google Scholar

56. Vahdati, M., Gholizadeh HamlAbadi, K., Saghiri, A.: IoT-Based healthcare monitoring using blockchain. In: Applications of Blockchain in Healthcare, pp. 141–170 (2021)

Google Scholar

57. Topol, E.: High-performance medicine: the convergence of human and artificial intelligence. Nat. Med. **25**, 44–56 (2019)

Article Google Scholar

58. Saghiri, A., Vahdati, M., Gholizadeh, K., Meybodi, M., Dehghan, M., Rashidi, H.: A framework for cognitive Internet of Things based on blockchain. In: 2018 4th International Conference on Web Research (ICWR), pp. 138–143 (2018)

Google Scholar

59. Watkins, C., Dayan, P.: Q-learning. Mach. Learn. **8**, 279–292 (1992)

Article Google Scholar

60. Clifton, J., Laber, E.: Q-learning: theory and applications. Ann. Rev. Stat. Appl. **7**, 279–301 (2020)

Article MathSciNet Google Scholar

61. Thomas, R., Friend, D., DaSilva, L., MacKenzie, A.: Cognitive networks: adaptation and learning to achieve end-to-end performance objectives. IEEE Commun. Mag. **44**, 51–57 (2006)

Article Google Scholar

62. Khan, A., Rehmani, M., Rachedi, A.: Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. IEEE Wirel. Commun. **24**, 17–25 (2017)

Article Google Scholar

63. Arslan, H., Mitola, J.: Cognitive radio, software defined radio, and adaptive wireless systems. (Springer 2007)

Google Scholar

64. Nikhalat-Jahromi, A., Saghiri, A., Meybodi, M.: Q-Defense: when q-learning comes to help proof-of-work against the selfish mining attack. In: Proceedings of the 16th International Conference on Agents and Artificial Intelligence, ICAART 2024, Volume 1, Rome, Italy, February 24-26, 2024, pp. 37–46 (2024). https://doi.org/10.5220/0012378600003636

65. Zhao, W., et al.: A survey of large language models. ArXiv Preprint ArXiv:2303.18223. (2023)

66. Zhao, H., et al.: Explainability for large language models: a survey. ACM Trans. Intell. Syst. Technol. **15**, 1–38 (2024)

Google Scholar

67. Schaeffer, R., Miranda, B., Koyejo, S.: Are emergent abilities of large language models a mirage?. In: Advances In Neural Information Processing Systems, vol. 36 (2024)

Google Scholar

Author information

Authors and Affiliations

Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran
Ali Nikhalat-Jahromi, Ali Mohammad Saghiri & Mohammad Reza Meybodi

Corresponding author

Correspondence to Ali Nikhalat-Jahromi .

Editor information

Editors and Affiliations

LIACC, University of Porto, Porto, Portugal
Ana Paula Rocha

Barcelona Supercomputing Center, Barcelona, Spain
Luc Steels

Leiden University, Leiden, The Netherlands
Jaap van den Herik

Rights and permissions

Copyright information

About this paper

Cite this paper

Nikhalat-Jahromi, A., Saghiri, A.M., Meybodi, M.R. (2025). A Framework for Cognitive Defense in Blockchain: A Case Study on AI-Based Protection Against Selfish Mining Attacks. In: Rocha, A.P., Steels, L., van den Herik, J. (eds) Agents and Artificial Intelligence. ICAART 2024. Lecture Notes in Computer Science(), vol 15591. Springer, Cham. https://doi.org/10.1007/978-3-031-87327-0_2

.RIS .ENW .BIB

DOI
https://doi.org/10.1007/978-3-031-87327-0_2

Published
26 April 2025

Publisher Name
Springer, Cham

Print ISBN
978-3-031-87326-3

Online ISBN
978-3-031-87327-0

eBook Packages
Computer Science
Computer Science (R0)

Publish with us

Policies and ethics