IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain

Rohan Kumar C L[1], Ali Mohammed Zain[2], Sanjay Kumar H P[3], Prajwal A V[4], Dr. Sudarshan R[5]
Students, Department of Information Science and Engineering[1,2,3,4]
Professor & Head, Department of Information Science and Engineering[5]
Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

Abstract: *Fraudulent transactions have a huge impact on the economy and trust of a block chain network. Consensus algorithms like proof of work or proof of stake can verify the validity of the transaction but not the nature of the users involved in the transactions or those who verify the transactions. This makes a block chain network still vulnerable to fraudulent activities. One of the ways to eliminate fraud is by using machine learning techniques. Machine learning can be of supervised or unsupervised nature. In this paper, we use various supervised machine learning techniques to check for fraudulent and legitimate transactions. We also provide an extensive comparative study of various supervised machine learning techniques.*

Keywords: Fraud, Comparative Study, Blockchain, Machine learning.

REFERENCES

[1]. Cai, Y., Zhu, D. Fraud detections for online businesses: a perspective from blockchain technology. Financ Innov 2, 20 (2016).
[2]. Hyv¨arinen, H., Risius, M. & Friis, G. A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. Bus Inf Syst Eng 59, 441–456 (2017). https://doi.org/10.1007/s12599-017- 0502- 4
[3]. Xu, J.J. Are blockchains immune to all malicious attacks? Finance Innov 2, 25 (2016). https://doi.org/10.1186/s40854-016-0046-5
[4]. Ostapowicz M., ˙ Zbikowski K. (2019) Detecting Fraudulent Accounts on Blockchain: A Supervised Approach. In: Cheng R., Mamoulis N., Sun Y., Huang X. (eds) Web Information Systems Engineering – WISE 2019. WISE 2020. Lecture Notes in Computer Science, vol 11881. Springer, Cham. https://doi.org/10.1007/978-3-030-34223-4 2
[5]. Podgorelec, B., Turkanovi´c, M. and Karakati˘c, S., 2020. A Machine Learning-Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection. Sensors, 20(1), p.147.
[6]. Farrugia S, Ellul J, Azzopardi G. Detection of illicit accounts over the Ethereum blockchain. Expert Systems with Applications. 2020 Jul 15;150:113318.
[7]. Pham, Thai, and Steven Lee. "Anomaly detection in bitcoin network using unsupervised learning methods." arXiv preprint arXiv:1611.03941 (2016).
[8]. Monamo, Patrick, Vukosi Marivate, and Bheki Twala. "Unsupervised learning for robust Bitcoin fraud detection." 2016 Information Security for South Africa (ISSA). IEEE, 2016.