Paper ID: MISS21_94

A Survey on Unsupervised Machine Learning Approach for Fraud Detection in Bitcoin

Amit Kumar Mandal[1*], Prosenjit Dinda[2]

[1]Bengal Institute of Technology, No. 1 Govt. Colony, Basanti Road, Kolkata-700150

[2]Saroj Mohan Institute of Technology, Guptipara, Hooghly, Pin-712512

*Corresponding author

Abstract

Background: The Global market size of cryptocurrency is huge now a days and may hit $4.94 billion by 2030[1]. Since its inception, the first ever cryptocurrency, Bitcoin has been the leader in terms of market capitalization. Decentralized cryptocurrency like Bitcoin faces major challenges like anonymity and privacy, cybersecurity, fraud transactions etc. at the time of global trading [2]. Bitcoin, the leader of cryptocurrency market has emerged as a soft target of money laundering or illicit activities. For anomaly or fraud detection, unsupervised techniques [3][4] are based on clustering algorithms. Objectives: To protect the trustworthiness and stability of cryptocurrencies, fraud detection i.e. identifying the suspicious behavior in the transaction network is very much important. Machine Learning techniques may be the ideal for fraud or scam detection of cryptocurrencies like hacking, phishing, money laundering, ponzi-scheme and many such more. Methodology: Unsupervised Support Vector Machine (SVM), K-Means Clustering, Kd-trees, Mahala Nobis Distance Based Method, Gaussian Mixture Model (GMM) and other methods have been used on the available sample of Bitcoin dataset for potential fraud detection. Based on global and local outliers, an unsupervised or semi-supervised way have been followed to find illicit activity in the cryptocurrency transaction network [5]. Results and discussion: These algorithms generate clusters of non-negative matrix where the small ones treated as fishy [6]. Various estimation of illicit activities comes out from the application of different methods on cryptocurrency ecosystem. For estimation of fraudant activities, the identification of addresses with anomalous transaction patterns is important [6].

Conclusions and future work: As of October 2021, more than 6000[7] different cryptocurrencies in the market which also includes some very newest one. So, deal with the various types of security threats are becoming the greatest challenges for this global market. There exists huge scope of research work to tackling the security and privacy issues of other cryptocurrencies.

References

[1] "Cryptocurrency Market Will More Than Triple by 2030: Study" Available: https://www.nasdaq.com /articles/cryptocurrency-market-will-more-than-triple-by-2030%3A-study-2021-08-25

[2] F. Sabry, W. Labda, A. Erbad, Q. Malluhi, "Cryptocurrencies and Artificial Intelligence: Challenges & Opportunities," *Digital Object Identifier 10.1109/ACCESS.2020.3025211, Volume 8, 2020, pp. 3, 11*

[3] P. Monamo, V. Marivate, B. Twala, "Unsupervised Learning for Robust Bitcoint Fraud Detection,"*Conference: Information Security for South Africa (ISSA), 2016*

[4] T. T. Pham, S. Lee, "Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods," *arXiv:1611.03941*

[5] P. M. Monamo, V. Marivate, B. Twala, "A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers," *15th IEEE International Conference on Machine Learning and Applications*

[6] X. Fan Liu, X-J Jiang, S-H Liu, C. Kong Tse, "Knowledge Discovery in Cryptocurrency Transaction: A Survey," *Digital Object Identifier 10.1109/ACCESS.2021.3062652, Volume 9, 2021, pp. 18-19*

[7] "Number of Cryptocurrencies Worldwide from 2013 to October 2021" Available: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

DOI: 10.21467/abstracts.120

ISBN: 978-81-954993-2-8