Exploring Energy Flow Classifier to Identify Fraudulent Cryptocurrency Transactions

Kevin S. Araujo[1], **Rodrigo Bonifacio de Almeida**[1], **Fabiano Cavalcanti Fernandes**[2]

[1]Departamento de Ciências da Computação – Universidade de Brasília (UnB) – Campus Universitário Darcy Ribeiro, Brasília-DF

[2]Instituto Federal de Brasília (IFB) – Taguating, DF – Brazil

kevin.araujo@aluno.unb.br, rbonifacio@unb.br, fabiano.fernandes@ifb.edu.br

Abstract. *This is a work in progress.*

1. Introduction

In 2008, a global financial crisis in the real estate sector occurred [Bordo 2008], which was caused by the State providing easy credit [Murphy 2008]. A cryptographic document began circulating on a mailing list for cryptographers, signed by the pseudonymous Satoshi Nakamoto, which compiled detailed data and discoveries made through cypherpunk innovations. Nakamoto utilized this knowledge to create an electronic transaction system that did not require the involvement of a third-party moderator. In essence, Nakamoto's work involved using math, programming, and cutting-edge cryptography to publish a map for removing governmental presence from financial transactions. The recent collapse of the economy had demonstrated that governments cannot be trusted, and Nakamoto's solution was to create a currency that was mathematically impossible to be corrupted — Bitcoin [Nakamoto 2008]. Although Bitcoin does present a solution to the corruptible nature of money, it does possess flaws and is target of more sophisticated frauds.

Detecting such sophisticated frauds requires advanced analytical techniques. Identifying anomalous patterns within complex data streams, such as network traffic or financial transactions, remains a critical challenge. Traditional methods often struggle with the high dimensionality, evolving nature, and sheer volume of modern data. In the domain of Network Intrusion Detection (NID), flow-based analysis offers a valuable abstraction by aggregating packet-level information into connection summaries, reducing data complexity while retaining essential behavioral characteristics. Within this context, a promising approach grounded in principles from statistical physics is the Energy-based Flow Classifier (EFC). Originally proposed using the Inverse Potts model, EFC characterizes the probability distribution of normal network flows through an energy function derived from observed data patterns [Pontes et al. 2019]. Configurations representing typical, legitimate flows are assigned low energy values by the model, whereas anomalous or potentially malicious flows, deviating from the learned normality, manifest as high-energy states. Subsequent research has further explored the capabilities of this energy-based framework, highlighting its potential for open-set recognition the challenging task of identifying novel anomalies not encountered during the model's training phase [Souza et al. 2022]. The fundamental principle of assigning an energy score as a measure of typicality provides a robust and theoretically grounded mechanism for distinguishing normal system behavior from potentially illicit activities.

While Bitcoin was designed to circumvent traditional financial system vulnerabilities [Nakamoto 2008], it is not immune to manipulation and anomalous activities, necessitating robust detection mechanisms [Zhang et al. 2020, Zainal et al. 2018]. Addressing this challenge within the Bitcoin ecosystem, this paper investigates the application of the Energy-based Flow Classifier (EFC), a technique adept at identifying deviations from established norms in complex data [Pontes et al. 2019, Souza et al. 2022]. Leveraging its foundation in statistical physics, EFC quantifies the typicality of data points through an energy score, whereby normal, expected transaction patterns correspond to low energy states, and significant deviations—potentially indicative of fraud or manipulation—manifest as high-energy anomalies. The central objective of this work is, therefore, to explore the efficacy of EFC in identifying such anomalous operations within a real-world Bitcoin transaction dataset, assessing its potential as a tool for enhancing the security and integrity of cryptocurrency exchanges.

Referências

Bordo, M. D. (2008). An historical perspective on the crisis of 2007-2008. Technical report, National Bureau of Economic Research.

Murphy, A. (2008). An analysis of the financial crisis of 2008: causes and solutions. *An Analysis of the Financial Crisis of*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`.

Pontes, C. F. T., Gondim, J. J. C., Bishop, M., and Marotta, M. A. (2019). A new method for flow-based network intrusion detection using inverse statistical physics. *CoRR*, abs/1910.07266.

Souza, M. M. C., Pontes, C., Gondim, J., Garcia, L. P. F., DaSilva, L., and Marotta, M. A. (2022). A novel open set energy-based flow classifier for network intrusion detection.

Zainal, A., Kamruzzaman, J., and Sarker, R. A. (2018). A review on machine learning techniques for the detection of financial statement fraud. *International Journal of Financial Studies*, 6(3):70.

Zhang, X., Wen, Y., Zhou, J., Zhang, W., and Liao, X. (2020). Financial fraud detection in cryptocurrency exchanges: A comprehensive survey. *IEEE Access*, 8:193150–193172.