# Representation Learning on Graphs at Scale for Anomaly Detection, with Blockchains as a case study

Marya Bazzi, Giovanni Colavizza, Mihai Cucuringu, Xiaowen Dong, Lucas Jeub

Graph neural networks and representation learning on networks have gained in popularity due to their ability to perform well on a variety of tasks on non-Euclidean graph data. Among the significant open challenges in this area of research is the question of scalability both during training and inference. We contributed to this line of work, in collaboration with GCHQ, by proposing a decentralized divide-and-conquer approach (*local2global*) to improve the scalability of network embedding techniques [7, 8][1].

We propose to build on our recent work on both application and methodological fronts. On an application front, our main area of interest is to build on our anomaly detection work (see Section 5 in [8]) and to explore new timely applications in emerging technologies, such as using *local2global* to detect anomalies in graphs constructed from Non-Fungible Token (NFT) data. We note that while our pimary case study will be NFT networks, which will serve as a proof-of-concept, the methods we will develop will be more broadly applicable and we will consider other application areas (e.g., internet connectivity networks), as the project develops. We also note that the work on emerging technologies may have fruitful synergies with the Turing's recent launch of the Centre for Emerging Technology and Security[2] (CETaS). On a methodological front, we noted in our earlier work that the complexity of *local2global* with the embedding dimension can be improved. This is particularly desirable in large-scale graphs with heterogeneous structure and in classification downstream tasks where the number of classes is large (e.g., section 4.5.2 in [8]) or more generally where feature engineering for the classification problem at hand is challenging. In this follow-up work, we plan to significantly improve how well *local2global* scales with the embedding dimension by introducing a methodological extension to our existing pipeline. We give further detail on these points below.

**Anomaly detection in NFT transaction networks.** The increasing popularity of blockchains offers a compelling opportunity for applying *local2global*, given the complete availability of semi-anonymous transaction data. Non-Fungible Tokens (NFTs) are certificates of authenticity of an asset, registered and exchanged on smart-contract blockchains, such as Ethereum [6]. NFTs have been primarily used to trade or exchange collectibles [10]. NFT transaction networks suffer from significant obstacles to their reliable and secure use. On the one hand, detecting suspicious activities on highly volatile and large-scale markets of non-fungible assets is inherently challenging and requires one to deal with multi-modal data. On the other hand, the lack of regulation makes the space ripe for fraud and other illicit behaviour, such as wash trading or copyright infringement. We propose to apply *local2global* on large-scale NFT transaction networks collected from openly available sources[3]. The use of machine learning for forecasting and detecting anomalies on blockchain networks is an open and timely area of research [1].

Security vulnerabilities in NFT networks are widespread and remain strikingly underexplored [4]. Given the complexity of NFT networks, where smart contracts interact with distributed file systems and marketplaces, several security vulnerabilities exist. These can be distinguished as vulnerabilities related to marketplaces ('server-side'), users ('client-side'), and external entities (can be either) [4]. Examples of server-side vulnerabilities include: rug pulls, tampering and fakes, insider trading. Examples of client-side vulnerabilities include: wash trading, money laundering, sanction evasion. We focus this proposal on rug pull and wash trading detection due to their potential for wide reaching impact. Furthermore, they belong to two dominant tasks related to blockchain transaction networks: **address classification and clustering**.

[1] Associated code available at: https://github.com/LJeub/Local2Global and https://github.com/LJeub/Local2Global_embedding

[2] https://cetas.turing.ac.uk/

[3] E.g., https://opensea.io.

**Rug pulls.** are a common issue in NFT projects, where the developers get investors to buy in large quantities of tokens through marketing promotions and then flee with the money under the pretext of abandoning the project. Rug pulls are similar to 'pumps-and-dumps', yet they constitute an exclusive server-side vulnerability since they are driven by malicious developers/owners of a project. An estimated 50% of tokens listed on Uniswap, a major cryptocurrency exchange, are suspected to be fraudulent in a related way [15]. The detection of rug pulls is a new area of applied work. Methods have been proposed which use heuristics in combination with feature engineering and machine learning [15, 9] yet, to the best of our knowledge, graph embedding techniques have never been explored for this task.

We therefore propose to cast **rug pull detection as an address classification problem**. Given a transactions graph, we propose to explore appropriate embedding techniques to represent the topology of the graph and relevant node attributes. Our design is extensible since, via node attributes, auxiliary information can also inform the task. Secondly, we propose to use data from known cases of rug pulls, to train and test a neural classifier for predicting addresses in a situation of high risk to a rug pull. There are several known cases of rug pulls: *BabyBoomersNFT*, *NFYe*, *LuckyBuddhaLuckyClub*, *PsychoTeddyNFT*, *My8Bit*, *SimpMermaids*, *CashCows*, and more.

**Wash trading.** is a known phenomenon in financial markets referring to the repeated trading of assets for the purpose of misleading the market, for example to inflate an asset's valuation [14]. Detecting wash trading is hard since the task can only be performed as the timely flagging of suspicious activity. In NFT networks, the techniques for wash trading detection proposed so far are mostly based on heuristics such as detecting cyclic and frequent transactions across the same few addresses. As a consequence of heuristic-based approaches and the intrinsic difficulty of the task, estimates of the impact of wash trades in NFT networks vary widely: from just 2% [14], to about 30% [13] to over 70% [3] of transacted volumes.

The presence of wash trades on a transaction graph can be estimated via statistical tests such as adherence to Benford's law or the presence of herding behaviour based on the Pareto—Levy test [12]. The detection of patterns in the graph has also been proposed and investigated. For example, Cao et al. [2] illustrate wash trade patterns in ring, star, tree, and mesh topologies and detect the patterns using digraphs and dynamic programming. More recently, wash trading algorithms have been proposed to find strongly connected components (SCC) or weakly connected components (WCC) in the transaction graph to detect closed cycles. Transactions involved in such cycles can be flagged as possible wash trades [4]. On top of cycles, path-like transaction patterns and high-speed transactions can also be signals of suspicious activities as adversaries could avoid closed cycles to escape detection [14, 11].

We propose to cast **wash trading detection as an address clustering problem**. An initial proposed approach can be described as follows: first, appropriate graph embedding methods are selected, taking into account the importance of the local topology of the graph, as well as any relevant node attributes. Second, the graph topology and embeddings are used to perform a clustering of addresses. Third, we consider the temporal paths of traded NFTs through the embedded graph topology. One can then try to flag potential wash trades by combining the signal of graph clusters and frequent trades (e.g., by identifying any NFTs which are frequently traded within clusters). As part of our analysis, we will investigate different ways of incorporating temporal information (e.g., clustering and embedding techniques in time-dependent graphs), which is key in the study of wash trades. A comparison with leading published methods will also be provided.

Rug pulls and wash trades constitute two key vulnerabilities in NFT/blockchain transaction networks. Since they can be cast as instances of the general problems of address classification and clustering, successful methods promise to have a broader applicability in detecting vulnerabilities in NFT/blockchain transaction networks. Two further challenges emerge with such networks: (1) the need to consider, at once, the topology of the graph and the attributes of the nodes; and (2) the need to deal with large, sometimes massive graph scales. Our *local2global* approach is designed to cater to both of these challenges.

**Project objectives: This project will not only advance the state-of-the-art on the pressing challenge of detecting vulnerabilities in NFT transaction networks, but also explore further questions and objectives. Firstly, we will investigate which embedding techniques are most suitable to represent addresses in blockchain transaction networks. Secondly, we will create high-quality reusable datasets for testing our proposed approach. There are several sources of NFT transaction data which can be used for this purpose, including OpenSea and Uniswap. Lastly, as previously mentioned, while our pimary case study will be NFT networks, which will serve as a proof-of-concept, the methods we will develop will be more broadly applicable**

**and we will consider other application areas (e.g., internet connectivity networks), as the project develops. Visualization techniques that are effective on large-scale networks will also be considered throughout the project.**

**Improved scalability of *local2global*** Throughout the project we will make use of our *local2global* methodology to be able to compute embeddings at scale (e.g., to use them as features in classification tasks). **A methodological improvement to *local2global* that we propose to undertake in this project is to improve its complexity as one increases the embedding dimension. This is relevant in a wide-range of applications, e.g., those that involve large-scale graphs with heterogeneous structure or instances where feature engineering for the classification problem at hand is challenging (e.g., section 4.5.2 in [8]).**

The over-arching idea for *local2global* is as follows. One first divides the input graph into overlapping subgraphs (or "*patches*") and trains local representations for each patch independently. In a second step, one combines the local representations into a globally consistent representation by estimating the set of rigid motions that best align the local representations using information from the patch overlaps, via group synchronization. A key distinguishing feature of *local2global* relative to existing work is that patches are trained independently without the need for the often costly parameter synchronization during distributed training. The resulting benefits of our decentralized approach are fourfold: • (1) it is highly parallelisable as each patch is trained independently; • (2) it can be used in privacy-preserving applications and federated learning setups, where frequent communication between devices is often a limiting factor [5], or "decentralized" organizations, where one needs to simultaneously consider data sets from different departments; • (3) it can reflect varying structure across a graph through asynchronous parameter learning; and • (4) it is a generic approach that, in contrast to most existing approaches, can be applied to a large variety of embedding techniques.

Our proposed modification lies in the way the transformations are obtained for each patch. Namely, for each patch $P_i$, we have a linear transformation consisting of scaling $s_i$, orthogonal transformation $R_i$, and shift $t_i$. Rather than training transformations by solving an eigenvalue problem to minimize the Procrustes error (the complexity of this step heavily depends on the embedding dimension), we propose to train transformations for each patch by optimising an objective function directly. A first sensible option to try would be a least-squares objective, such as:

$$\min_{s,R,t} \sum_{n\in V} \sum_{P_i\in P} \sum_{P_j\in P} ||s_i X_n^{(i)} R_i + t_i - (s_j X_n^{(j)} R_j + t_j)|| 1_{n\in P_i} 1_{n\in P_j} \tag{1}$$

with some regularisation on scales (e.g., $||\log s||_1$ to prevent exploding scales), and transformations (e.g., $\sum_{P_i\in P} ||R_i R_i^T - I||$ to encourage transformations to remain close to orthogonal) to keep the optimisation problem well-behaved. Here $X_n^{(i)}$ denotes the locally-trained embedding of node $n$ for patch $P_i$. One can then use standard mini-batch Stochastic Gradient Descent based methods to train the transformations. Furthermore, for semi-supervised downstream objectives, we can incorporate label information during training of the transformations by using mean-pooling over the transformed embeddings for each node.

# References


[1] Madhuparna Bhowmik, Tulasi Sai Siri Chandana, and Bhawana Rudra. Comparative study of machine learning algorithms for fraud detection in blockchain. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, pages 539–541, 2021.

[2] Yi Cao, Yuhua Li, Sonya Coleman, Ammar Belatreche, and Thomas Martin McGinnity. Detecting Wash Trade in Financial Market Using Digraphs and Dynamic Programming. *IEEE Transactions on Neural Networks and Learning Systems*, 27(11):2351–2363, November 2016.

[3] Lin Cong, Xi Li, Ke Tang, and Yang Yang. Crypto Wash Trading. *SSRN Electronic Journal*, 2019.

[4] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. Understanding Security Issues in the NFT Ecosystem, April 2022. arXiv:2111.08893 [cs].

[5] P. Kairouz *et al.* Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1), 2021.

[6] Massimo Franceschet, Giovanni Colavizza, T'ai Smith, Blake Finucane, Martin Lukas Ostachowski, Sergio Scalet, Jonathan Perkins, James Morgan, and Sebastián Hernández. Crypto Art: A Decentralized View. *Leonardo*, 54(4):402–405, August 2021.

[7] Lucas G. S. Jeub, Giovanni Colavizza, Xiaowen Dong, Marya Bazzi, and Mihai Cucuringu. Local2global: Scaling global representation learning on graphs via local training. In *KDD 2021 workshop on Deep Learning on Graphs*, DLG-KDD'21, 2021.

[8] Lucas G. S. Jeub, Giovanni Colavizza, Xiaowen Dong, Marya Bazzi, and Mihai Cucuringu. Local2global: A distributed approach for scaling representation learning on graphs. *arXiv:2201.04729*, 2022.

[9] Bruno Mazorra, Victor Adan, and Vanesa Daza. Do Not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection. *Mathematics*, 10(6):949, March 2022.

[10] Matthieu Nadini, Laura Alessandretti, Flavio Di Giacinto, Mauro Martino, Luca Maria Aiello, and Andrea Baronchelli. Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, 11(1):20902, December 2021.

[11] Sven Serneels. Detecting wash trading for nonfungible tokens. *Finance Research Letters*, page 103374, September 2022.

[12] Syed Ahzam Tariq and Imtiaz Sifat. Suspicious Trading in Nonfungible Tokens (Nfts): Evidence from Wash Trading. *SSRN Electronic Journal*, 2022.

[13] Friedhelm Victor and Andrea Marie Weintraud. Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. In *Proceedings of the Web Conference 2021*, pages 23–32, Ljubljana Slovenia, April 2021. ACM.

[14] Victor von Wachter, Johannes Rude Jensen, Ferdinand Regner, and Omri Ross. NFT Wash Trading: Quantifying Suspicious Behaviour in NFT markets. *SSRN Electronic Journal*, 2021.

[15] Pengcheng Xia, Haoyu Wang, Bingyu Gao, Weihang Su, Zhou Yu, Xiapu Luo, Chao Zhang, Xusheng Xiao, and Guoai Xu. Trade or Trick?: Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 5(3):1–26, December 2021.