# CX4242 Project Progress Report: Fraud Detection in NFT Marketplace

Philip Kang
pkang@gatech.edu

Andrew Li
lia@gatech.edu

Yunsong Liu
el@gatech.edu

Jason Marfey
jmarfey3@gatech.edu

Eric Qiu
eqiu7@gatech.edu

Mingxiao Song
msong@gatech.edu

## 1 Introduction

With the popularization of cryptocurrencies, market manipulation has become more prevalent. Our objective is to identify suspicious market manipulation specifically in the NFT (non-fungible token) marketplace through graph-based analysis and interactive visualization.

With the decentralized nature of blockchain, it's impossible to regulate suspicious behaviors and thus important to create tools that can deliver transparent and liquid pre-trade and post-trade information to investors, supporting identification of unnecessary risks while creating a compelling case for improved security scrutiny.

## 2 Problem Definition

The problem to be solved is the lack of reachable services for NFT amateurs to validate prices and identify fraudulent prone NFT collections and users. Our solution, employing pattern-searching algorithms, graph statistical inferences and interactive visualizations that clearly highlight potential fraudulence is a completely novel functionality as there is currently no software that apply similar approaches for the NFT market.

## 3 Survey

For background knowledge, we survey literature that summarized the background history of NFT. Ante [1] and Dowling [2] overview the development of the NFT market, ethereum blockchain and cryptocurrencies, supplemented by Cornelius's [3] discussion about NFT fraud traceability and identification and Putnins' [4] description of market manipulation, which all reach a consensus that NFT market manipulation is a serious problem worth detection and attention. Specifically, Imisiker et al. [5] and Kaihua et al. [6] detect security risks in blockchain washing trading activities and blockchain extractable value, proving again that suspicious manipulation behaviors are prevailing. The severity of such problems inspire us to design reachable services that can help investors assess risk with quantitative measures and interactive interfaces, such as how Nadini et al. [7] visually analyzes NFT market revolutions and trading networks.

We then survey more academic papers with practical fraud detection methods in traditional financial markets. Xu et. al [8] outlines a metrics-based detection method for pump and dump schemes, but fails to capture instances of more secretive fraud. Monamo et. al [9] summarizes the use of unsupervised learning in Bitcoin fraud detection, opening the possibility of using machine learning for NFT trading data analysis. Chen et. al [10] identifies abnormal bitcoin exchange structures with leaked transaction history, which matches our goal of discovering irregular behaviors through trade networks. Wu et. al [11] presents a literature review on understanding the cryptocurrency transaction networks and divides crypto-related network techniques into three major parts, providing us a framework for building a network graph. Similarly, Camino et. al [12] and Zhai et. al [13] present methods to analyze cryptocurrency transactions using unsupervised learning with real-world case studies and a hybrid ML model combining SVM and HMM that detects disruptive market activities, providing us an additional approach to detect suspicious behaviors. Finally, Ross Phillips and Heidi Wilder use clustering algorithms to categorize crypto-related online scams and analyze blockchain campaigns structures, which motivates us to use graph and cluster based approaches to identify fraud.

These literature analyses seem promising, but matured fraud detection models in the NFT market are deficient. Many methods proposed in the following surveys lack implementation or experiments in real world scenarios and are mostly scientific research findings that cannot be utilized as reachable services. Chen et. al [15] and Zhang et. al [16] present learning algorithms in a data-driven approach that show and justify evidence for stock price manipulation, which is useful as foundational knowledge for a ML approach, but with limitations in scope, as stock markets do not necessarily correspond to NFT markets. Golmohammadi et. al

[17] and Kumar et. al [18] also utilizes machine learning for stock market trend prediction, which concrete our understanding of trends in financial markets and abnormal behaviors in financial trading and transactions, given the close relation between stock market and cryptocurrency markets.

# 4 Proposed Method

The novelty of the NFT generates challenges for finding authoritative references, but it also creates endless possibilities for innovations. Our design supports innovations from three domains: *combination of token-centric and user-centric datasets, usage of graph pattern recognition together with statistical inferences for improved fraud detection accuracy, and interactive force-directed diagrams serving as representative explanations of our finding*. We introduce these innovations in detail in the following subsections.

## 4.1 Data Collection & Preprocessing

An NFT is a digital art piece stored on a blockchain created in collections with a specific contract address, nested with individual NFT items with token ids ranging from 1 to 10000. Each user account in the marketplace has unique wallet address and may sell or transfer tokens.

Our datasets come entirely from Moralis.io, an API that allows us to retrieve real time data from OpenSea. Calling the API recursively with JavaScript, we collect the transaction history for each of 50 most popular NFT collections on OpenSea. With each collection having at least 50,000 transaction records, we collect a total of 2,680,043 transaction records and have cross validated with real online data.

To identify both suspicious token and account in our algorithm and visualization, we combine transactions of all 50 collections and transformed them into token-centric and user-centric data structures. Token-centric data structure is a dictionary that allows us to get a list of transactions related to a specific token given a token as key. User-Centric data structure is a dictionary that contains transactions given a wallet address as key. In each dictionary, the following information is available: token id, target id (the hashed wallet address of the other party), timestamp, and value.

## 4.2 Fraud Detection Algorithms

The best way to recover the liquidity, depth and volatility of the NFT market is through graph representations and analyses [19]. Our NFT trading graph is represented as G = (V,E,w), where V is a set of nodes representing sellers and buyers wallet addresses, E is a set of edges representing transactions between nodes (including transfers, sales and documented sales from other platforms) and w is the weight represented by number of transactions.

Motivations behind market manipulation involve market making (inflating item price), rate making (increasing popularity), and incentivizing (getting trading rewards) [20]. Accordingly, we define three key properties for fraudulent behaviors: *grouped, circular and frequently repetitive*. Specifically, a group of accounts that repeatedly transact low amount internally might have an abnormal market manipulation tendency; cyclic transactions can also be identified as suspicious transfer between its sub accounts. Given these assumptions, we propose graph pattern recognition algorithms, price/time-controlled DFS and maximum clique enumeration, and graph statistical inference belief propagation algorithm.

**Price/Time-controlled DFS** is an innovative algorithm we propose for circle detection in NFT trading graphs. In our user-centric dataset, the transaction history of all tokens start with user address 0x0 when it is minted. We start the DFS algorithm from here and expand along the trading record of each NFT token. Whenever a node reappears in the search we mark a new subcycle. With a list of basic sets of cycles, we XOR these patterns to obtain all cycles. We then filter the list base on indexes we defined after analyzing typical fraudulent trading patterns and mark most anomalous tradings as those with shorter cycles, smaller trading intervals and higher value deviations.

**Maximum Clique Enumeration**, the Bron-Kerbosch algorithm, employs a recursive backtracking method to find maximal cliques, representing anomaly grouped behaviors in undirected graphs [22]. Given three disjoint sets R, P and X, with R representing growing cliques, P standing for prospective nodes (neighbors of nodes already in the clique), and X containing nodes already processed, the algorithm extracts nodes from set P, adds to set R, and terminates when both set P and X are empty. Further efficiency can be gained with pivoting. To make the algorithm more suitable for our purpose, we only consider a clique with size greater than two.

**Belief Propagation Graph Algorithm** can identify possible fraudulent structures in NFT trading graphs, such as cliques of fraudulent users, or complex operations of fraudsters and accomplices, which can simplify the classification of users as either honest or fraudulent participants in the market. The algorithm initially assigns each node an equal weight (probability) of being either a fraudster or an honest trader, and then a propagation matrix is used to send beliefs between neighboring nodes about the state of their neighbor.

For example, a fraudulent user will interact more with other fraudulent users, so neighbors of a node with high fraudulent weight will have their fraudulent weight increased accordingly. After some iterations, the algorithm converges to some state, where each user has some honesty “score”.

These three methods are innovative approaches that haven’t been used in any NFT networking analyses. The patterns will be visualized to support intuitive understanding and the honesty score can be used to indirectly predict the risky "score" of a NFT token or collection.

## 4.3 Visualization Interface

To create a simple, interactive and understandable software service, the main innovation is that the results of our algorithm are intuitive and explainable as we display supportive evidence to the users, such as the price changes due to abnormal price manipulation and circular trading loops in transaction networks, making them an active part in the fraud detection process. Also, our design is highly interactive aiming to provide the most relevant information related to the suspicious user or NFT item the user is interested in.

From the entry interface, the user can select collection and NFT IDs through a drop-down menu to see visualization for specific NFT tokens. The software generates a line graph of the price of the NFT with nodes representing buyers and sellers and line intervals connecting them representing transactions, serving as surface-level information for investors to filter through. Unusual prices are highlighted compared with the average price of the NFT shown as a horizontal line. Data obtained through the algorithms is also displayed - notably, it visually marks users with a low "honesty score" within the NFT’s transaction history and their potential influences with the price trend. When hovering over a transaction edge, detailed information such as buyer/seller user address, timestamp and value will be displayed. When hovering over a user node, the "honesty score" of the user will be shown with the user’s activeness trading this NFT collection. Initially, our trading network, a force-directed diagram, is centered by the last buyer of the NFT and selecting a particular node on the line graph will make it centered by the selected node with its transaction history in all NFT collections. The graph propagates down by layers of users until it involves enough observable complication. Abnormal patterns, such as cycles and cliques, recognized by the algorithms, will be highlighted with weights and colors. Whenever the user clicks on a user account on the force-directed graph, it will be recentered at the new account.

Combination of these two visualizations exposes a degree of NFT fraud on the market in ways that are clearly observed. We used and will use D3 together with web development tools to implement these visualizations.

# 5 Experiments & Evaluation

## 5.1 Data Analysis

Two most prevalent fraud behaviors in the NFT market, wash trading and pump and dump, typically feature repetitive transfer between two accounts to gain platform reward or fake a trading volume increase. Therefore, in order to select the most representative dataset for analyses, we locate most suspicious collections/tokens by checking whether their number of historical transfers is larger than usual, indicating the existence of frequent repetitive transfers. Fig 1(a) shows the average number of transactions per token of 10 most popular collections, with mean appearing to be consistently around 4 and below 7. This can be explained by the fact that the field of NFT is still at its early stage and the fact that most NFT holders hold for long terms. From Fig 1(b), we can see that a small number of tokens in Meebits Collection exhibit a number of transactions significantly higher than the average. By checking the transaction history of 10 of these tokens, we found that 9 of these tokens exhibit frequent transfers between the same set of accounts. Thus, we came to conclusion that a token’s number of historical transaction is a good indicator of fraudulent behavior, inspiring us to choose the most active NFT collections for analyses.

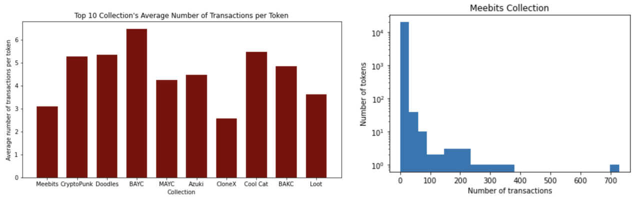


***Figure 1: (a) Avg Transactions per Token (b) Meebits NFT Collection Number of Transaction Distribution***

## 5.2 Visualization

We have done visualization experiments on three scales: Fig 2 shows a whole NFT collection trading graph, Fig 3(a) focuses one NFT token, and Fig 3(b) for transaction records based on user expansion. Visualization based on NFT collections will be too complicated and messy, whereas visualizing one NFT token will be too trivial and not informative. Therefore, given the results of the experiment, we choose to use force-directed diagrams that are user centered and expanded by layers of user accounts that can best represent the anomalous patterns we detect and get rid of irrelevant information.

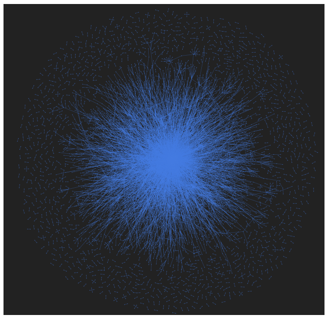


*Figure 2: Transaction Histories Among Top 10,000 Active User Pairs From Doodles NFT Collection.*

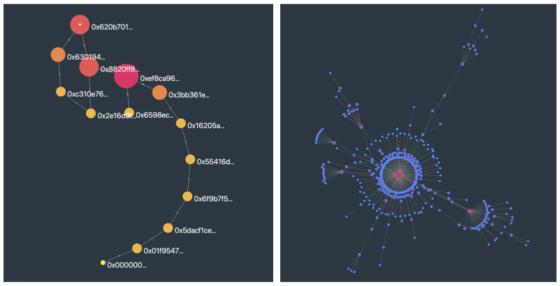


*Figure 3: (a) Token Doodle #8965 Transactions (b) User Centric Doodles NFT Collection*

## 5.3 Pattern Recognition

We get Fig 4(a) running the DFS circle detection algorithm with NFT token Doodle 9582, with a counterexample Fig 4(b) showing a normal transaction graph without cycle. The algorithm successfully detected four loops within the transaction flow which are highlighted in red, proving that our proposed method is correct and such circular patterns do exist in the NFT marketspace. This is when we will implement price and time indicators to filter cycles that are most suspicious. For further evaluation, this token is labeled as suspicious on OpenSea, proving the effectiveness of our proposal.

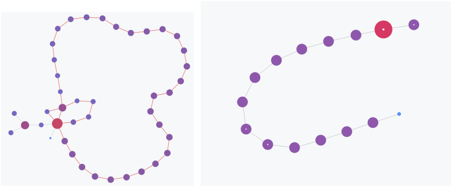


*Figure 4: (a) Doodle #9582 Force-directed Diagram (b) Doodle #303 Force-directed Diagram*

## 5.4 More Experiments & Evaluation

We plan to do the following experiments while constructing the final product. 1) We will do more data analyses to find the most characteristic fraudulent behaviors by visualizing risk-prone trading network and looking into the transaction histories manually. For example, we will prove the credibility an indicator, the number of transactions of a NFT token divided by number of interactors, as a promising factor for fraudulent level in more NFT collections. 2) We will test our algorithms with a larger portion of our dataset. For example, we have already tested the DFS algorithm on 10 NFT collections and found reliable results and will test its efficiency with all the collections we have. Also with the belief propagation algorithm, we have tested it with our synthetic dataset, but will need to do more experiments with real dataset. 3) Finally, we plan to improve our visualization design especially when we expand our experimental dataset. There might be problems with, for example, the number of layers of users displayed in the force-directed graph because more data entries may lead to increased complexity and unclarity. We also plan to add more innovative informative visual designs to show the risk ranking of multiple NFT collections or the distributions of the new indexes we propose among multiple NFT collections.

The elusive nature of anomalous behavior makes it hard for us to validate our prediction result, so we propose three ways to make evaluations. 1) We use multi-scope analyses, using graph pattern recognition and honest scoring methods, which will serve as cross validation for the correctness of our findings. 2) We will generate synthetic data that contains predefined anomalous behaviors and check if our algorithms can detect them. 3) Finally, we will inject fraudulent data into real datasets, dynamically mimic real world scenarios. These evaluation methods will provide concrete evidence of the performance of our proposed method.

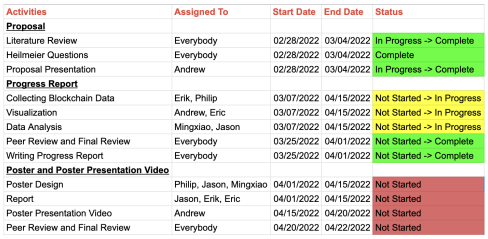
# 6 Conclusions & Discussion

The NFT market is indeed risky for suspicious market manipulation, thus important to provide investors risk assessment services to prevent obtrusive investments.

The innovative methods we proposed offer more intuitive and interactive results compared with existing research and the interactive nature of our visualization also makes our software reachable and user-friendly.

# 7 Plan of Activities

All team members contribute similar amounts of effort.



| Activities | Assigned To | Start Date | End Date | Status |
|---|---|---|---|---|
| **Proposal** | | | | |
| Literature Review | Everybody | 02/28/2022 | 03/04/2022 | In Progress -> Complete |
| Heilmeier Questions | Everybody | 02/28/2022 | 03/04/2022 | Complete |
| Proposal Presentation | Andrew | 02/28/2022 | 03/04/2022 | In Progress -> Complete |
| **Progress Report** | | | | |
| Collecting Blockchain Data | Erik, Philip | 03/07/2022 | 04/15/2022 | Not Started -> In Progress |
| Visualization | Andrew, Eric | 03/07/2022 | 04/15/2022 | Not Started -> In Progress |
| Data Analysis | Mingxiao, Jason | 03/07/2022 | 04/15/2022 | Not Started -> In Progress |
| Peer Review and Final Review | Everybody | 03/25/2022 | 04/01/2022 | Not Started -> Complete |
| Writing Progress Report | Everybody | 03/25/2022 | 04/01/2022 | Not Started -> Complete |
| **Poster and Poster Presentation Video** | | | | |
| Poster Design | Philip, Jason, Mingxiao | 04/01/2022 | 04/15/2022 | Not Started |
| Report | Jason, Erik, Eric | 04/01/2022 | 04/15/2022 | Not Started |
| Poster Presentation Video | Andrew | 04/15/2022 | 04/20/2022 | Not Started |
| Peer Review and Final Review | Everybody | 04/20/2022 | 04/22/2022 | Not Started |

*Figure 5: The New/Current Plan of Activities.*

# References

[1] Ante, Lennart. (August 13, 2021). Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration, and interrelations. https://papers.ssrn.com/sol3/papers.cfm?abstract$_{i}d =$ 3904683.

[2] Dowling, M. (April 29, 2021). Is non-fungible token pricing driven by cryptocurrencies? Elsevier Finance Research Letters, 44. https://doi.org/10.1016/j.frl.2021.102097.

[3] Cornelius, Kristin. (August 31, 2021). Betraying Blockchain: Accountability, Transparency, and Document Standards for Non-Fungible Tokens (NFTs). Information 2021, 21, 358-375. https://doi.org/10.3390/info12090358.

[4] Putnins, Talis J., An Overview of Market Manipulation (October 1, 2018). Forthcoming in: Handbook of Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation. https://ssrn.com/abstract=339825.

[5] Serkan Imisiker, Bedri Kamil Onur Tas. (September 10, 2018). Wash Trades as a Stock Market Manipulation Tool. Journal of Behavioral and Experimental Finance, Elsevier, Volume 20.

[6] Kaihua Qin, Liyi Zhou, and Arthur Gervais. (Dec 10, 2021). Quantifying Blockchain Extractable Value: How dark is the forest? https://arxiv.org/abs/2101.05511.

[7] Matthieu Nadini, Laura Alessandretti , Flavio DiGiacinto, Mauro Martino, Luca MariaAiello and Andrea Baronchelli. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. https://www.nature.com/articles/s41598-021-00053-8.pdf.

[8] Jiahua Xu, Benjamin Livshits. (August 14, 2019). The Anatomy of a Cryptocurrency Pump-and-Dump Scheme. https://www.usenix.org/system/files/sec19-xu-jiahua$_0.pdf$.

[9] Patrick Monamo, Vukosi Marivate, Bheki Twala. (2016). Unsupervised Learning for Robust Bitcoin Fraud Detection. https://digifors.cs.up.ac.za/issa/2016/Proceedings/Full/paper

[10] Weili Chen, Jun Wu, Zibin Zheng, Chuan Chen, and Yuren Zhou. (Jan 19, 2019). Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network. https://arxiv.org/pdf/1902.01941.pdf.

[11] Wu, J., Liu, J., Zhao, Y., Zheng, Z. (August 7, 2021). Analysis of cryptocurrency transactions from a network perspective: An overview. https://arxiv.org/abs/2011.09318.

[12] R. D. Camino, R. State, L. Montero and P. Valtchev, Finding Suspicious Activities in Financial Transactions and Distributed Ledgers. 2017 IEEE International Conference on Data Mining Workshops (ICDMW), 2017, pp. 787-796, doi: 10.1109/ICDMW.2017.109.

[13] Zhai, J., Cao, Y., Yao, Y., Ding, X., Li, Y. (September 23, 2016). Computational intelligent hybrid model for detecting disruptive trading activity. Decision Support Systems. https://www.sciencedirect.com/science/article/pii/S016792361630152X?via

[14] Ross Phillips and Heidi Wilder. (2020). Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. https://arxiv.org/pdf/2005.14440.pdf.

[15] Chen, W., Wu, J., Zheng, Z., Chen, C., Zhou, Y. (April 29, 2019). Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network. IEEE Conference on Computer Communications, 2019, 964-972. https://doi.org/10.1109/INFOCOM.2019.8737364.

[16] Zhang, J., Wang, S., Xu, S., Yu, M. (March 3, 2017). Stock Price Manipulation Detection Based on Machine Learning Technology: Evidence in China. Geo-Spatial Knowledge and Intelligence, 2016, 150-158. https://doi.org/10.1007/978-981-10-3966-9$_1$6.

[17] Golmohammadi, K., Zaiane, O., Díaz, D. (October 3, 2014). Detecting stock market manipulation using supervised learning algorithms. International Conference on Data Science and Advanced Analytics (DSAA), 2014, 435-441. https://doi.org/10.1109/DSAA.2014.7058109.

[18] Kumar, I., Dogra, K., Utreja, C., Yadav, P. (April 20, 2018). A Comparative Study of Supervised Machine Learning Algorithms for Stock Market Trend Prediction. Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, 1003-1007, https://doi.org/10.1109/ICICCT.2018.8473214.

[19] Federico Musciotto, Jyrki Piilo, and Rosario N. Mantegna. (June 25, 2021). High-frequency Trading and Networked Markets. https://www.pnas.org/doi/10.1073/pnas.2015573118.

[20] Mayukh Mukhopadhyay and Kaushik Ghosh. (Oct 8, 2021). Market Microstructure of Non Fungible Tokens. https://arxiv.org/pdf/2112.03172.pdf.

[21] Using Bron Kerbosch Algorithm to find maximal cliques. https://iq.opengenus.org/bron-kerbosch-algorithm/.