Dec 12th, 12:00 AM

Non-fungible Tokens - Exploring Suspicious Washtrader Communities in NFT Networks

Nargess Tahmasbi
Penn State University, nargess.tahmasbi@gmail.com

Alexander Fuchsberger
Bucknell University, afuchsberger@unomaha.edu

Non-fungible Tokens - Exploring Suspicious Washtrader Communities in NFT Networks

Completed Research

Nargess Tahmasbi
Pennsylvania State University
nvt5061@psu.edu

Alexander Fuchsberger
Bucknell University
a.fuchsberger@bucknell.edu

Abstract

Non-fungible Tokens (NFTs) have received increased attention since 2021. NFTs can be susceptible to fraudulent activities such as washtrading or trading of counterfeit digital assets. Such behaviors threaten the trust in this new trading space and for this reason, NFT skeptics are suspicious of the true values of highly priced digital assets. In this paper, we propose a two-step methodological approach to identify washtraded assets, and the suspicious communities of washtraders. Our approach uses bipartite graph characteristics to provide an efficient algorithm that does not require computationally intensive methods. We also identify the challenges in this stream of research and propose suggestions to address those challenges. Our method demonstrates practical applicability on real life networks of NFT transactions and opens doors for several future directions for investigating and exploring the communities of suspicious washtrading actors.

Keywords: Non-fungible Tokens, NFT, washtrading, graph techniques, bipartite graph

Introduction

Non-fungible tokens (NFTs) are unique digital assets that reside on the Blockchain technology. An NFT can take many forms ranging from digital arts to event tickets, to any digitally tokenized form of physical asset. The exchange and trading of digital assets are executed by smart contracts through which the ownership of the asset is represented. NFTs have received increased attention in recent years. NFT transactions totaled $150,000 in dollar volume in 2017, $5.3 million in 2019, and $12 billion in 2021 (White et al. 2022). Most notable events occurred in early 2021 that made NFT a topic of media outlets. Examples include Christie's sale of "the first 5000 Days" (Damiani 2021), Jack Dorsey's Tweet (Howcroft 2021), and the earliest NFT projects that became popular in 2017: CryptoKitties and CryptoPunks. In May 2021, nine assets in CryptoPunks collection sold for $16.9 million in Christie's (Franceschet 2021). Most of these events pertain to a specific form of NFT as known as crypto art. NFT skeptics are suspicious of the true values of such highly-priced digital assets.

Similar to more traditional marketplaces such as eBay or auction markets, where fraudulent activities such as shill bidding threaten the trust of traders, NFTs can be susceptible to fraudulent activities such as washtrading or trading of counterfeit digital assets. Washtrading in traditional markets happens when a buyer and a seller exchange the same asset back and forth to artificially drive up the price. In the NFT market, actors sell the asset back and forth to different wallets potentially owned by the same person or a colluding group of people to distort the price of NFTs and create false demand. Preventing and identifying washtrading behavior in NFT is important because the prevalence of this behavior can harm the market adoption. Among other factors such as unfamiliarity with the new technology, trust seems to be the most important factor in the adoption of NFTs and that can be threatened by the prevalence of fraudulent behaviors. A few attempts have investigated identifying such incidents by exploring the network of traders to look for cycled

trade patterns. Graph cycle identification methods used in previous studies are computationally intensive and do not sound practical especially in large trading networks.

Moreover, the evaluation of the effectiveness and accuracy of the existing methods is challenged by the lack of annotated data due to regulatory issues concerning privacy and the emergence of this new space. Suggestions to tackle this challenge have been proposed in research pertaining to online auction houses, but this challenge is yet to be explored in the new space of NFT.

In this paper, we propose a two-step methodological approach to identify washtraded assets, and the suspicious communities of wash traders. While we do not claim 100% accuracy of identification, we aim to provide a base for more cautious and rigid monitoring of suspicious actors in the NFT market. Our method demonstrates practical applicability on real life networks of NFT transactions and opens doors for several future directions for investigating and exploring the communities of suspicious washtrading actors.

The rest of this paper is structured as follows. We provide an overview of the NFT and the works done to combat the fraudulent behaviors in the stock market, online auctions, cryptocurrency, and finally NFT space. Then, we propose our two-step methodology for finding suspicious NFTs and suspicious actors. We provide a discussion of our result and discuss the efficiency of our method and its implications for future research.

Background

NFTs Explained

Physical assets can be tokenized. The tokens can then be stored on the digital ledgers technology (DLT). Tokenization enables management of unique digital assets and ownership. A Non-fungible Tokens (NFT) is a unique unit of data, called a digital asset, that is stored on a blockchain. Its digital certificate of ownership is offered through smart contracts of Ethereum (Wang et al. 2021).

NFTs and cryptocurrencies are similar as they are both considered digital tokens. However, cryptocurrencies such as Bitcoin are fungible tokens. It means that a Bitcoin can simply be exchanged for another Bitcoin as two Bitcoins have the same value at any moment. Similarly, a dollar bill is considered fungible as it can be exchanged for another dollar bill and is divisible as well. NFTs on the other hand are non-fungible. This means that each NFT is unique, and the token is not interchangeable or divisible (Regner et al. 2019).

The non-fungibility of NFTs and asset organization has opened new doors to a variety of use-cases including but not limited to digital art galleries and marketplaces (Whitaker 2019), digital trading card games (Murray 2021), and event tickets (Regner et al. 2019). One of the most dominant use cases of NFT is crypto art. Crypto art is a rare digital art asset that is tokenized and unique. Marketplaces such as OpenSea, Rarible, SuperRare, and Mintable provide exchange environment for art collectors and artists to buy and sell crypto art.

NFT Pricing

Studies have focused on understanding of NFT pricing mechanisms and drivers for value. For example, Dowling (2022b) investigated the co-movement of the cryptocurrency market and NFT market to understand how NFT prices are driven by cryptocurrency prices. They did an analysis on three popular NFT projects in different contexts including virtual worlds (Decentraland), crypto art (CryptoPunks), and gaming (Axi Infinity). They concluded that the low volatility of NFT prices makes them uncorrelated and detached from cryptocurrency market (Dowling 2022b). In another study, Dowling 2022a researched the pricing behavior of Decentraland project and found that although the pricing models are inefficient due to the market being in its early stage, the data shows a rapid rise in value.

The pricing mechanism in NFTs has inspired research to investigate whether the introduction of NFTs has any impact on the prices of their physical counterparts. Kanellopoulos et al. 2021 found out that introduction of sports trading cards through NFT has caused the price of physical trading cards collectibles on eBay drop

by 5%.

NFT pricing is a complex mechanism. Research in this area is scarce due to the novelty of this technology. One could expect that similar to a traditional artwork, the quality of the crypto art asset be a driver for its value. Yet, many NFTs in collections like CryptoPunks share similar characteristics with slight differentiation and yet sell for prices with significant differences. Studies claim that the media can play an important role in the value of NFTs mainly by creating the fear of missing out (White et al. 2022). The media outlets are capable of fueling hype by reporting the high trading volumes, which in turn creates a feedback loop by spiking participation interest. Yet not much negativity appears to be present in the media coverage of NFTs. A sentiment analysis by (White et al. 2022) shows that only 9% of the NFT related media news convey negative sentiment (White et al. 2022).

This feedback loop however can be a double-sided sword: Users with malicious intentions can orchestrate a chain of fictitious transactions in an attempt to inflate the trade volume and consequently the price of particular assets; a malpractice that is called "*washtrading*" in NFT space.

Fraudulent Activities in Online Markets

Washtrading is not unique to the NFT space. Similar fraudulent behaviors can be observed in online and traditional auction houses.

Shill Bidding in Auctions

Trevathan and Read (2007) have done extensive research on shill bidding. Shill biding is a similar behavior to washtrading but the former occurs in traditional or online auction houses where traders bid on items. The purchase is only made after a bidder wins, thus the goal of a shill bidder is to not win, but to make multiple higher bids to spike bidding interest (Trevathan and Read 2007). In their later works, Trevathan and Read (2021) target the colluding shill bidders. In this type of shill bidding, the seller has friends bid in her auctions, or controls multiple fake bidder accounts that are used for the sole purpose of shill bidding. This way, the shill bidders distribute the risk of being detected to multiple accounts (Trevathan and Read 2021). They proposed calculating a shill bidding score to be made visible by other bidders. This score not only detects shill bidders but also has a deterrent effect: other bidders can make an informed decision about bidding on a particular item (Trevathan and Read 2021).

Studies on shill bidding detection are more mature than that of washtrading detection in the NFT space as the latter is still in its early stage of adoption. Although bidding and pricing process on traditional marketplaces is different than that of decentralized NFT market, they share some similarities. Consequently, the detection methods used in traditional studies may inspire new approaches to combat the fraudulent activities in the new market.

The majority of studies pertaining to the traditional and online auction markets use mathematical and machine learning techniques to identify the fraudulent actors. These methods mostly compete for accuracy aiming at minimizing suspicious activities. Some of those use graphical models like Markov Random Field and anomaly detection techniques such as Local Outlier Factor (LOF) for better accuracy (Majadi et al. 2019).

Adabi et al. (2022) use a genetic algorithm and aim to focus on increasing the accuracy of shill bidding detec-tion while maximizing trading opportunities (Adabi et al. 2022). Fire et al. (2022) uses a supervised machine learning algorithm on a big e-commerce data set that was already labeled. They argue that shill bidders form cliques to support each other and use this characteristic to increase the accuracy of their algorithm (Fire et al. 2022).

One of the big challenges in this area that impacts the practicality of the proposed solutions is that not all approaches can aim at detecting the real-time shill bidding incidents. For example, Tsang et al. (2014) could manage to achieve a high detection accuracy, however, it lacks the ability to detect shill bidding in running auctions (Tsang et al. 2014). There are studies that could claim to detect the incidents in running auctions. One of them is a study by Abidi et al. (2021) that uses support vector machine (SVM) and artificial neural network (ANN) to tackle the real time detection problem (Abidi et al. 2021).

Washtrading in Stock Markets, Cryptocurrency, and NFT

The detection of fraudulent activities has also been a concern in the stock and cryptocurrency markets. Studies adapt machine learning algorithms, mostly supervised, to combat the issue (Golmohammadi et al. 2014). Some of the studies in this context take a higher level look at the market as a whole to study the prevalence of washtrading in the market. For example, Eigelshoven et al. (2021) investigated the type of manipulations that exist in these markets and the vulnerabilities that facilitate such manipulations. They found out that after Pump & Dump, washtrading is the second most common topic appeared in their collection of literature dataset. Cong et al. (2021) performed power-law fitting on the cryptocurrency transaction graph and argue that the power-law pattern implies the existence of a small influential community of traders that have the power to manipulate the market. It appears that apart from the overall market studies and machine learning approaches for more fine-grained detection of fraudulent cases, stock and cryptocurrency market studies also adopted the graph methods, an approach that has not been widely adopted by studies pertaining to shill bidding context. One of the first few attempts was made by Cao et al. (2014) who identified four network topologies: ring, star, tree, and mesh in the real market data of four stocks. Then Victor and Weintraud 2021 used graph methods to find cyclical transaction patterns to identify washtrading in cryptocurrency market (Victor and Weintraud 2021).

In the NFT space, actors can participate in different forms of transactions, sale, transfer, or bid. The bidding is similar to the existing bidding form that occurs in auction houses. But what affects the trading volume in NFT space is only successful sales. Thus, NFT washtraders can perform similar behavior to shill biding in auctions to spike participation, but that participation should be in the form of successful sales in a hope to increase the price of a digital asset. An effective way to inflate the price of assets is to perform a series of successful sales transactions, each at a higher price than the previous one, to increase the trading volume. This can also increase interest in the asset from potential buyers. The term washtrading commonly pertains to the NFT space as apposed to shill biding that is more commonly used in the auction context.

There are works in progress that investigate the shill bidding behavior in NFT space (Mukhopadhyay and Ghosh 2021). However, research on identification of washtrading in NFT is scarce. NFTs are different than cryptocurrency market in multiple ways. NFTs are scarce: the supply of each NFT is limited to 1. Moreover, NFT market involves secondary market royalties that go to the original creator. A gas fee is charged for minting an NFT. This cost is variable due to factors such as the time of transaction and the underlying Blockchain in which the NFT resides. In some exchanges users can have only one active wallet, although it can not be technically prevented. These characteristics make NFT space unique and different from other trading spaces. Consequently, the motivation for washtrading in NFT can also be unique. Some buyers just buy NFTs for the purpose of collecting them and showcasing them on their social media platform and not necessarily for financial reasons. Reasons that motivates washtrading in NFT could be market making, rate making, and project promotion (Mukhopadhyay and Ghosh 2021). All NFT transactions are traceable and publicly available, which means that the data collection in this space is more convenient although the lack of annotated data is still an issue. But that means the methods involving washtrading identification could benefit from the availability of the data to use graph methods for finding cyclical patterns of transactions. Wachter et al. (2021) finds that cyclical patterns are conducted at relatively rapid intervals. Their paper focuses less on the methods of finding the cyclical patterns but more on the metrics on prevalence of wash trading in their data set. They do not provide an evaluation of their method, which is actually a challenge in this type of research because of the lack of a baseline and a source of truth to compare the results with.

Another circumstance in this area of research is the lack of labeled data set that challenges the evaluation of the effectiveness and accuracy of the existing methods. Due to to regulatory issues in some traditional and online markets and concerns related to bidders' privacy, an annotated dataset is not easily accessible for research purposes. This issue is less sever in the context of traditional markets. Studies in those contexts could use data from market manipulation case studies (Golmohammadi et al. 2014) and annotated dataset from big e-commerce websites (Fire et al. 2022). Some other studies in the literature have provided suggestions to tackle this issue by synthesizing artificial manipulation cases by shill biding agents (Majadi et al. 2019; Mukhopadhyay and Ghosh 2021; Trevathan and Read 2007). The above challenges are yet to be addressed in the NFT space. In such contexts, where the absence of real market washtrading cases introduces a challenge, studies suggest that it is acceptable to the financial industry business to reproduce and synthe-

size artificial manipulation cases. Such synthetic exploratory financial data are also accepted in academic research for evaluation of the proposed algorithms (Cao et al. 2014)

In the following, we explain our methodology for data collection and washtrading identification both at the assets level and at the collectors level. Then we discuss our results and propose a method for the evaluation of our method.

Methodology

Data Collection

We collected the data using the OpenSea public API. The OpenSea API provides various endpoints for retrieving data regarding various aspects of the NFT transactions including events, collections, and assets. There are multiple event types in OpenSea: *created* for new auctions, *successful* for sales, *canceled* for cancelled auctions, *bid entered*, *bid withdrawn*, *transfer*, *offer entered*, and *approve*. We used Python scripts to collect all *success* events that occurred in the CryptoPunks collection. We also collected the data about all CryptoPunks assets. We were specifically interested in the data from this collections, because the CryptoPunks collections is one of the earliest NFT projects with some known washtrading incidents that were mentioned in the news. And more importantly, in designing our identification method, we tried to rule out other factors such as the characteristics of the NFT asset itself. CryptoPunks was one of the few collections that satisfied this requirement. It includes 10,000 assets that are algorithmically generated, have very similar characteristics, and yet sell for different prices, sometimes with a large gap. The collected data from this collection includes token id, image URL, last sale date if applicable, assets traits, and the smart contract address. The event object includes data about the asset being transferred/sold, the date when the event was recorded, the accounts associated with the event, the payment information including the payment token (ETH, WETH or DAI), quantity, and total price (including any royalties). Figure 1 shows an example of a CryptoPunks asset as displayed on the OpenSea platform.

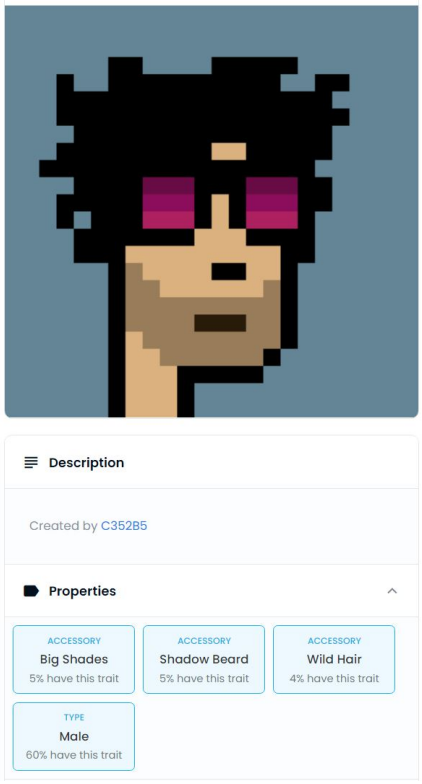

Figure 1. CryptoPunk #9766 and its traits. Source: opensea.io

In total, we collected all the 10,000 assets that exist in CryptoPunks collection along with 10,050 successful sales as of October 2021.

Modeling the Bipartite Transaction Graph

We constructed a network of all sales and transfer transactions among the collectors of CryptoPunks assets. We recognize two types of transactions in our data set: sales and transfer. A sales transaction involves an *asset* being sold by *collector1* to *collector2* for a specific amount of ETH. A transfer transaction involves a transfer of an asset from *collector1* to *collector2* with no monetary exchange. We model the transaction graph *G(V, E)* as a bipartite graph where *V(G)* is a set of all the assets and the collectors, and *E(G)* represents all the transactions involving a collector and an asset. A sales/transfer transaction of *asset1* from *collector1* to *collector2* will generate a directed edge from *collector1* to *assets1* and a directed edge from *asset1* to *collector2*.

Building a graph in the bipartite mode helps us design an algorithm to detect cycles involving the same asset in an efficient way without the need to use algorithms such as depth-first search to find the closed cycles in a graph. In the following, we explain our proposed algorithm that takes advantage of the bipartite property of this graph to identify the assets that were involved in a closed transaction cycle.

Step 1. Identifying Suspicious Assets and Collectors

In the first step of our methodlogy, we focus on identifying the suspicious assets and find the actors involved with the suspicious washtraded asset in order to narrow our focus down on a smaller set of collectors for further monitoring in future.

Washtrading can take many forms. A majority of them involves a single asset being sold back to one of the previous owners after a chain of transactions. Mukhopadhyay and Ghosh (2021) identify nine different motifs for washtrading (Mukhopadhyay and Ghosh 2021). The simple type of washtrading in their categorization of the motifs are included in Table 1.

Motif Name	**Motif Description**
Washtrading 101	*collector1* sells *asset1* to *collector2*, *collector1* shortly buys it back.
First seller buys it back	*collector1* sells *asset1* to *collector2*; *collector2* transfers it for free to *collector3*; *collector1* buys it from *collector3*.
First buyer buys it back	*collector1* sells *asset1* to *collector2*; *collector2* transfers it for free to *collector3*; *collector2* buys it from *collector3*.
Best selling creator	*collector1* sells *asset1* to *collector2*; *collector2* transfers it for free back to *collector1*; *collector1* sells it to a third wallet *collector3*.
The tornado	*collector1* sells *asset1* to *collector2*; asset1 is sold between different collectors (wallets), and is finally bought back by *collector1* after several sales.

Table 1. Simple washtrading motifs (Mukhopadhyay and Ghosh 2021).

We declare an asset to be suspicious if it has been involved in a closed cycle of sales and transfer transactions. With this definition, we aim to cover the simple washtrading types according to the categories defined in (Mukhopadhyay and Ghosh 2021).

We argue that if an asset is not involved in a cycled chain of transactions, in a bipartite sub-graph containing n nodes (*n - 1* collectors and one asset), each collector would have maximum of two transactions involving the asset except for the first seller and the last buyer, where the number of transactions they are involved must

be one, otherwise there would be a closed cycle. Thus, the sum of degrees (both indegree and outdegree) of the asset in the sub-graph must not exceed $1 + 1 + 2 * (n - 3)$, which equals $2 * (n - 2)$.

With that being said, we devised an algorithm to go through all the assets in this collection, and for each asset examine the degree to see whether it exceeds the "safe" value calculated above. The suspicious assets are then labeled as potentially suspicious if their degree in the sub-graph exceeds the "safe" value.

Figure 2 shows a sub-graph containing the CryptoPunks #9998 and the collectors that were part of a transaction involving this asset. This incident of potential washtrading was noticed by media outlets soon after its occurrence [1]. In this scenario, *collector1* (with an Ethereum address beginning with 0xef76) transferred the CryptoPunk #9998 (the red node) to *collector2* (with address starting with 0x8e39). Later, *collector2* sold the NFT to *collector3* (with an address starting with 0x9b5a) for 124457 ETH. Finally, the asset was transferred back to *collector1* (with the address 0xef67). Notice that the collectors may not necessarily be different real individuals and they may be separate wallets associated with an individual. This resembles the "First seller buys it back" motif.

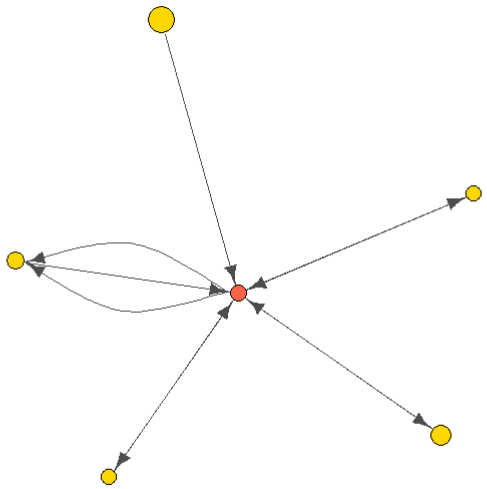

Figure 2. An example of a bipartite graph: The sub-graph involving CryptoPunks #9998 (the red node) and the collectors (the yellow nodes) involved in transactions.

We define a suspicious score as the frequency at which a collector is involved in a transaction with a suspicious asset identified using the above method. The more frequent a collector appears in such transactions, the more likely the collector is a washtrader. Note that the bipartite graph does not specify which collectors were involved in the washtrading cycle. Thus, in the second step, we increment the suspicious score of all the collector nodes in the sub-graph involving a suspicious asset. Algorithm 1 shows the steps of our procedure for identifying the suspicious assets and collectors. The actual code of the algorithm is implemented in R Software (R Core Team 2021).

Analysis of the algorithm complexity

The above algorithm goes through each asset ($m = 10{,}000$) and in case it is suspicious for washtrading, it goes through all the transactions involving this asset. If the total number of transactions is considered as the

[1] https://beincrypto.com/cryptopunk-9998-sold-532m-not-really/

Algorithm 1 Identifying suspicious scores for assets and collectors

```
1: procedure findsuspicious(V(g))                          ▷ calculates suspicious scores
2:     suspiciousScores ← 0
3:     for asset in V(g) do
4:         V(subgraph) ← V(g) [where asset in (e.source, e.target)]
5:         if degree(asset) > 2 * (length(unique(V(subgraph))) − 2) then
6:             incrementSuspiciousScore(asset)
7:             for collector in neighbours(asset) do
8:                 incrementSuspiciousScore(collector)
9:             end for
10:        end if
11:    end for
12: end procedure
```

problem size (*n*), then in the worse case (where all assets are suspicious), visits each transaction once. Thus the time complexity of this algorithm will be *O(n)*, where *n* is the number of transactions. Hence we can argue that the algorithm falls in the category of fast performing algorithms with the linear time complexity. Regarding the space complexity, the algorithm makes a copy of a sub-graph in each loop, which is a portion of the entire graph. Thus in the worse case, the space complexity is *O(n)*, which is again a linear space complexity.

Step 2. Digging Deeper into the Suspicious Collectors' Community

In the second step of our methodology, we aim to refine the suspicious score of collectors based on their connections with other suspicious collectors in order to reach a higher accuracy.

Washtraders stick together and form separate communities in which they have more frequent transactions with each other than with other actors in other communities. We argue that if we construct the collector transactions graph, then the graph should show signs of modularity where each module represents a community of orchestrated washtraders. Of course not all the nodes in the community are necessarily washtraders, but this can give us an insight on who to have an eye on when monitoring the NFT space for suspicious activities. We used the modulairty function in Gephi to calculate the graph modulairty considering the edge weight (the frequency of transactions between two nodes).

Hence, we started with modeling the collectors transaction graph to be used as an input to the modularity function. The transactions graph *G(V, E)* is an indirected graph where *V(G)* is a set of collector nodes and *E(G)* is a set of all transactions among the nodes (collectors). An edge $E_{i,j}$ represents a transaction (sales or transfer) between collector node *i* and collector node *j* at any point of time involving any asset. The edge weight corresponds to the frequency of transactions between the two nodes.

Adjusting the suspicious transaction weight

Algorithm 1 assigns a positive suspicious score to all collectors who appear at least once in a cycled transaction chain. To enhance the granularity of this method, we propose adjusting the suspicious transaction edge weight in the collector transactions graph. In this graph, the weight of a transaction edge in the graph indicates the frequency at which a transaction occurs between two actors. We calculate a suspicious transaction weight by adjusting the transaction frequency measure using the following equation:

$$adjustedWeight_{i,j} = \frac{weight_{i,j} * (score_i + score_j)}{(1 + |score_i - score_j|)}$$

where $weight_{i,j}$ is the current transaction frequency between $collector_i$ and $collector_j$, and $score_i$, $score_j$ are the suspicious scores for $collector_i$ and $collector_j$ respectively. Adding 1 to the denominator is to prevent the division by zero error. With this approach, the suspicious score similarity between two collectors has an inverse effect on adjusted suspicious transaction weight; meaning that the higher similarity of the suspicious

scores of two collectors leads to higher increase in the adjusted weight of the transaction between them. This is to favor the similarity of actors in calculating their tie strength. We argue that the new graph with the adjusted weights, if it involves the suspicious collectors, will show stronger signs of modularity as washtrader communities tend to collude and form cliques in which they have stronger transaction ties.

Results

The Bipartite Transaction Graph

Figure 3 shows a sub-graph of the bipartite transaction graph. It includes the edges with weight > 2 and the vertexes with betweenness centrality measure > 10. The assets are shown in yellow and the collectors are shown in red. The sub-graph seems sparse with some collectors being involved in a few transactions and the others being involved in a more connected chain of transactions that at some point leads to highly popular assets that have been owned by multiple collectors over separate time episodes. Overall, this graph resembles a pattern of scale free networks where a few nodes are well-connected and can potentially have influential power over the entire network; in this case, the power pertains to influencing the projected price of the assets and the perception of their market value.

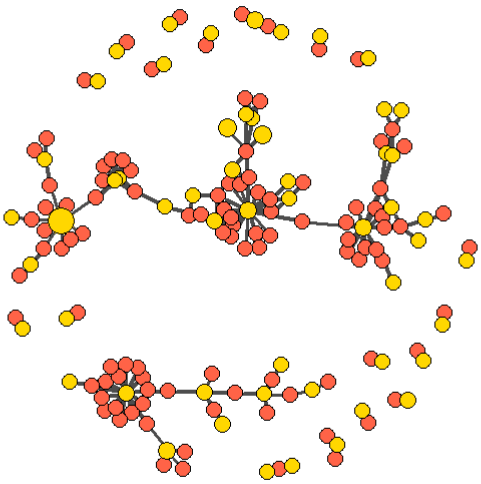

Figure 3. The bipartite transaction graph with edge weight > 2 and vertex centrality > 10. Red nodes represent assets, and yellow nodes represent collectors.

The Suspicious Assets and Collectors

Our algorithm has identified 285 (out of 10,000) potentially washtraded assets. It also found 745 collectors (out of 5659) involved in transactions with a suspicious asset at least once. The highest suspicious score for the collectors was 82 (three collectors), which means three collectors were involved in a transaction with a suspiciously washtraded asset 82 times. Further investigation of the top three collectors yields that they are potentially separate wallets belonging to the same individual or a group of colluded individuals. Two of the collectors solely transferred assets (105 times) to or received assets for free (107 times) from the third collector. The third collector was the only one involved in buying or selling assets with monetary exchange (107 times). All three actors have an anonymous profile that is unnamed and does not include an avatar or

any social media handle. This trend has been observed among many other collectors. Although the assets in the CryptoPunks and other NFT collections are quite identifiable and some of them are very well-known (e.g., CryptoPunks #9998), the collectors who buy those assets are not necessarily identifiable and chose not to include any identifiable information such as social media handles or websites.

Transaction Graph Modularity

The modularity function is performed with the randomize parameter "on" and the use of edge weights "enabled". The results yield a modularity measure of 0.665 for the graph, and with resolution = 1.0 it detects 37 communities. Figure 4 shows the size distribution of the detected modules in a scatter plot.

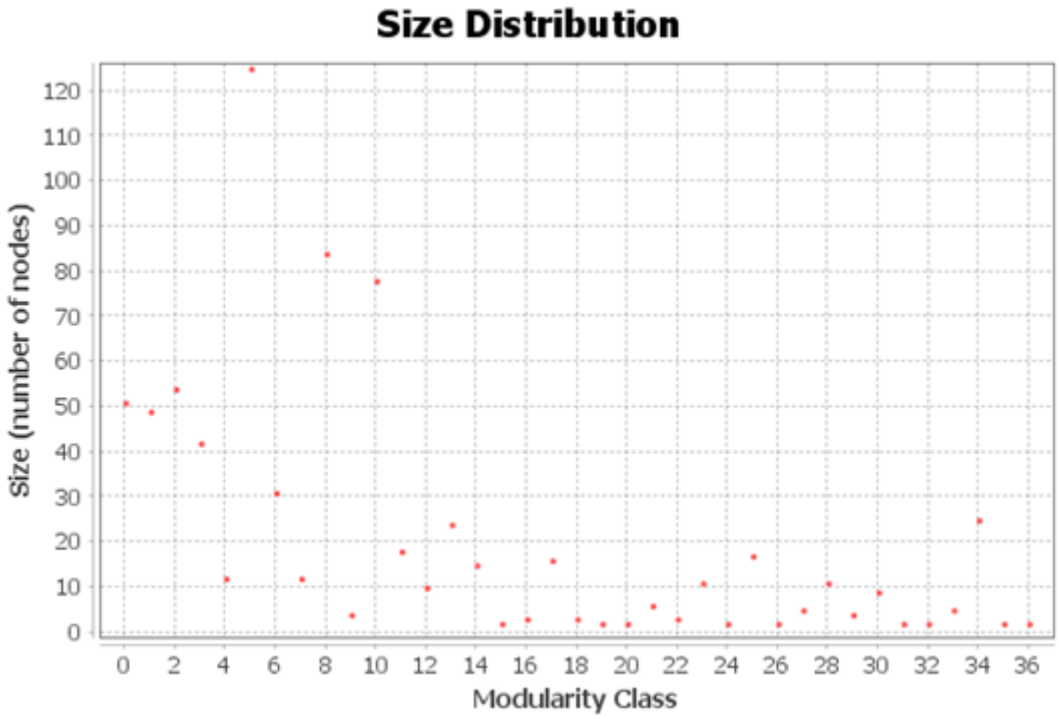

Figure 4. Transaction graph modularity size distribution

For simplicity of the presentation, we selected a cut-off point of 40 for the size of the communities and hence considered the top seven communities for presentation. Figure 5 shows the communities of potentially suspicious collectors in the transaction graph. The size of the node is proportional to its suspicious score. As seen in the graph, there are a few highly suspicious collectors in each community with the orange colored community including the top three suspicious collectors mentioned earlier.

Transaction Graph Modularity with Adjusted Edge Weight

After adjusting the edge weight in the potentially washtraders sub-graph, and including only the transactions with the adjusted weight > 3 (filtering out "innocent" actors), we ended up with 460 suspicious transactions among 397 collectors. The sub-graph modularity is calculated with the same approach in Gephi, and this time, a modularity of 0.878 is calculated. The modularity of the sub-graph is higher than the modularity of the original graph, which indicates a higher tie strength and more cliques inside each community compared to outside the communities. This can be a sign of suspicious activities going on inside each community. Figure 6 shows the distribution of community sizes and Figure 7 shows the top 9 communities of suspicious actors in a modular sub-graph. The biggest modules in this sub-graph are module 13 (purple) with 29 nodes, module 3 (light green) with 26 nodes, and module 10 (blue) with 23 nodes. Other modules in this sub-graph include 10 to 18 nodes.

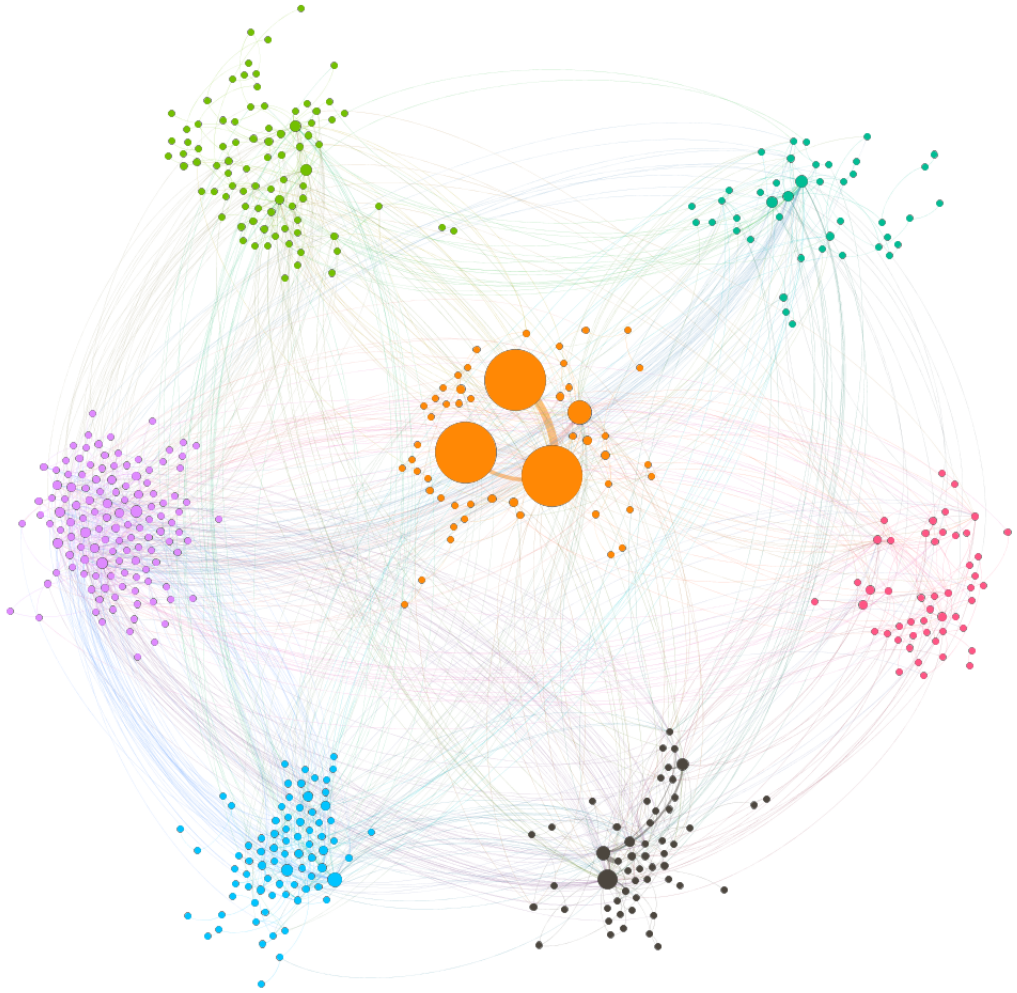

Figure 5. Network graph representing top 7 communities of suspicious accounts. color represents community, size represents suspicious rank, and edge weigh represents transaction frequency.

We measured the local clustering coefficient of each node. The local clustering coefficient of a node measures how close its neighbours are to being a clique. The measure is between 0 and 1, where one means all possibles connections among the neighbours are present. We found six nodes in this sub-graph with clustering coefficient of 1. These nodes belong to module 13 and module 10 with size 29 and 26 respectively.

We also examined the number of triangles each node appears in. The highest number of triangles that a node is part of is 17. This node appears in module 3 with size 26. Another node in this module appears in 16 triangles. Module 10 ranks second as it involves two nodes each appearing in 10 triangles. Based on the above statistics, it appears that the three biggest modules (13, 3, and 10) show stronger evidence of cliques, which can inform us about potential washtrading activities to watch for.

Discussion

The modularity of a graph partition is a value between -1 and 1. This value measures the density of links inside communities as compared to links between communities. As for the transaction graph modularity,

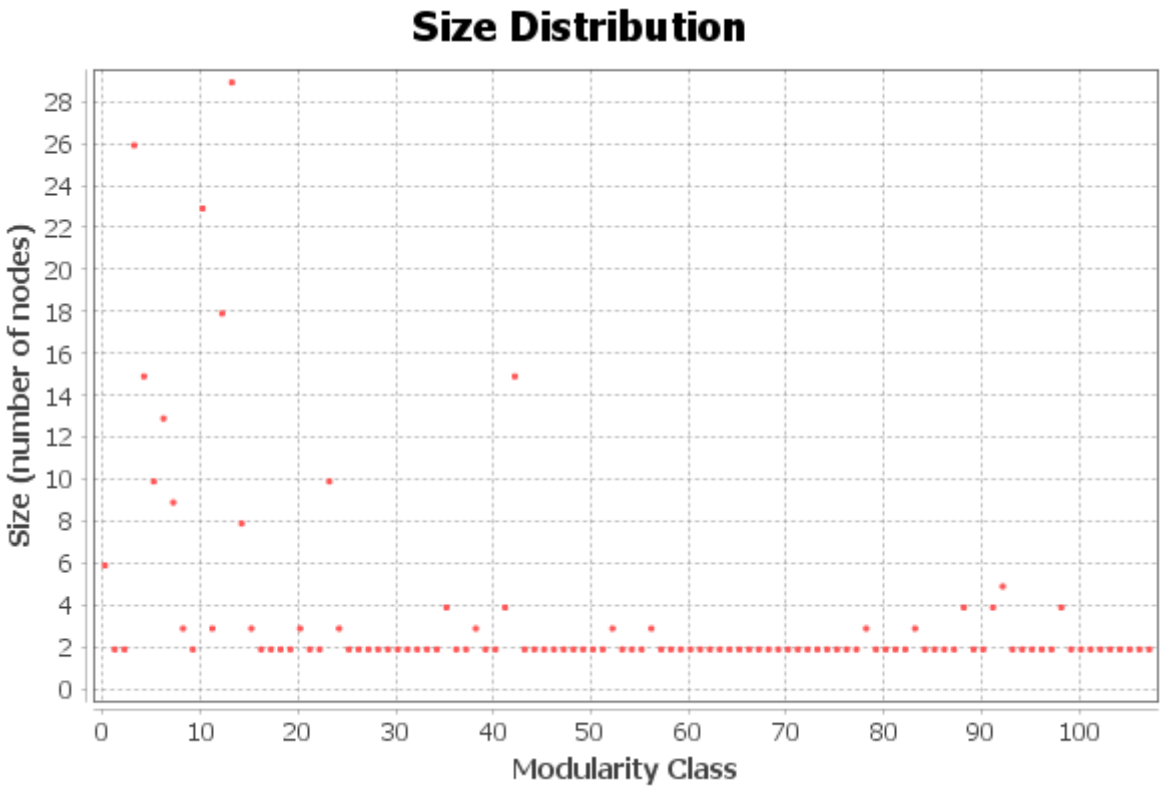

Figure 6. The adjusted sub-graph modularity size distribution

this value is closer to 1 (0.665). We argue that this measure is a convincing indicator that the transaction graph containing the suspicious collectors is modular. Each module represents a community of suspicious washtraders. Although we do not imply that all the nodes (collectors) in each community are potential washtraders, we believe that the suspicious score is a good indicator to identify which actors in the network should be watched for potential suspicious activity in future. Combating washtrading is a nontrivial task. It is computationally intensive to identify all cycles in a graph in the hope to identify the washtraders. Our approach bypasses this step by taking advantage of a bipartite graph structure, which does not require us to literally detect the cycles using a conventional depth-first search method. By focusing on the simple washtrading motif types only, we were able to take on a two-step methodological approach that performs efficiently: Going through each asset to identify whether it is involved in a closed cycle, and only then update the suspicious score for collectors involved in the transactions with the asset.

Our methodology can be done in real-time, as the suspicious scores can be calculated as new actors with new transactions come in. As mentioned in the methods section, the time complexity of the method is linear and is independent of the number of transactions, which means the time complexity does not increase with the growing number of transactions. Since the suspicious scores are stored for each collector, at a later transaction involving an existing collector, the suspicious score can be extracted and updated in real-time.

Our method was intended to provide a tool for more rigid monitoring of fraudulent activities in the NFT market. Platform owners are the entities who can technically implement the measures such as the suspicious scores for collectors as a risk indicator, and can apply sanctions if any. However, we should acknowledge some limitations especially regarding the market regulations that may potentially hinder the practical implications of our approach by platform owners in this emerging asset class; although washtrading is considered illegal and actors can be subjected to sanctions in more traditional markets, the same regulatory scrutiny is not yet established and present in the NFT market. Meanwhile, the recent volatility in the NFT market can potentially give actors increased motivation to abuse the situation to pursue their washtrading activities.

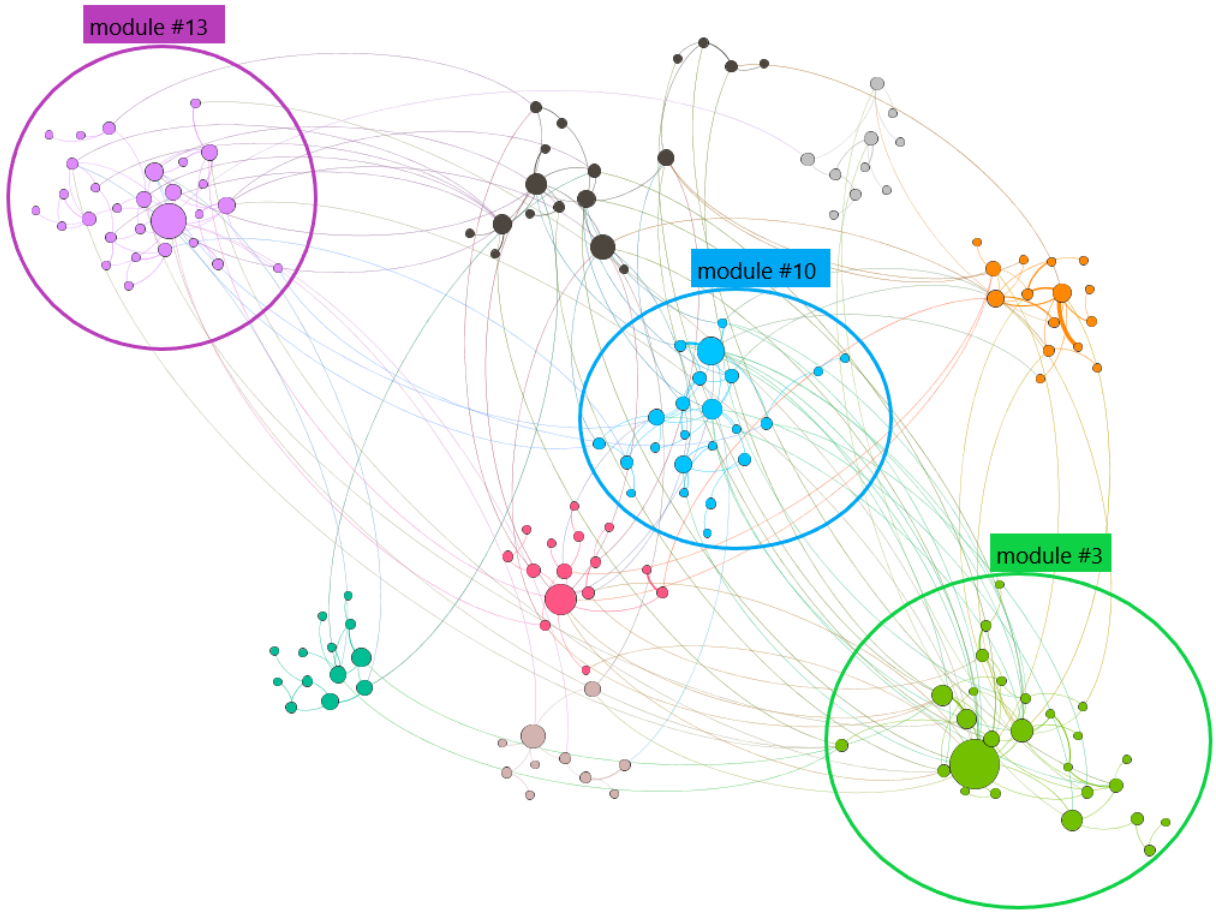

Figure 7. Top 9 top suspicious communities with adjusted edge weight

Thus, it is likely for the NFT market to be faced with even greater frequency of fraudulent activities such as washtrading. This calls for NFT platforms to seek written policies and implement more robust control against such incidents.

It is also important to note that although the present approach is suggested for washtrading identification in NFT networks, we expect that the conventional markets such as online auctions can also benefit from this two-step methodology as these markets already have a more rigorous regulatory establishments to combat these issues.

One limitation observed in the study of washtrading, is that there is merely no single source of truth that can act as a baseline for detection algorithms for validity test. Some of the washtrading incidents that involve popular assets find their way to media outlets and become publicized, but platforms are still exploring methods to detect all those incidents. Our approach is one of the few first steps to shed light on the pos-

sible methods to combat this issue. Although a robust evaluation of the method is not available, the fact that the identified potentially suspicious collectors form modular communities can be a justification of the effectiveness of this approach. After all, even the publicized incidents of washtrading do not claim 100% accuracy and there is always an "aleged" term used when describing such situations. Thus, as potentially another limitation of this study, we emphasize that we do not claim that the identified incidents are 100% washtrading incidents, rather our goal is to provide a base for more cautious and rigid monitoring of actors in the network.

For further evaluation of the current method and potentially other approaches proposed in research in this area, we recommend a technique to synthesize washtrading scenarios in a random transaction graph. The available graph packages in R software provides methods to produce an acyclic graph with a given topology such as scale-free network pattern. The following is our suggested approach to generate such data. In the next step we propose a random selection of collectors in multiple groups, and make them washtrading agents where they would add edges to the graph in their group to simulate a washtrading scenario. In both steps we need to consider the fact that each transaction should be associated with an asset and make sure that the transactions are valid, meaning that an asset is not being sold multiple times to the same collector without being sold to other collectors. Synthesizing a graph in the above manner with random washtrading agents will provide us a ground truth to compare proposed washtrading detection algorithms against.

Another direction we propose is a further investigation of the suspicious communities. In this study, we did not differentiate between the short-lived transactions and the transactions that lasted longer. It is not surprising that sometimes washtraders may attempt to conduct several transactions in short period of time to increase the transaction volume in a limited time frame (e.g., 24h) in a hope to artificially inflate the asset price. Future studies can consider the time factor to give more weight to transactions that occur in a shorter time frames. This might increase the accuracy of the results.

As mentioned above, the NFT market can sometimes be highly volatile and many aspects of the market can be impacted by this volatility. Such impacts may include increased motivation for opportunistic actors to take on malicious behavior in the market. Future research can explore such impacts and provide insights on the effect of market volatility on the malicious behavioral patterns in the market.

Conclusion

In this research we tackled a prevalent issue in the NFT trading space. Washtrading is not unique to NFT and similar forms of it can be observed in other markets such as online auctions and cryptocurrency. In this paper, we acknowledged several differences between NFTs and other markets and provided a unique method for identification of washtrading incidents that can be best applied to this domain. We also identified several challenges in NFT washtrading identification research. One of those challenges is the lack of ground truth data of washtrading incidents in NFT space that makes it challenging to evaluate proposed methods. Our paper provided suggestions for future research to address those challenges.

References

Abidi, W. U. H., Daoud, M. S., Ihnaini, B., Khan, M. A., Alyas, T., Fatima, A., and Ahmad, M. (2021). "Real-Time Shill Bidding Fraud Detection Empowered With Fussed Machine Learning," *IEEE Access* (9), pp. 113612–113621.

Adabi, S., Farhadinasab, H., and Jahanbani, P. R. (2022). "A genetic algorithm-based approach to create a safe and profitable marketplace for cloud customers," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–33.

Cao, Y., Li, Y., Coleman, S., Belatreche, A., and McGinnity, T. M. (2014). "Detecting wash trade in the financial market," in *2014 IEEE Conference on Computational Intelligence for Financial Engineering & Economics (CIFEr)*, IEEE, pp. 85–91.

Cong, L. W., Li, X., Tang, K., and Yang, Y. (2021). "Crypto wash trading," *arXiv preprint arXiv:2108.10984*

Damiani, J. (2021). *Beeple's 'the first 5000 Days' sold to metakovan, founder of metapurse, for $69,346,250*. en. https://www.forbes.com/sites/jessedamiani/2021/03/12/beeples-the-first-5000-days-sold-to-metakovan-founder-of-metapurse-for-69346250/?sh=520cf2a24de4. Accessed: 2022-4-17. 2021.

Dowling, M. (2022a). "Fertile LAND: Pricing non-fungible tokens," *Finance Research Letters* (44), p. 102096.

Dowling, M. (2022b). "Is non-fungible token pricing driven by cryptocurrencies?," *Finance Research Letters* (44), p. 102097.

Eigelshoven, F., Ullrich, A., and Parry, D. (2021). "Cryptocurrency Market Manipulation: A Systematic Literature Review,".

Fire, M., Puzis, R., Kagana, D., and Elovici, Y. (2022). "Large-Scale Shill Bidder Detection in E-commerce," *arXiv preprint arXiv:2204.02057*.

Franceschet, M. (2021). "The Sentiment of Crypto Art," *Proceedings http://ceur-ws. org ISSN* (1613), p. 0073.

Golmohammadi, K., Zaiane, O. R., and Díaz, D. (2014). "Detecting stock market manipulation using supervised learning algorithms," in *2014 International Conference on Data Science and Advanced Analytics (DSAA),* IEEE, pp. 435–441.

Howcroft, E. (2021). *Twitter boss Jack Dorsey's first tweet sold for $2.9 million as an NFT*. en. https://www.reuters.com/article/us-twitter-dorsey-nft/twitter-boss-jack-dorseys-first-tweet-sold-for-2-9-million-as-an-nft-idUSKBN2BE2KJ. Accessed: 2022-4-17. 2021.

Kanellopoulos, I. F., Gutt, D., and Li, T. (2021). "Do Non-Fungible Tokens (NFTs) Affect Prices of Physical Products? Evidence from Trading Card Collectibles," *Evidence from Trading Card Collectibles* .

Majadi, N., Trevathan, J., and Bergmann, N. (2019). "Collusive shill bidding detection in online auctions using Markov random field," *Electronic Commerce Research and Applications* (34), p. 100831.

Mukhopadhyay, M. and Ghosh, K. (2021). "Market Microstructure of Non Fungible Tokens," *arXiv preprint arXiv:2112.03172*.

Murray, J. A. (2021). "Sell your cards to who: Non-fungible tokens and digital trading card games," *AoIR Selected Papers of Internet Research*.

R Core Team (2021). *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria.

Regner, F., Urbach, N., and Schweizer, A. (2019). "NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application,".

Trevathan, J. and Read, W. (2007). "Investigating shill bidding behaviour involving colluding bidders," *Journal of Computers* (2), pp. 63–75.

Trevathan, J. and Read, W. (2021). "Detecting multiple seller collusive shill bidding," *Electronic Commerce Research and Applications* (48), p. 101066.

Tsang, S., Koh, Y. S., Dobbie, G., and Alam, S. (2014). "Detecting online auction shilling frauds using supervised learning," *Expert systems with applications* (41:6), pp. 3027–3040.

Victor, F. and Weintraud, A. M. (2021). "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proceedings of the Web Conference 2021,* pp. 23–32.

Wachter, V. von, Jensen, J. R., Regner, F., and Ross, O. (2021). "NFT Wash Trading: Quantifying suspicious behaviour in NFT markets," in *Financial Cryptography and Data Security. FC 2022 International Workshops*.

Wang, Q., Li, R., Wang, Q., and Chen, S. (2021). "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*.

Whitaker, A. (2019). "Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts," *Artivate* (8:2), pp. 21–46.

White, J. T., Wilkoff, S., and Yildiz, S. (2022). "The Role of the Media in Speculative Markets: Evidence from Non-Fungible Tokens (NFTs)," *Available at SSRN 4074154*.