Association for Information Systems
AIS Electronic Library (AISeL)

Wirtschaftsinformatik 2023 Proceedings | Wirtschaftsinformatik

10-9-2023

Revealing Hidden Self-financed Wash Trading in Non-Fungible-Token Markets

Henri Beyer
University of Cologne, Germany, beyer@wim.uni-koeln.de

Patrick Seidel
University of Cologne, Germany, seidel@wim.uni-koeln.de

Sven Stahlmann
University of Cologne, Germany, stahlmann@wim.uni-koeln.de

Detlef Schoder
University of Cologne, Germany, schoder@wim.uni-koeln.de

Follow this and additional works at: https://aisel.aisnet.org/wi2023

Recommended Citation

Beyer, Henri; Seidel, Patrick; Stahlmann, Sven; and Schoder, Detlef, "Revealing Hidden Self-financed Wash Trading in Non-Fungible-Token Markets" (2023). *Wirtschaftsinformatik 2023 Proceedings*. 24.
https://aisel.aisnet.org/wi2023/24

This material is brought to you by the Wirtschaftsinformatik at AIS Electronic Library (AISeL). It has been accepted for inclusion in Wirtschaftsinformatik 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Revealing Hidden Self-financed Wash Trading in Non-Fungible-Token Markets

Research in Progress

Henri Beyer[1], Patrick Seidel[1], Sven Stahlmann[1], and Detlef Schoder[1]

[1] University of Cologne, Cologne Institute for Information Systems, Cologne, Germany
{beyer,seidel,stahlmann,schoder}@wim.uni-koeln.de

Abstract. Pricing and sales volumes for non-fungible tokens (NFTs) have seen a meteoric rise and fall in recent years. Partially because of a loss of faith in the true values of NFT assets. Wash trading has emerged to artificially inflate asset prices and trading volumes of NFTs. This not only endangers the integrity of NFT markets but also raises doubts about the authenticity of NFT values. Previous research has identified wash trading actors with techniques such as cyclical trading. Many of the presented techniques, however, can be associated with flaws concerning obviousness or feasibility with constrained capital resources. We propose a method to identify a more intricate and concealed form of wash trading called self-financed trading. Our approach identifies suspicious activities by tracking cash and asset flows between blockchain addresses. This enables us to reveal networks of wash trading designed to reap marketplace rewards or insinuate demand to drive up prices.

Keywords: Non-Fungible-Tokens (NFTs), Wash Trading, Price Inflation, Cryptocurrency

1 Introduction

With the rise of blockchain technology entire new classes of digital assets have emerged. One of these asset types that has gained a lot of traction recently is Non-Fungible-Tokens (NFTs). NFTs are typically employed to represent a digital certificate of ownership for unique assets (Ethereum Foundation, 2022). These assets can take various forms such as digital art, event tickets (Regner et al., 2019) and collectibles (Tahmasbi & Fuchsberger, 2022) as well as physical assets like real estate.

Decentralized blockchain networks offer benefits such as increased transactional security and privacy (Rejeb et al., 2021). However, the lack of regulation and a high degree of anonymity fosters fraudulent activities such as market manipulation or scams (Eigelshoven et al., 2021).

One popular market manipulation technique is wash trading. Wash trading describes the practice of one or more parties creating artificial transactions in a marketplace for their own gain (Tom C. W. Lin, 2017). As both sides of these trades are colluding the

18th International Conference on Wirtschaftsinformatik,
September 2023, Paderborn, Germany

traders are not exposed to any financial risk. Wash trading has the goal to drive prices of assets up or down, deceive unknowing parties to buy assets at artificial prices (Pouncy, 1995), or reap kickbacks from exchanges or brokers (SEC, 2006).

Wash trading in traditional financial markets has been an established research topic in many market environments such as trading at stock exchanges (Cumming et al., 2011, p. 2) and agricultural markets (Culver, 1985, p. 1). The focus has mostly been on the effects on market integrity and market designs. Due to its threat to the stability of said markets, many regulatory bodies such as the Commodity Futures Trading Commission prohibit wash trading activities (CFTC Glossary, 2023).

NFT wash trading is done by trading NFT assets between blockchain addresses (often referred to as wallets) within the realm of control of a single or colluding group of wash traders. Wash trading is employed to artificially increase an asset's price or trading volumes to insinuate inherent value or demand. Since prices of NFTs are determined by unregulated offer and demand of anonymous actors fair values of assets are inherently hard to quantify (Jordanoska, 2021, 716).

Few studies already attempt to identify wash trading activities in NFT markets by tracking the transaction history of NFT assets. These studies apply the concept of cyclical trading to identify malicious trading activities using graph-based methods (Das et al., 2022; Tahmasbi & Fuchsberger, 2022; Wachter et al., 2022). Cyclical trading denotes the concept of trading assets in a circular fashion generating risk-free trading activity at previously set prices. However, we argue that this detection technique is associated with significant flaws. Small cycles are easily visible in the transaction histories on NFT markets and are therefore easily recognizable for end-users, while large cycles of unassociated addresses require increasing capital expenditure. The arbitrary generation of Ethereum addresses also makes circumventing cyclic trading trivial for colluding wash traders.

Therefore, we propose a more comprehensive approach by additionally incorporating the transaction history of blockchain tokens to detect cyclical wash trading activity. Our approach can identify self-financed wash trading which denotes the practice of funding a previously unassociated blockchain address to buy NFTs from oneself. This leads to concealed wash trading activity. Since wash traders need to move capital to execute their artificial trades, we screen the transaction data for value cycles. These value cycles are comprised both of NFT asset transactions and blockchain capital flows for example of ETH. Incorporating the transaction history has certain advantages. First, the arbitrary generation of wallets does not circumvent detection if the trade is self-financed. Second self-financed trades are not easily visible to end users and therefore more likely to be used by malicious actors.

In this study, we analyze transactional data within an NFT collection on the popular Marketplace LooksRare. Using our proposed approach, we are able to find multiple accounts of self-financed wash trading. In this paper, we report the found malicious trading behavior regarding the associated trading volume and asset price developments. Our finding highlights the importance of monitoring suspicious trading activity in unregulated markets such as NFT marketplaces.

2 Theoretical Background

Research regarding wash trading in NFT marketplaces is scarce since it is still in its early stage of adoption (Tahmasbi & Fuchsberger, 2022). Instead, research has focused on a broad range of security issues, such as copycat art (Das et al., 2022) theft of personal information, and shill bidding (Mukhopadhyay & Ghosh, 2021).

Wash trading in traditional markets has been known to be subject to regulatory penalties. Thus, techniques for detecting wash trading are more developed in stock and commodity markets. Research has been focused on market environments such as trading at stock exchanges (Cumming et al., 2011) or agricultural markets (Culver, 1985, p. 1) and examined the effects on market integrity and market designs.

Motivations for wash trading in the NFT realm generally fall into three categories. Firstly, a wash trader might aim to artificially alter prices or trading volumes of assets within his possession. Some marketplaces offer rewards for trading volume generation which opens the possibility of wash trading to reap marketplace rewards (Mukhopadhyay & Ghosh, 2021). Cong et al. (2022) have studied wash trading in the taxation domain concerning cryptocurrencies and NFTs identifying a strategy of tax-loss harvesting during end-of-year periods (Cong et al., 2022).

Initial approaches studied wash trading solely in cryptocurrency trading, e.g. analyzing whether exchanges aim to inflate their trading volume to increase their relevance among other competitors (Cong et al., 2019). The approaches to detect instances of wash trading or flag suspicious behavior can be categorized into anomaly- and graph-based techniques. Cong et al. (2019) follow the anomaly-based approach utilizing first-digit-distributions following Benford's law and transaction roundness (clustering at round sizes) to quantify suspicious transactions totaling an average of 70% at unregulated cryptocurrency exchanges (Cong et al., 2019). Victor and Weintraud (2021) identify cyclical wash trading activity by searching for strongly connected components in transaction graphs to quantify a lower-bound estimate of wash trading frequency in cryptocurrency exchanges (Victor & Weintraud, 2021).

In the context of NFTs Tariq & Sifat (2022) utilize the anomaly-based approach to identify widespread suspicious and non-human-like behavior. Due to the unique non-fungible nature of NFTs mainly graph-based techniques have been considered to detect wash trading in NFT markets. Wachter et al. (2022) have detected closed-cycle trading as well as rapid trading sequences by building transaction graphs. Tahmasbi & Fuchsberger (2022) further expand cycle detection by proposing a more efficient algorithm based on bipartite graphs. All of the above literature only considers the flow of NFT assets which due to the arbitrary generation of Ethereum addresses makes the avoiding of cycles trivial to achieve.

3 Method

To detect self-financed wash trading activity, we will introduce the concept of self-financed trading events and search for such events in the collected data. A self-financed trading event can be described as a directed multigraph, called quiver,

consisting of two vertices and two edges in one direction and a third edge in the opposite direction, as can be seen in Figure 1. More specifically, let $Q = \{V, E\}$ be a quiver, where $V = \{u, v\}$ is a set of two vertices representing Ethereum addresses and $E = \{(u, v), (u, v), (v, u)\}$ is a set of three edges representing token transactions between these addresses. For any edge $e = (u, v) \in E$, u is the source vertex and v describes the destination vertex. The weight $w(e)$ represents the transferred tokens, which can consist of NFTs (ERC-721 tokens) as well as the Ethereum currency wrapped in ERC-20 tokens as WETH. A legitimate NFT sale would be represented by a pair of two edges $\{e_1 = (u, v), e_2 = (v, u)\}$ and the corresponding weights $w(e_1)$ being an NFT asset and $w(e_2)$ being Ethereum currency flow. If a third edge $e_3 = (u, v)$ exists, with $w(e_3)$ being Ethereum currency flow, we define this quiver as a self-financed trading event, since the buying address v receives funds from the selling address u. This allows us to look past the cyclic asset trading and detect cyclic value flows which could be used to conceal wash-trading by hiding it from NFT Marketplace users.

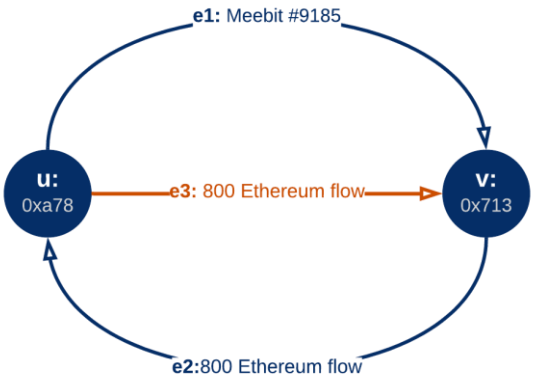

Figure 1. Graph representation of a self-financed trading event

Using the previously defined concept we build a directed multigraph by getting NFT flows and buyer and seller Ethereum addresses from the NFT Marketplace LooksRare as well as payment flow directly from the Ethereum blockchain, utilizing the block explorer Etherscan and the blockchain infrastructure provider Alchemy. The publicly available transaction histories of the selected collection were systematically scraped using LooksRare's API and the seller's Ethereum address, the buyer's Ethereum address, the amount that the buyer paid, and the platform's name of the NFT asset were saved. We used this information to model each sale event in the history of the collection as a quiver of the previously described format with u being the seller's address and v being the buyer's address.

Further, we combined this data with the payment flow data from the Ethereum blockchain. Specifically, for every sale on the NFT marketplace, the buyer's entire Ethereum transaction history was scraped using the public API of Etherscan and enriched with metadata obtained from Alchemy. It was checked whether any flow of

Ethereum currency fitted the description of an edge $e = (u, v)$ with $w(e)$ consisting of the Ethereum funds, meaning the seller's address had funded the buyer's address. These self-financed trading events were recorded and used four our preliminary results.

We focused on a NFT collections with a high amount of trading volume in a short period of time. This was conducted to increase the likelihood of wash trading finds under the hypothesis that wash trading activity leads to spikes in transaction volumes and asset prices. For our preliminary analysis, we chose one collection from this data.

4 Preliminary results

Following the approach outlined above we were able to successfully identify self-financed wash trading activity. Examples of identified self-financed trades are displayed in Table 1. The first such finding concerns the NFT art piece "Meebit #9185" of the "Meebits" collection. It was sold in January of 2022 at a sale price of 800 ETH. The transaction history displayed on the LooksRare marketplace indicates a regular NFT transaction between the seller's contact address and the buyer's contact address.

Our self-financed wash trading detection approach screened the buyer and seller for previous Ethereum currency flows. This revealed a previous transaction indicating the original seller address funded the subsequent buying side with 800 ETH in a separate transaction mere minutes before the NFT sale.

This is a severe indication of suspicious wash trading activity as the buyer and seller are connected by a prior financial connection pertaining to almost the exact amount of the asset sale. The close vicinity of the initial funding further deepens suspicions of malicious trading behavior. While highly unlikely, it is theoretically possible that this financial connection is merely a coincidence. This, however, is refuted by the high frequency of suspicious transactions within this collection indicating systematic wash trading activities.

Table 1. Example instances of self-financed trades in the Meebits collection

Asset name	Previous ETH flow	Sale Price (ETH)	Fund Date	Sale Date
Meebit #9185	800	800	2022-01-28	2022-01-28
Meebit #15377	600	600	2022-01-14	2022-01-14
Meebit #7814	600	600	2022-02-03	2022-02-03
Meebit #15115	392	392	2022-01-17	2022-01-17

Our analysis revealed 5580 self-financed trading events involving 527 individual Ethereum addresses. The total trading volume of sales that we flagged as suspicious in this collection was 6,068,162,419.74 USD. The funding volume in this single collection shows the potential scale of fraudulent NFT transactions and supports our hypothesis that these activities are potentially fraudulent and aimed at artificially inflating the trading volume and value of the NFT collection.

Our preliminary results provide significant evidence of fraudulent activity in the NFT market, and the potential scale of these transactions highlights the need for action to prevent and monitor this behavior.

However, there are certain restrictions to these results, primarily regarding the financial linkage between the colluding entities. At present, we only monitor for direct capital transfers between the implicated addresses. This detection method could be bypassed by incorporating extra addresses to mask the origin of the funding. With improvements in detection techniques and computational resources, we could also spot these more complex networks. Besides, wash traders might opt to finance their Ethereum addresses off the blockchain, using fiat currency to acquire cryptocurrency via a coin exchange. In such instances, we would be unable to identify financial collusion between the buyer and seller. Nonetheless, this procedure would be incredibly laborious for wash traders, especially those dealing with a significant number of Ethereum addresses.

5 Conclusion and Outlook

In this paper, we propose an approach to identify self-financed wash trading activity and analyze trades of a single collection. Our results indicate that up to 6,068,162,419.74 USD of trading volume in that collection could stem from fraudulent activity. We plan to further extend our study by incorporating a more diverse set of NFT collections. We believe that an expansion of the underlying dataset across a diverse range of NFTs would yield more instances of wash trading activity. Furthermore, applying our approach to a representative sample of NFT transactions we can make a more robust estimate for the overall frequency of self-financed wash trading activity in NFT markets.

A core goal of wash trading is the deception of unassuming buyers to purchase NFTs at artificial prices (Pouncy, 1995). Therefore, the identification of buyers that unknowingly purchased a wash-traded asset is a core future research focus. Precise identification of flagged transactions enables the quantification of the financial damage induced by artificial price inflation. Wash trading activity is associated with cost by the accumulation of transaction fees (gas fees) for each artificial transaction. It is possible to then assess the profitability of wash traders by calculating both their gain resulting from an inflated sale and the "cost of attack" (Wachter et al., 2022) incurred by transaction fees.

Finally, keeping a record of suspicious wash trader accounts in a database would allow us to conduct a more focused search. Rather than randomly sifting through vast amounts of transaction data for signs of wash trading, we could concentrate our efforts on accounts linked to identified wash traders. This approach would likely uncover a greater number of wash trading transactions and reveal extensive networks of colluding wash traders. Additionally, this directed approach would also make the search for value cycles across multiple accounts computationally manageable at a larger scale.

References

CFTC Glossary. (2023, February 28). https://www.cftc.gov/LearnAndProtect/EducationCenter/CFTCGlossary/glossary_wxyz.html

Cong, L., Landsman, W. R., Maydew, E. L., & Rabetti, D. (2022). Tax-Loss Harvesting with Cryptocurrencies. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.4033617

Cong, L., Li, X., Tang, K., & Yang, Y. (2019). Crypto Wash Trading. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.3530220

Culver, J. (1985). Market Integrity Issues and the Agricultural Markets.

Cumming, D. J., Zhan, F., & Aitken, M. J. (2011). Exchange Trading Rules, Surveillance, and Insider Trading. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.1990453

Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2022). Understanding Security Issues in the NFT Ecosystem. In H. Yin, A. Stavrou, C. Cremers, & E. Shi (Eds.), *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 667–681). ACM. https://doi.org/10.1145/3548606.3559342

Eigelshoven, F., Ullrich, A., & Parry, D. (2021). Cryptocurrency Market Manipulation: A Systematic Literature Review. *ICIS 2021 - International Conference on Information Systems*.

Ethereum Foundation. (2022, May 14). *Non-fungible tokens (NFT) | ethereum.org*. https://ethereum.org/en/nft/

Jordanoska (2021). The Exciting World of NFTs. A Consideration of Regulatory and Financial Crime Risks. *BUTTERWORTHS JOURNAL of INTERNATIONAL BANKING and FINANCIAL LAW,*

Mukhopadhyay, M., & Ghosh, K. (2021). Market Microstructure of Non Fungible Tokens. Advance online publication. https://doi.org/10.5281/zenodo.5654779

Pouncy, C. (1995). *The Scienter Requirement and Wash Trading in Commodity Futures: The Knowledge Lost in Knowing*. Cardozo Law Review, Vol. 16, No. 5, 1995. https://ssrn.com/abstract=1629256

Regner, F., Schweizer, A., & Urbach, N. (2019). NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application. *Fortieth International Conference on Information Systems, Munich 2019*. https://aisel.aisnet.org/icis2019/blockchain_fintech/blockchain_fintech/1

Rejeb, A., Rejeb, K., & G. Keogh, J. (2021). Cryptocurrencies in Modern Finance: A Literature Review. *ETIKONOMI*, *20*(1), 93–118. https://doi.org/10.15408/etk.v20i1.16911

SEC, U. S. (2006). Commission Opinion: Irfan Mohammed Amanat: SECURITIES EXCHANGE ACT OF 1934 Rel. No. 54708. https://www.sec.govlitigation/opinions/2006/34-54708.pdf

Tahmasbi, N., & Fuchsberger, A. (2022). Non-fungible Tokens - Exploring Suspicious Washtrader Communities in NFT Networks. *ICIS*.

Tariq, S. A., & Sifat, I. (2022). Suspicious Trading in Nonfungible Tokens (Nfts): Evidence from Wash Trading. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.4097642

Tom C. W. Lin (2017). The New Market Manipulation. *Emory Law Journal*.

Victor, F., & Weintraud, A. M. (2021). Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. In J. Leskovec, M. Grobelnik, M. Najork, J. Tang, & L. Zia (Eds.), *Proceedings of the Web Conference 2021* (pp. 23–32). ACM. https://doi.org/10.1145/3442381.3449824

Wachter, V. v., Jensen, J. R., Regner, F., & Ross, O. (2022, February 7). *NFT Wash Trading: Quantifying suspicious behaviour in NFT markets*. http://arxiv.org/pdf/2202.03866v1