Data Science

Capstone Report - Fall 2022

Wash Trading Detection on AMM Decentralized Exchanges

Henrikas Krukauskas

supervised by
Olivier Marin

Preface

I am a senior double-majoring in Data Science and Business & Finance at NYU Shanghai. Over the past few years, I have closely followed the crypto world and the emergence of Web3. This research paper is a supplement for learning more about crypto assets and the issues that exist in these new and uncontrolled markets. In addition, what efforts could be taken to resolve the problems and develop more reliable financial instruments that could aid in the distribution of wealth to the people.

Acknowledgements

I want to thank my supervisor, Professor Olivier Gilles Marin, for guiding and supporting me during this project. In addition, I would like to thank Professor Victor Friedhelm for steering me in the right direction with data collection.

Abstract

Due to the recent rise in popularity of Automated Market Maker Decentralized Exchange, illicit conduct has become widespread in those marketplaces. As there were no studies that evaluated how to detect and quantify wash trading in these exchanges, this research employs a basic z-score statistical method to propose a solution. The complexity of the issue lies in the specificity of the on-chain data, as AMM DEX transactions do not have the bilateral data to implement existing methods for the identification of these activities. This research develops a straightforward yet effective approach to finding or analyzing AMM DEXs, such as Pancake Swap or UniSwap. The results represent only a small portion of the potential wash traded volumes, but it efficiently defines the types and patterns of these malicious activities.

Keywords

Capstone; Computer science; NYU Shanghai; AMM; DEX; Crypto assets; Wash trading; Pancake Swap

Contents

1 Introduction

Since the popularization of smart contracts on a blockchain in 2015, a list of financial securities has been mirrored and recreated in the form of cryptocurrencies or NFTs. Due to the lack of regulations, similar to SEC-enacted regulations for financial securities, in these new financial markets, users have adopted malicious techniques to inflate or manipulate prices. One of the ways to misleadingly increase the price of the security is wash trading, where the user with multiple accounts buys and sells digital goods from and to oneself, causing an increase in trading volume. These illegal methods lead to an increase in the volume that creates more interest from other potential investors. Higher demand and influx of money from new users increase the price of the good as it creates a false feeling of higher popularity of that asset [1]. Blockchain features may enable these illegal activities in digital markets: lack of central regulation, multiple accounts under the same identity, and no limitation on the number of transactions. In [2], Cong et al. introduce statistical methods to analyze financial transactions to evaluate the accounts that do wash trading and cause the inflation of the prices. However, this type of analysis is only possible after the transactions are finalized, and data is correctly collected. The lack of continuity of this analysis lets users get away with their illegal activity and only exposes the problem rather than fixing it. Nevertheless, if we want to find a more hands-on solution to eliminate wash trading, blockchain infrastructures have the means to provide real-time data about every transaction within the nodes [3]. As an objective, the first step of the project is to identify the ways wash trading attacks happen on AMM DEX Pancake Swap. The second step is to learn more about statistical and analytical methods that are helpful in detecting and finding accounts that execute illegal trades. The third step is to design and implement detection code on the AMM DEX Pancake Swap and enhance the existing information about wash trading detection within a blockchain.

2 Related Work

2.1 Defining Wash Trading and Related Activities

Wash trading is a malicious financial activity that inflates the volume of transactions in the exchanges with the purpose of creating more traction and interest from other investors. The Commodity Futures Trading Commission (CFTC) defines it as "Entering into, or purporting to enter into, transactions to give the appearance that purchases and sales have been made, without

incurring market risk or changing the trader's market position" [4]. On cryptocurrency exchanges, wash trading resembles one or multiple accounts executing sell and buy orders among themselves that, in the end, constitute no change in their initial positions and incur no market risk [3]. Most of the time, the accounts would belong to one or several actors that profit from inflated transaction volume for targeted crypto tokens. Currently, this activity is illegal in the U.S. under the Commission Exchange Act of 1936. The traditional financial markets are thoroughly spectated and regulated by SEC to make sure that wash trading activity would not happen. With the popularization of the mirrored traditional financial markets on the blockchain, cryptocurrencies, and NFTs became the new target of wash trading [2]. In the past couple of years, many changes were brought to blockchain-based centralized and decentralized exchanges to stop malicious financial activities from happening; however, based on the previous works [1, 2], wash trading is still present in almost every unregulated crypto token exchange. Wash trading is the most popular malicious financial activity to inflate the transaction volume and increase the interest from other investors or create monetary benefit for the fraudulent agent. For comparison, La Morgia et al. analyze Pump and Dump trends that extremely correlate or happen simultaneously with wash trading on DEX markets [5]. The authors conducted an in-depth statistical analysis based on standards in finance. CFTC defines Pump and Dump as "a manipulative scheme that attempts to boost the price of a stock or security through fake recommendations. These recommendations are based on false, misleading, or greatly exaggerated statements" [4]. In other words, due to public statements on social media outlets, such as Twitter, Reddit, and Discord, the fraudulent agents trick people into joining the joint action of wash trading, where the wash traded volume and real purchases from overblown promotion inflate the price of the crypto assets. Huge amounts of tokens are sold, enriching the fraudulent agents and swiftly reacting investors. Another research paper by Fratrič et al. provides an agent-based case study that runs ML models to replicate and analyze Pump and Dump schemes on the Bitcoin blockchain [6]. Both [5, 6], provide statistical methods and financial trend graph analysis describing how these schemes differ from traditional financial market manipulations. It is important to note that Pump and Dump requires some form of wash trading to inflate the purchase price, as stated in both papers.

2.2 Defining the Decentralized Exchange Types

In a paper [3], Friedhelm and Weintraud elaborate on the importance of understanding the differences between DEXs. Decentralized exchanges lack certain required policies that might be

absent or not enforced. As such, DEXs are the place to produce illicit activities for profit. The authors elaborate on the types of DEX by stating, "The two main DEX variants are based on limit order books (LOB) or automated market makers (AMM)." In their research paper, they analyzed Limit Order Book Decentralized Exchanges because it was easy to track the node transaction between buyer and seller with their respective account information. However, their research indicates that on AMM DEX, the same tracking model would not work because the agents are interacting with a smart contract that executes the trades by balancing liquidity pools. In other words, AMM lacks the bilateral transaction that happens on LOB DEX. In [7], Cui and Gao produce a similar coded tracking model to identify and quantify wash trading on specific crypto tokens on LOB DEXs. While LOB DEX exchanges are still the most popular type of DEX to trade on, AMM is the novelty of blockchain financial markets that is gaining subsequent traction but has not been examined in a similar coded manner. There is a lot of evidence from the authors that their proposed models, if slightly altered, could be feasible in detecting wash trading for single account transactions on AMM DEX. Regardless, no similar research has been conducted to test it. In addition, in the last year, a new type of DEX emerged called Hybrid. Hybrid Decentralized Exchanges use both Automated Market Makers and Limit Order Book functionalities to create the most advanced form of DEX that eliminates many problems that are present in both types of DEX separately [8]. So far, no openly accessible research analyzes this new type of DEX. Nevertheless, there is evidence that in the case of models from [3, 7], there could be a possibility to track potential wash trading activities in these exchanges.

2.3 Understanding the Statistical Methods Applicable

To better understand the tools currently accessible to enhance [3] model, multiple papers were taken into account because of their importance in identifying and analyzing wash trading. However, the major limitation of all these papers is the lack of practical evidence and an abundance of opinions on what is the exact amount of volume that is wash traded. In [1], Le Pennec et al. constitute that from 72% to 98% of the total volume is suspicious on all cryptocurrency exchanges. Another research paper by Amiram et al. constitutes the mean proportion of fake trades that would include wash trading activities is about 19% with a maximum of 89% [9]. In [2], Cong et al. indicate that on average 70% of total volume on cryptocurrency exchanges is wash traded. All these numbers are not fairly indicative of anything except the fact that cryptocurrencies do have wash trading activity that needs to be fixed. Furthermore, many statistical methods used provide

discrepancies on crypto decentralized exchanges with the traditional centralized exchanges. For example, Benford's Law is one of the statistical methods used to identify if the cryptocurrency DEXs conform to the general norms defined by the law [2, 9]. The law indicates that the first significant digit for each transaction would comply with the general distribution of each digit defined by Benford. Nevertheless, smart investors that commit wash trading could bypass this test by embedding certain rules in their smart contracts to execute transactions in a manner that complies with Benford's Law. Thus, multiple statistical approaches used by those authors are not applicable in quantifying and detecting wash trading. Trade Graph and Time Series Analysis were the most convincing methods to identify wash trading as the same methods are extensively used to monitor traditional financial markets [10, 5, 6]. Moreover, most of the researchers mainly used statistical approaches that do not include the use of Machine Learning or Deep Learning techniques, which have the potential to produce better results [10]. Thus, this research will try to use hands-on detection algorithms provided by Friedhelm et al. and Cui et al. [3, 7].

2.4 Additional Methods for Possible Implementation

In [11], Zhou et al. explain the reputation system that could potentially help with either restricting or tracking wash trading on DEXs. However, after deepening the understanding of the wash trading problem on Blockchain exchanges, reputation systems would not be able to limit the occurrence of this illicit activity because it would not stop investors from creating multiple accounts and executing illegal trades. Moreover, reputation systems require monetary incentives for users to execute the rating of each other, which is an additional problem for part of the users that are providing their goods in the market, as the seller has to pay for the rating incentive. Another source that provided an interesting insight into what additional methods could be used in our research was written by Hussan et al. [10]. In the paper, the authors survey currently available methods to detect anomalies within Blockchain. As mentioned before in the subsection above, Trade Graph and Time Series Analysis were the best methods to identify suspicious amounts of volume and wash trading statistically. Machine Learning models were mentioned as the further possible pathway to detect and possibly quantify wash trading. However, research on crypto wash trading has not been using ML models successfully as of right now.

2.5 Orientation of the this Research

This research paper paves the way for an academic understanding of AMM DEXs and how to work with the unique data found in those markets. In addition, it expands on the concept of wash trading in crypto markets and defines a straightforward but effective way to detect and quantify this fraudulent behavior on AMM DEXs. One research paper by Friedhelm et al. gives the foundational knowledge regarding the identification of wash trading on DEXs; nonetheless, the methodology is novel [3]. The objective of the research is to quantify detectable wash trading and to enhance other academics' understanding of these specific marketplaces.

3 Solution

3.1 Dataset and Preprocessing

In this section, I detail what type of data I have collected and how it was preprocessed. In addition, I offer concise observations about the data as well. I decided to gather data on Automated Market Maker Decentralized Exchange Pancake Swap. I chose to utilize BscScan's Developer API, which provided me with access to blockchain data on the Binance platform, where Pancake Swap is hosted. Due to the difficulty of working with massive volumes of data, I choose to utilize data from small time frames, such as the three or six most recent hours. Using the BscScan API, I was able to collect transactions and events, which allowed me to acquire data on executed trades. To extract all trades conducted on Pancake Swap, I had to filter the data to include only transactions executed on the Pancake Swap Router V2 smart contract ("0x000000000000000000000000010ed43c718714eb63d5aa57b78b54704e256024e"). At that time, I had compiled all logs and events that occurred on the DEX. Additionally, the data had to be parsed into a dataframe in which every hex input was translated to human-readable data. To collect only successful swap events, as only those could be utilized to monitor wash trade activity and follow accounts committing legitimate transactions, I filtered data to swaps executed. The table includes 111,872 transactions between 2022-12-15 21:20:47 and 2022-12-16 03:26:58 within the 6-hour timeframe. I was able to compute the overall Pancake Swap volume for the selected time period using the data collected.

After reviewing the information, I decided to delete inactive accounts with fewer than five transactions in the preceding six hours. In the end, I was left with 1022 addresses, 73067 transactions, and 953 distinct pair swap contracts denoting traded tokens. The Table 1 provides a

summary of the resulting data set. Figure 1 depicts the Class Diagram matching the dataset.

Table 1: Overview of Pancake Swap Dataset

	Pancake Swap
Start Date	2022-12-15 21:20:47
End Date	2022-12-16 03:26:58
Number of Swaps	73,067
Number of Traders	1,022
Number of Tokens	953

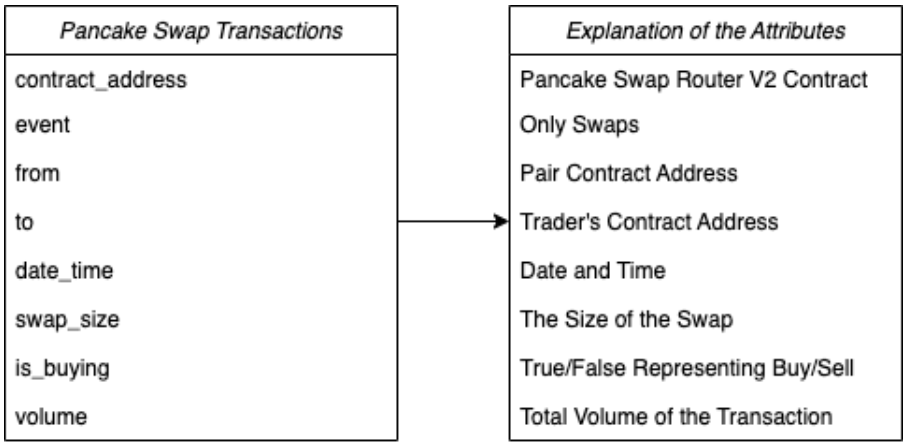

Figure 1: Simplified Class Diagram of the Dataset

3.2 Methodologies and Approaches Analyzed

Due to the lack of prior research examining wash trading on AMM Decentralized Exchanges using on-chain data analysis, it was not easy to come up with a solution for this study. The majority of the approaches I examined were derived from the notion of wash trading and the particulars of the data. To detect wash trading, I had to learn how to identify addresses that commit swaps that result in a minor or little change in their position ratio. Friedhelm et al. evaluated LOB DEXs by looking for round-trip trades executed by several accounts whose position ratio remained unchanged [3]. However, this strategy is ineffective on AMM DEXs because addresses interact with pair contract addresses, which are smart contracts that quickly execute swaps by balancing liquidity pools. Therefore, there is no recipient address on the transaction data that may be associated with round-trip trades. The only approach to discover round trip trades is to examine a single account and observe whether it executes buy and sell swaps with the same pair contract address. However, the majority of wash traders on AMM DEXs bypass this by employing several addresses to engage in illegal activities. After reviewing the accounts, I've observed three distinct

types of wash trading on AMM DEXs:

- As previously stated, the first type occurs when an address executes several buy and sell swaps with the same pair contract address while keeping similar swap sizes. The committed trade swap sizes often follow a normal distribution with a small standard deviation. In addition, the position ratio of these transactions is near to 1, indicating that the position of the address has not changed. Figure 2 provides a more detailed description of the initial type of wash trading.

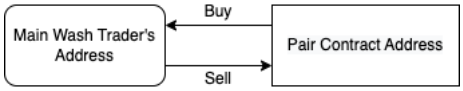

Figure 2: First Type of Wash Trading in AMM DEX

- The second type takes a different method, consisting of many addresses engaging with a pair address contract, with one address executing only buy or sell swaps and the other addresses conducting swaps of the opposing type. In this instance, the algorithms should identify any accounts that execute swaps of comparable sizes to the main address (in most cases, these transactions will fall within three standard deviations of the main account's average swap size). I have never witnessed a situation in which only two addresses engaged in this type of activity; rather, one address would conduct one-sided swaps, and multiple accounts would perform a few trades to maintain a position ratio of about 1 cumulatively. The Figure 3 provides a more detailed description of the second type of wash trading.

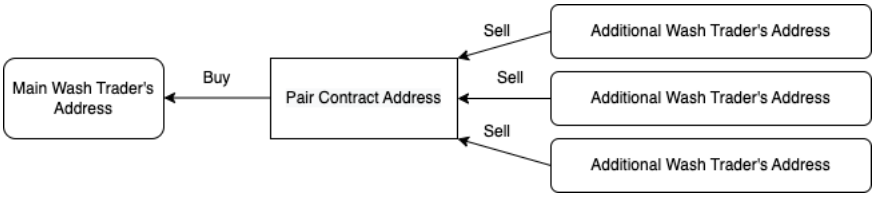

Figure 3: Second Type of Wash Trading in AMM DEX

- In the third type, many addresses execute a small number of trades with equivalent swap sizes, and their cumulative position ratio remains close to 1. Figure 4 provides a more detailed description of the third type of wash trading.

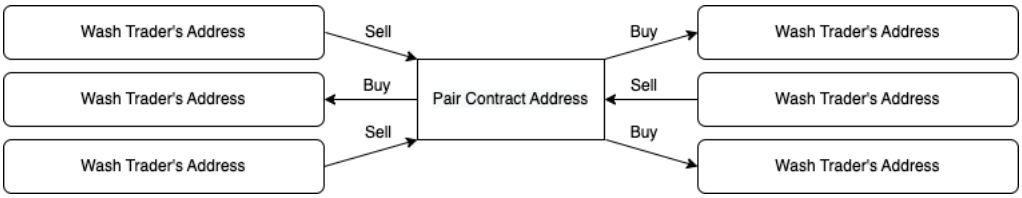

Figure 4: Third Type of Wash Trading in AMM DEX

Based on the data, I have only encountered the first and second types of wash trading. However, the third category remains a distinct possibility. I've also witnessed instances in which multiple addresses adjusted their swap sizes to lesser or larger amounts, making it more difficult to detect these activities and identify the addresses that contribute to wash trading. To detect wash trading with algorithms, I've decided to examine three methods and determine which one is the most effective at detecting wash trading. My initial concept was a straightforward swap size analysis using normal distribution and z-scores. This strategy has yielded noticeable results in locating addresses with comparable swap sizes. In the case of an address that commits the first or second type of wash trading and whose swap size mean changes spontaneously, this method would not provide accurate results, as it would be difficult to identify addresses that are committing wash trading alongside the main address, as the z-score method would include unrelated addresses that executed multiple swaps within three standard deviations of the main address's swap size mean. To address the issue of inaccurate classification of the transactions, I chose to investigate and evaluate two machine learning techniques. K-means algorithm with the hot-one encoding of categorical data was the initial technique. The method examines swap sizes (numerical variable) and contract addresses (categorical variable) to construct data clusters based on the normal distribution. I've created the code that automatically determines the number of clusters for each pair of contract addresses and performs clustering. This strategy yielded findings in which, in many instances, the algorithm classified addresses with a large number of swap transactions as separate clusters and grouped addresses with a small number of swap transactions as separate clusters. Since the results were highly unreliable, I discarded this strategy as a potential solution for detecting wash trading on AMM DEXs. I also wanted to test the K-prototypes technique, which classifies numerical data using K-means and categorical data using K-modes independently. After combining these two results, a single classification dataset for every address is produced. Nonetheless, this method yielded similar results, but the issue this time was determining the number of clusters. As my goal is to detect and quantify wash trading algorithmically, the

elbow method failed to define the correct number of clusters. Elbow method is a technique for determining the ideal number of clusters for K-means or K-prototypes algorithms by testing between 1 and 9 (or more) clusters and estimating cost values. After that, it is straightforward to determine the elbow value that corresponds to the optimal number of clusters for the particular dataset. I discarded both clustering approaches since they produced misleading findings. After rereading the definition of wash trading, I realized that the normal distribution and z-score approach would be the ideal methods for detecting wash trading, as the position ratio would prevent addresses from being misclassified as wash traders. Hence, I added the first method to the code.

3.3 Implementation of Normal Distribution and Z-Score Approach

Implementing the normal distribution and z-score approach is straightforward. I was required to extract from the dataset all unique pair contract addresses during the six-hour interval. Then, I iterated through the pair contract addresses to locate each pair's transactions. For the sake of simplicity and accuracy, I omitted pair contract addresses with fewer than 20 transactions throughout the specified time period. Thus, our z-score methodology would offer data with a large enough sample size to locate the addresses of associated wash traders. In addition, I was required to calculate the token prices in order to provide a price trend for the graphs that would be exhibited later in the paper.

Then, I needed to identify the most active address on the pair contract. If there were numerous most active addresses with the same number of transactions, I would select the one that was at the top of the list. The choice does matter; however, in the time frame that we are looking at, either the addresses would be related to wash traders, or there is no wash trading present in the pair contract address. The number of transactions of most users is small, but if the address represents a smart contract that executes multiple trades, then we would be able to identify it as a wash trading account because the position ratio of those transactions would be close to 1. Obviously, this method is not foolproof, and mistakes are possible; nonetheless, the purpose of this study is to identify big wash trading patterns, as small-scale wash trading would be of no use to the owners of the addresses involved in illegal behavior.

Next, all transactions associated with the most active address were filtered. After collecting and storing this data in a dataframe, I calculated the mean and standard deviation of these transactions. Having done so, I isolated the other addresses and transactions into a different

dataframe and conducted a z-score test, where I included all the transactions that were within three standard deviations of the most active address. The data was then split into addresses with transactions that may constitute wash trading and addresses with transactions that are excluded based on a z-score test.

Then, I computed the position ratio of the addresses and respective transactions suspected of engaging in wash trading. Here is the formula for the position ratio:

$$position\ ratio = \frac{(amount0In.sum() + amount1Out.sum() + 1)}{(amount1In.sum() + amount0Out.sum() + 1)}$$

The addition of 1 to the fraction's numerator and denominator is required to rule out division by 0. In addition, it is advantageous to work with positive numbers because there will be no confusion or computational errors in the code.

Then, I determined whether the position ratio falls between 0.8 and 1.2. If this is the case, then I claimed confidently that the inspected addresses and their related transactions are engaged in wash trading. As you can see, I include position ratios with a 20 percent margin in both directions. It is necessary to account for the fact that I am using data in the 6-hour window and not full historical data of the pair contract address and position ratio might have the deviation because of the lag between executed transactions. For example, not all buy and sell transactions in wash trading occur simultaneously. Some transactions are purposefully delayed in order to generate specific price patterns for the tokens. Ultimately, the objective of these transactions is to attract outside traders by inflating the volume and manipulating the price to generate a false price change trend. Particularly on AMM DEXs, it is significantly simpler to alter the price because some pair contract addresses are initially unpopular, and tiny transaction amounts can have a significant impact on the price shift. In addition, Friedhelm et al. employed a 1% margin in their research, but their approach of locating round trip trades was more tangible [3]. Their chosen margin is too small and unreasonable for this research. After personally analyzing the data, it was determined that the observable and varied wash trade activity varied closely within a 20 percent margin.

The final stage was to collect the results and plot the price line of the pair contract address with the buy and sell transactions of wash traders and other traders. I have compiled the four most descriptive results and listed them in Table 2.

As seen in the table, wash trading activity for different pair contract addresses or tokens behaves differently. I picked these as examples to showcase the variety of forms of wash trading that could

Table 2: Examples of Wash Traded Coins on Pancake Swap for the 6-Hour Window Time Frame

	Type	Name of Token	Position Ratio	Percentage of Volume Wash Traded	Number of Wash Trader Addresses
a.	1st	Staked Shiba Inu	1.0509	93.37%	1
b.	2nd	Amaten	1.0743	77.37%	13
c.	2nd	HI	0.8801	13.27%	10
d.	2nd	Ginoa	0.9189	73.55%	3

be found on Pancake Swap only. Some of these tokens are more popular than others, but based on Figure 5, Figure 6, Figure 7, and Figure 8 in Section 4.1: Graphs, the tokens follow similar patterns of wash trading, with traders purchasing at higher prices and selling at lower prices. In other words, wash traders are attempting to lower the price while increasing volume. The graphs enhance comprehension of how wash trading is conducted and justify the method used to detect and quantify this illegal activity.

The x-axis of each graph reflects the time points at which the swaps occurred, while the y-axis represents the relative price of the tokens or stable coins used in the exchange. In addition, green bubbles reflect wash traders' buys of the corresponding token or stable coin shown on the y-axis, whilst red bubbles represent their sales. The green and red crosses in the graphs represent the same relationship for the other transactions analyzed. Moreover, the relative sizes of the bubbles and crosses signify swap sizes.

After running the algorithm and collecting the results from all pair contract addresses, the final total volume wash traded on Pancake Swap for the selected time frame was only **0.0000003958%**. Nonetheless, this is a noteworthy finding because wash trading is more widespread towards the beginning of a coin's life cycle when it is first deployed. Eventually, wash trading could be used to regain some of the traction that was lost due to shifting crypto market trends.

4 Results and Discussion

No research is available that might be utilized to validate the results. However, because it is a relatively new crypto asset, soon, further research may support or refute the statements made in this study. Indeed, the approach is not flawless, but this research provides a fantastic starting point for detecting and quantifying malicious and illegal activities on AMM DEXs. In addition, as previously stated in the paper, there are several limitations, including the detection of wash trading where none was present, the inaccuracy of the chosen approach in identifying all the

addresses that executed wash trading, and the existence of more complex types of wash trading events that have not been analyzed in this research paper.

4.1 Graphs

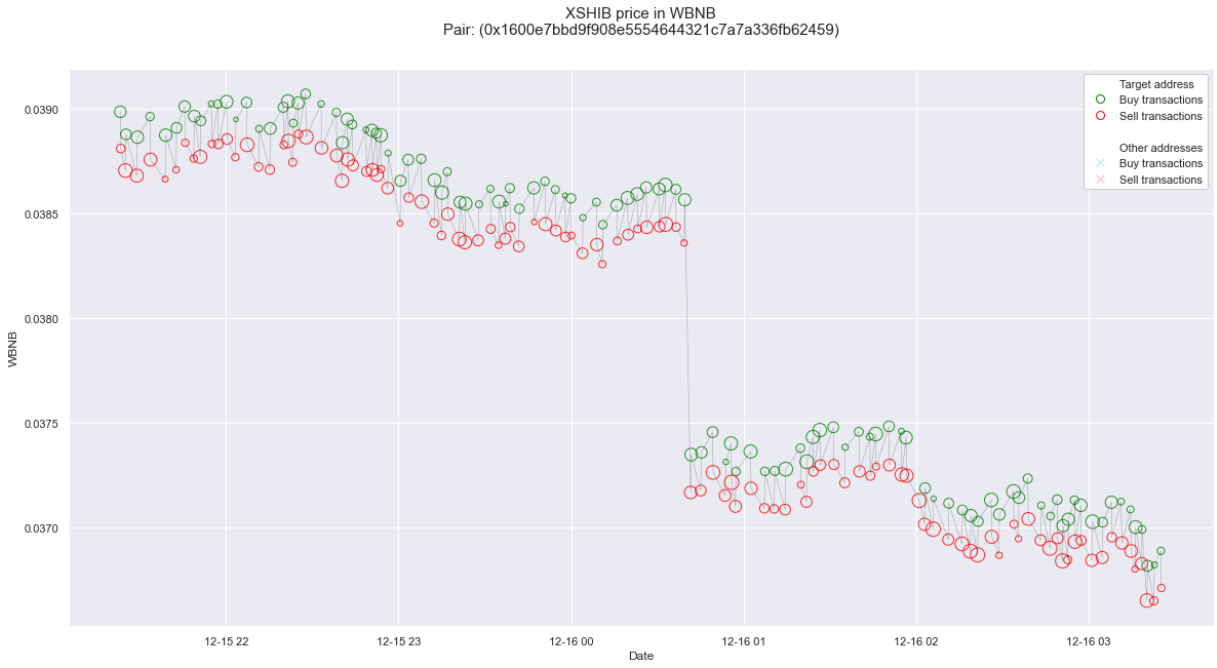

Figure 5: Staked Shiba Inu Token's Wash Trading Activity Graph

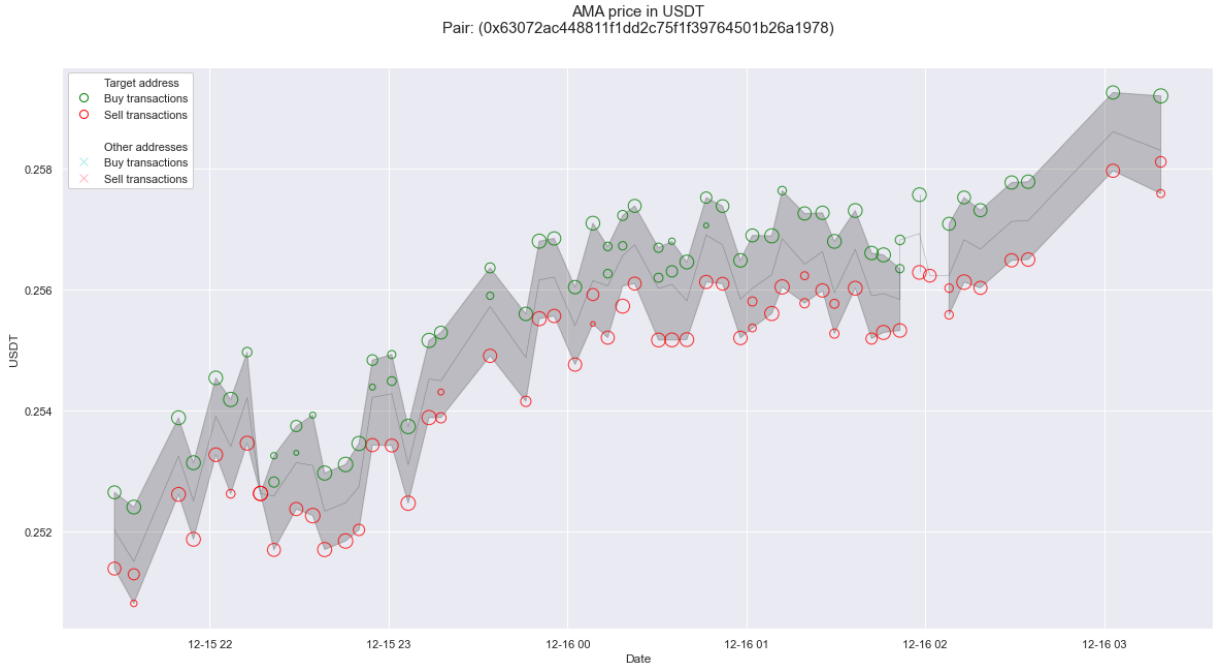

Figure 6: Amaten Token's Wash Trading Activity Graph

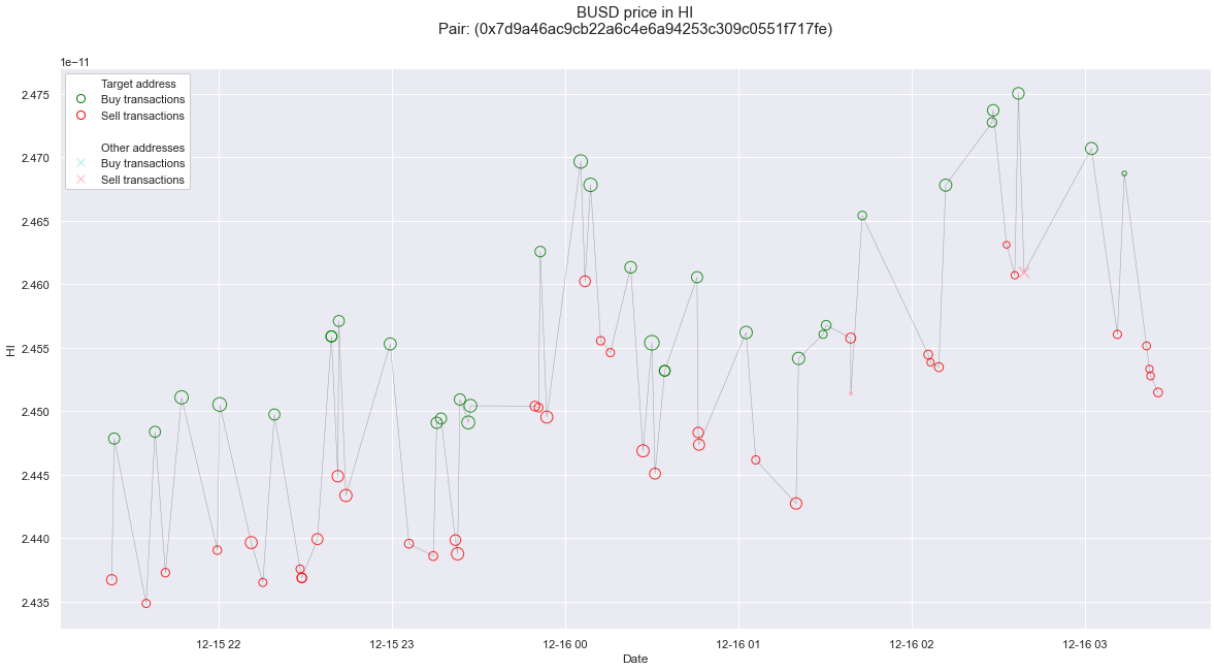

Figure 7: HI Token's Wash Trading Activity Graph

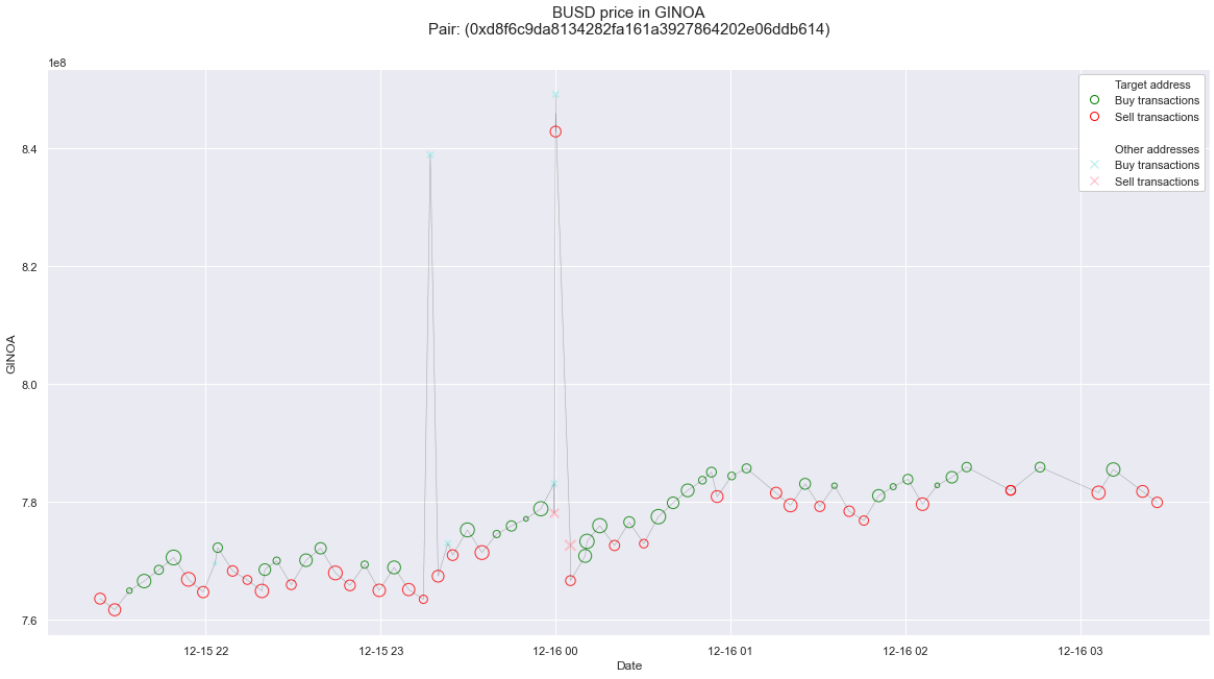

Figure 8: Ginoa Token's Wash Trading Activity Graph

4.2 Github Repository

`https://github.com/Heractos/Data-Science-Capstone.git`

5 Conclusion

In conclusion, this study successfully detected and quantified wash trading with significant results. Even though it captured only a small portion of possible wash trading on Pancake Swap AMM DEX, 0.0000003958 percent of the total volume over 6 hours is a fairly significant outcome. In addition, the study discovered the types and patterns of wash trading detected on Pancake Swap. In addition, the research presents four scenarios that represent two of the three types of wash trading, together with their associated graphs. The results were displayed in Table 2. The table depicts the quantity of wash trading that occurred on specific token pair contract addresses and identifies the number of accounts that engaged in this illegal activity. Implementing more advanced machine learning algorithms could improve the accuracy of the results if the work is expanded.

References

[1] G. L. Pennec, I. Fiedler, and L. Ante, "Wash trading at cryptocurrency exchanges," *Finance Research Letters*, vol. 43, 2021. [Online]. Available: https://doi.org/10.1016/j.frl.2021.101982

[2] L. Cong, X. Li, K. Tang, and Y. Yang, "Crypto wash trading," *arXiv preprint arXiv:2108.10984*, 2021. [Online]. Available: https://arxiv.org/abs/2108.10984

[3] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," *Proceedings of the Web Conference 2021*, 2021. [Online]. Available: https://arxiv.org/abs/2102.07001

[4] Commodity Futures Trading Commission. Commodity Exchange Act Regulations, 2020. [Online]. Available: https://www.cftc.gov/LawRegulation/CommodityExchangeAct/index.html

[5] M. L. Morgia, A. Mei, F. Sassi, and J. Stefa, "The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations," *CoRR*, 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2105.00733

[6] P. Fratrič, G. Sileno, S. Klous, and T. van Engers, "Manipulation of the bitcoin market: an agent-based study," *Financ Innov*, vol. 8, 2022. [Online]. Available: https://doi.org/10.1186/s40854-022-00364-3

[7] W. Cui and C. Gao, "Wteye: On-chain wash trade detection and quantification for erc20 cryptocurrencies," *Blockchain: Research and Applications*, 2022. [Online]. Available: https://doi.org/10.1016/j.bcra.2022.100108

[8] "Introducing IDEX v3 Hybrid Liquidity - The Solution to DeFi's Failed Trades, Slippage, Front-Running," 2021. [Online]. Available: https://blog.idex.io/all-posts/introducing-hybrid-liquidity

[9] D. Amiram, E. Lyandres, and D. Rabetti, "Competition and product quality: Fake trading on crypto exchanges," *SSRN Electronic Journal*, 2020. [Online]. Available: https://dx.doi.org/10.2139/ssrn.3745617

[10] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *CoRR*, vol. abs/2112.06089, 2021. [Online]. Available: https://arxiv.org/abs/2112.06089

[11] Z. Zhou, M. Wang, C.-N. Yang, Z. Fu, X. Sun, and Q. J. Wu, "Blockchain-based decentralized reputation system in e-commerce environment," *Future Generation Computer Systems*, 2021. [Online]. Available: https://doi.org/10.1016/j.future.2021.05.03