# Detecting Rug Pulls in Decentralized Exchanges: The Rise of Meme Coins

Alisa Kalacheva[a,b], Pavel Kuznetsov[c], Igor Vodolazov[d], Yury Yanovich[a,e]

[a] *Skolkovo Institute of Science and Technology, Moscow, Russia*
[b] *Moscow Institute of Physics and Technology, Moscow, Russia*
[c] *Moscow State University, Moscow, Russia*
[d] *Independent Researcher, Barcelona, Spain*
[e] *Faculty of Computer Science, HSE University, Russia*

**Abstract**

The surge in cryptoasset valuations and the expansive landscape for their inception have spurred a surge in illicit activities within the market. Decentralized exchanges (DEX) have facilitated trading with a wide array of tokens, even in scenarios of limited liquidity. Fraudulent practices manifest diversely, encompassing counterfeit tokens, rug pulls, and pump-and-dump schemes, all sharing a common thread of lacking functional innovation and relying heavily on aggressive social media and messenger marketing tactics. This study represents a critical stride towards the identification and profiling of deceitful tokens on DEX platforms. Our approach involved compiling data on new tokens spanning multiple years from the Ethereum blockchain, alongside tracking all associated purchase and sale transactions. Our analysis revealed that Uniswap V2 predominantly hosts the trading of new tokens, with an alarming discovery that over 98% of tokens minted daily exhibit fraudulent characteristics. Subsequently, a machine learning model was constructed to forecast the likelihood of a rug pull occurring shortly after trading commencement. The findings underscore the imperative nature of identifying fraudulent activities and stress the necessity for collaborative efforts between decentralized exchanges and regulatory bodies to mitigate financial losses experienced by investors.

*Keywords:* Decentralized Exchange, Scam Detection, Blockchain, Machine Learning, Ethereum

## 1. Introduction

In recent years, the rapid development of blockchain [1, 2], web3 technologies [3], and decentralized finance [4] has led to significant growth in the market capitalization of cryptocurrencies. According to CoinMarketCap analytics [5], as of May 2024, the market capitalization of cryptocurrencies has surpassed 2 trillion US dollars.

Emerging technologies within the web3 ecosystem include decentralized autonomous organizations (DAOs) [6, 7, 8], decentralized applications (dApps) [9], and a plethora of tokens following various standards [10, 11, 12]. To streamline token interactions and provide an alternative to peer-to-peer transactions, cryptocurrency exchanges and trading platforms have been established. These platforms generally fall into two categories: centralized exchanges (CEX) [13] and decentralized exchanges (DEX) [14]. While CEXs operate under a traditional financial model requiring intermediaries for transactions, DEXs leverage smart contract logic and mathematical rules for liquidity provision, ensuring asset reliability through cryptography.

Despite its potential, blockchain technology remains vulnerable to numerous fraudulent attacks [15]. According to the Chainalysis re-

*Email addresses:* {Corresponding author*}{alisa.kalacheva@skoltech.ru} (Alisa Kalacheva), pavelkuznetcov2002@gmail.com (Pavel Kuznetsov), inventandchill@protonmail.com (Igor Vodolazov), y.yanovich@skoltech.ru (Yury Yanovich)

port [16], fraudulent schemes, hacks, and exploits led to cryptocurrency users losing around 4.2 billion dollars in 2022 and approximately 2 billion in 2023. Without the implementation of robust regulatory measures to combat such fraud, these figures are likely to escalate further.

Among the most prevalent fraudulent schemes in blockchain technologies, the following stand out:

1. **Hacks.** Hacks can be carried out in multiple ways, such as exploiting smart contracts and planting malicious software on users' devices to siphon funds from crypto wallets. One notorious example is WeSteal, a Python program that scans for strings linked to wallet addresses copied to the clipboard [17].
2. **Deceptive Applications and Websites.** This common ploy involves websites that prompt users to authenticate using a web3 wallet. Unwittingly, users sign transactions on these sites, inadvertently transferring funds to scammers.
3. **Fraudulent ICO Schemes.** During the peak of 2017, fraudulent ICO schemes raised investments for products that were never realized [18]. Presently, a similar trend persists with meme coins [19], which lack technological innovation and rely on social media promotion and shilling (where paid supporters deceive people into risky investments).

In the realm of decentralized finance (DeFi) [20], the Rug Pull scheme prevails, wherein token creators drain liquidity essential for maintaining the token's value [21]. This scam typically unfolds with the developer selling off liquidity when the token price peaks, leading to a drastic drop in value, often plummeting to zero. The decentralized nature of trading on DEXs, coupled with lax regulations, exposes exchanges to various fraud schemes tied to token supply and demand.

Uniswap [22], one of the largest decentralized exchanges, has recorded a monthly trading volume exceeding 50 billion US dollars and over 2 trillion US dollars throughout its trading history. Despite its success, numerous instances of fraud have been identified on the Uniswap platform, ranging from Rug Pulls to fake tokens. Discussions are ongoing regarding the establishment of a registry for token names/symbols to ensure uniqueness.

Fraudsters leverage social networks and messaging platforms to lure investors into purchasing tokens. By artificially inflating prices through temporary spikes, they cultivate trust and deceive unsuspecting investors. This frenzy around meme coins mirrors the ICO bubble of 2017, where developers lacking technical acumen managed to attract significant capital and achieve explosive growth in ICO capitalization. Meme coins are a type of cryptoasset that prioritize community engagement over utility, raising funds from a large number of individuals rather than big investors [19]. They often have large supplies, resulting in prices with many zeros after the decimal point. While technically most meme coins are not native cryptocurrencies for blockchain networks, but rather tokens on top of existing ones, we still refer to them as coins due to established convention.

This study delves into the detection of fraudulent activities within meme coins, aiming to address the challenges posed by the ever-evolving cryptocurrency market and the introduction of novel financial instruments. Existing models and analysis techniques often fall short in capturing the unique characteristics of meme coins.

The research is centered around investigating meme coin bubbles and presents a predictive model aimed at forecasting token behavior on decentralized exchanges. In particular, the study focuses on recently launched tokens on the Uniswap V2 DEX [23] within a specified time frame. It utilizes trading data analysis and machine learning techniques to improve detection abilities.

The rest of the paper is organized as follows. Section 2 provides a background with a focus on meme coins and rug pulls. Section 3 offers an overview of related work in the field. Section 4 introduces our approach. Firstly, we discuss the dataset utilized in subsection 4.1 and the process of generating additional attributes in subsection 4.2. Following this, we present an overview of the dataset in 4.3, focusing on Uniswap V2

popularity growth in subsection 4.4 and liquidity pools that were used in subsection 4.5. The experiment section in Section 5 begins by outlining the problem our machine learning model addresses in subsection 5.1, providing details on the data collection process, paying special attention to the token labeling and preprocessing techniques employed in subsection 6.2. In Section 6, a quantitative analysis of the classification models is conducted, highlighting key input features of the model in subsection 6.2, and discussing the possible economic impact in subsection 6.3. Finally, Section 7 provides concluding remarks for the paper.

## 2. Background

This section provides brief background information on the evolution and current state of blockchain technology and cryptocurrencies, as well as the emergence and impact of meme coins on the cryptocurrency market.

### *2.1. Blockchain and cryptocurrencies*

The concept of distributed systems and decentralisation began to emerge at the end of the 20th century, with research focusing on consensus and various protocols [24, 25]. A significant step forward was made in 2008, when Satoshi Nakamoto introduced the world to the first cryptocurrency– the Bitcoin [1]. This showed the world the practical use of this technology and marked the beginning of the rapid development of the blockchain and, in particular, of cryptocurrencies.

Today, cryptocurrencies have a general definition of digital currencies within blockchain ecosystems, utilizing cryptography for security. A token, in this context, is a digital representation of an IOU (I owe you) concept, designed with anti-counterfeiting technologies to deter replication [26, 27]. These tokens symbolize specific assets or utilities and typically operate on blockchain platforms, facilitating secure transactions and interactions within digital ecosystems.

In recent years, the cryptocurrency market landscape has undergone a significant transformation that has been driven by the growing interest in meme coins [19]. A meme coin is a type of cryptocurrency that often lacks technological innovation, but gains popularity through internet culture and social media hype. The simplicity of creating new tokens and the excitement surrounding blockchain technology have led to the rise of this new class of cryptocurrency. Meme coins are often promoted through social media, mentions in large communities or celebrity endorsements.

Currently, the market capitalisation of meme coins has reached USD 55 billion, out of a total market capitalisation of over USD 2.4 trillion for all crypto assets [28]. A unique feature of meme coins is that they tend to be in high supply. For example, the popular Shiba Inu (SHIB) coin is the second largest meme coin by market capitalisation and ranks 12th among all cryptocurrencies. Its total supply is 1 trillion coins, leading to significant price volatility over short periods of time. Unlike traditional cryptocurrencies, meme coins are strongly influenced by trends and social factors. A prominent example is Dogecoin (DOGE), the most popular meme coin, which is often associated with Elon Musk.

The high volatility of meme coins attracts many speculative strategies and investors looking for significant short-term gains. More established tokens tend to slow down in price growth over time, prompting speculative investors to turn to newer assets.

### *2.2. Meme Coins Bubble*

Every day, hundreds of new contracts are created on the Ethereum network [2] implementing ERC-20 tokens [10], many of which are subsequently traded on DEX [14]. A significant number of these contracts are fraudulent; even if the smart contract code itself does not explicitly indicate fraud, it cannot fully prevent rug pulls – a scheme where token creators withdraw liquidity at an appropriate time [21].

While not all issued memecoins are fraudulent, they often lack technological and functional uniqueness. However, due to the speculative interest they generate, these tokens can become popular. For example, the price of the TARD coin (an ERC-20 token) has increased twenty-fold

since its creation. There are many similar cases where investors are looking to exit their positions before a broader sell-off occurs.

The current activity around memecoins mirrors the initial coin offering (ICO) surge of 2017, where many startups attracted investment through ICOs – a process similar to an initial public offering (IPO), but largely unregulated at the time. This led to an ICO bubble in which projects lacking development plans or the necessary expertise, and sometimes even outright scams, quickly raised millions of dollars [18]. Some studies suggest that more than 80% of ICOs eventually turned out to be fraudulent[29]. The memecoin situation is exacerbated by the ease and speed with which these tokens can be created, and the lack of legal protection for investors.

### *2.3. Crypto Scams*

The growing interest in the Ethereum blockchain and its associated tokens has attracted not only speculative investors but also a significant number of scammers, who often employ similar tactics. Common fraudulent methods include fake ICOs, Ponzi schemes, counterfeit tokens, backdoors in smart contracts, and, most frequently, rug pulls [30]. Rug pulls specifically involve the removal of liquidity from a token, rendering it worthless.

In the case of meme coins, the scheme typically unfolds as follows: anyone can create both the token and the liquidity pool on platforms like Uniswap without any verification, which poses considerable risks to memecoin investors. The developer deploys a meme token and, as the sole owner, creates a Uniswap pool for the meme coin-ether (ETH) pair, contributing the entire supply of the meme coin along with a fixed amount of ETH (usually 2 units) into that pool. In return for adding assets to the pool, the developer receives liquidity tokens, which allow them to convert those liquidity tokens back into meme coins and ETH at any time–essentially giving them the ability to extract liquidity.

Other users then trade the meme coin and ETH within the pool based on the decentralized exchange's automated market maker [31]. The developer earns exchange fees from each transaction, which serve as their income since a portion of these fees is denominated in ETH, holding value beyond the pool itself. However, since the developer is typically the main—and often the only—owner of the liquidity tokens, they can withdraw liquidity at will. This option for a rug pull makes it impossible for others to trade in that token pair. Consequently, as the developer extracts ETH from the pool, interest in the meme coin plummets, and no one is willing to trade it at favorable rates.

## 3. Related Work

Considerable research has focused on blockchain fraud, particularly schemes that are prevalent in token trading. Several studies have examined fraudulent schemes associated with initial coin offerings (ICOs) [32, 33, 34]. For example, regression analysis showed that tokens listed on exchanges, previously a sign of successful ICOs, had a higher incidence of fraud, around 10.1% [35]. These findings are significant as the situation with meme coins bears similarities to the ICO bubble and is susceptible to similar attacks and fraudulent schemes.

Numerous studies have focused on blockchain Ponzi schemes, with claims that there are at least 400 such cases on the Ethereum blockchain [36, 37]. Evidence suggests that the most successful scams were supported by significant contributions from a small number of victims [38].

Exchanges and the tokens traded on them are also identified by the researchers as a primary vulnerability. Tokens with potential backdoors in their code are considered to be particularly dangerous. Various analysis tools are currently available [39, 40, 41]. They can be applied to both centralised exchanges (CEX) and decentralised exchanges (DEX).

The cryptocurrency market is vulnerable to external manipulation. The main principles of market vulnerability are outlined in the book "Fraud and Corruption in Financial Markets: Malpractice, Misconduct and Manipulation" [42]. The authors highlight factors such as inconsistent reg-


Figure 1: Example of Rug Pull Scam: BIDEN/WETH on Uniswap

ulation, comparative anonymity, low barriers to entry and the lack of rigorous procedures for setting up exchanges. Exchange vulnerabilities account for a significant portion of cryptocurrency fraud. Between 2011 and 2017, 18 exchanges trading tokens were shut down due to fraud [43].

Uniswap, one of the largest exchanges that allows the trading of any token on the Ethereum blockchain, has been the subject of an investigation into 'fake' tokens. Fake tokens use names identical to major existing projects but have different contract deployment addresses. It is estimated that around 50% of tokens launched on Uniswap are fraudulent, resulting in losses of up to $16 million [43]. Previous research [44] reported that most counterfeit tokens on Uniswap have minimal transaction activity, with 90% having less than 45 transactions, estimating total fraud at $17 million.

The rug pull scheme has been studied by Bruno Mazorra [21], who analysed 28,000 tokens on Uniswap V2, 98% of which were flagged as fraudulent in the data. Their methodology sets up the task of time-series analysis using machine learning by evaluating token price drops. This work is crucial for the experiment discussed below, as despite the same research question, different methods and approaches are used. Based on this study [21], several other papers have been published, modifying and extending the proposed approach [45].

The paper [30] constructed its own dataset comprising 7,000 tokens on Uniswap V3. The authors emphasize the significance of incorporating on-chain data, time-series features, and automated labeling mechanisms. They address the development of scam detection models tailored for various time windows. While larger time windows enhance model accuracy, it is crucial to consider smaller time windows to prevent delayed scam identification post-rug pull incidents. The authors confirm that rug pull incidents on Uniswap V3 occur soon after token creation, similar to the pattern observed on Uniswap V2.

All the mentioned studies deal with data before early 2023. The cryptocurrency market is highly volatile and rapidly changing; hence, these studies did not capture the surge in meme coin activity and did not explore this phenomenon.

The new phenomenon of meme coins is covered in only a few articles [19, 46, 47]. Most often they focus on qualitative analyses or searching for trends and correlations, trying to explain economic events and relationships, and answering the question of how meme coins will affect the existing cryptosystem.

## 4. Methodology

### *4.1. Dataset*

For this research, data was collected using Bitquery, a tool designed for querying and analyzing blockchain transactions. This tool provided information on the creation of new ERC-20 tokens,

transactions on decentralized exchanges, the establishment of liquidity pools, and trading activity (Table 1).

To identify trends and peaks in token market activity, data on all ERC-20 standard tokens created between May 2020 and February 2024 was collected. Key features such as the time of token creation (timestamp and block height of the transaction), the address of the created token and its creator, the token standard and its decimal representation, and the transaction hash were obtained using the Bitquery API.

However, not all created tokens enter decentralized exchanges for trading. For instance, to get onto the Uniswap exchange, an event such as the creation of a pair (Uniswap V2) or the creation of a pool (Uniswap V3) must occur. In Uniswap V2, a pair corresponds to a liquidity pool, whereas in Uniswap V3, multiple pools with different fee structures can exist. We hypothesize that new tokens are predominantly traded on the second version of the Uniswap protocol, which will be examined further.

Therefore, information about all created pairs on Uniswap V2 was collected for the same time period 2020-2024. This dataset includes the address of the newly created pair, the addresses of the tokens in the pair, the timestamp, the block number, the transaction hash and the address of the liquidity pool creator. Furthermore, a dataset of all transactions made during 2023 and 2024, the years when memecoin trading activity was found to peak, was acquired. The data includes details of token movements, including amounts exchanged, addresses involved, transaction time and initiating user address.

The study of flash bots in acquiring newly minted tokens is particularly relevant. These bots automate trading activity on exchanges, allowing users to specify a preferred tip (reward) amount to validators for expedited inclusion in the block. This mechanism allows meme coin investors to prioritize their transactions, potentially increasing their returns. Among the services investigated, Banana Gun stands out as a prominent example, with its first transaction occurring on December 4, 2023, marking the outer boundary of our dataset.

Fraudulent tokens often use similar smart contracts with minor modifications. Detecting such cases can be facilitated by calculating checksums. Although there is no standardized method for this calculation, the process typically involves obtaining a list of smart contract methods, applying a hash function, and extracting the first 4 bytes of the result. However, fraudulent tokens often do not publish their code, precluding access to a public methods list. In this study, the TUFExtractor tool was used to get token checksums, addressing this challenge.

### *4.2. Additional Attributes Generation*

Following the creation of the dataset, novel features theorised to influence the likelihood of fraudulent activity were derived. Using the collected data, a time interval of approximately 5 minutes was calculated as appropriate for predicting token behaviour in subsequent trading hours. Consequently, for each new token traded alongside WETH, the trading characteristics observed within the first 5 minutes of the exchange debut were calculated:

Features were selected based on their potential impact on fraud detection, whether positive or negative. For example, a low volume of token sales could indicate limited selling opportunities, thereby inflating token prices and attracting more buyers, ultimately leading to a rug-pull scenario. By analysing data from new token release dates, spikes in fraudulent token activity in the market can be identified.

The checksum parameter is derived from a unique hash of the smart contract code. A perfect match in the smart contract code, even with different variable names, raises suspicion of fraudulent activity. It is also crucial to distinguish between fraudulent tokens and those that merely replicate a similar smart contract structure. To make this distinction, data was obtained on the prevalence of tokens with matching checksums in the rug pull.

| New tokens | Liquidity Pools | DEX Transactions | Banana Gun Activity |
|---|---|---|---|
| block.height | pair | protocol | amount |
| block.time-stamp.time | token0 | buyAmount | external |
| smartContract.-address.address | token1 | sellAmount | block.timestamp.-time |
| smartContract.-currency.decimals | block.timestamp.-time | block.timestamp.-time | block.height |
| smartContract.-currency.to-kenType | block.height | block.height | sender.address |
| transaction.hash | transaction.hash | smartContract.-address.address | receiver.address |
| transaction.-txFrom.address | transaction.-txFrom.address | buyCurrency.address | receiver.smartContract.contractType |
| | | sellCurrency.address | currency.address |
| | | transaction.hash | transaction.hash |
| | | transaction.tx-From.address | transaction.tx-From.address |

Table 1: Table of data fields collected from Bitquery

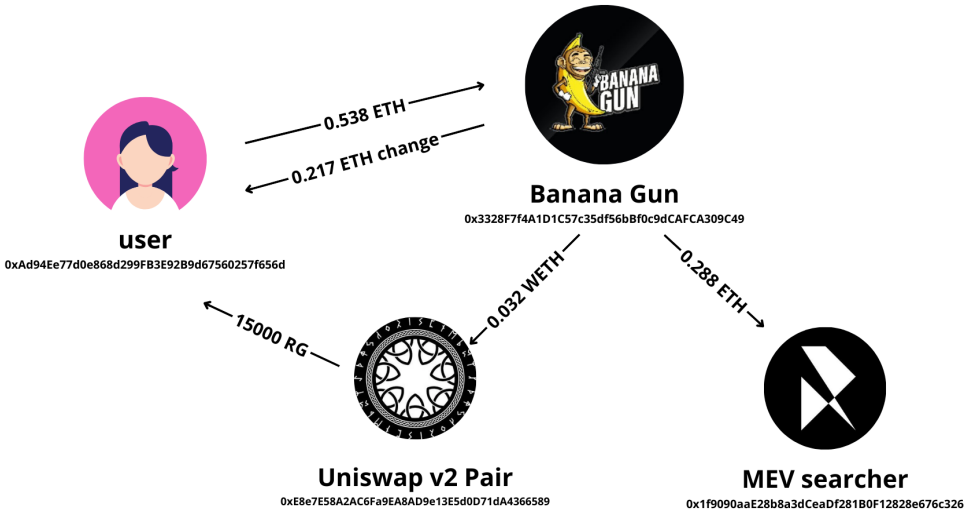



Figure 2: Banana Gun Interaction Scheme

### *4.3. Dataset Overview*

From the launch of Uniswap V2 in Spring 2020 to February 2024 inclusive, approximately 965,000 tokens were issued (see Figure 3). Despite a significant peak in October 2022, this spike is an outlier: over 47,000 new tokens were issued by a single address, with 89% of users issuing only one token each that month.

However, not all these tokens will appear on the decentralized exchanges. Data collected indicates that around 335,000 tokens were issued between 2023 and 2024, of which 177,000 were traded on Uniswap V2. When analyzing liquidity pools, such outliers are absent — the number of

| Feature | Description |
|---|---|
| count_tx | Number of all token transactions at the time of data collection |
| purchase_percentage | Percentage of token purchase transactions |
| sale_percentage | Percentage of token sale transactions |
| unique_buyers | Number of unique purchasers of the token |
| unique_sellers | Number of unique sellers of the token |
| total_eth_value | The total amount of WETH traded in all token transactions |
| sell_eth_value | Total amount of WETH sold in all token transactions |
| price_change_first_to_3_blocks | Price change from the start of trading to the price after 3 blocks |
| price_change_first_5min | price change from the start of the trade to the time of data collection |
| eth_volume_block_1 | Total amount of WETH traded in the first trading block |
| sell_eth_volume_block_1 | Total amount of WETH traded in the first trading block |
| tx_block_1 | Number of transactions in the first bidding block |
| creation_month_sin | Month of token creation (cyclic coding) |
| creation_month_cos | Month of token creation (cyclic coding) |
| creation_year | Year of token creation (bool) |
| decimals | Decimal representation of the token |
| checksum_count | Number of tokens previously created with this checksum |
| checksum_rug | Percentage of fraudulent tokens previously created with this checksum |
| tax_buy | Commission on token purchases |
| tax_sell | Commission to sell a token |
| creation_trade_delta | Time elapsed from token creation to the start of trading |
| creation_pool_delta | Time elapsed from liquidity pool creation to the start of trading |
| is_pool_creator | Equality of addresses of token creator and pool creator (bool) |
| supply | Initial supply of tokens |
| initial_price | Initial price of the traded pair |
| average_rsi | Average relative strength index |
| std_rsi | Standard deviation of the relative strength index |
| max_bribe_first_block | Maximum reward to the validator in the first block of trades |
| mean_bribe_first_block | Average reward to the validator in the first bidding block |
| count_bribes_first_block | Number of bribes to the validator in the first bidding block |
| unique_bribes | Number of unique users who have paid rewards to the validator |

Table 2: Table of attributes of the final dataset to be analysed

unique users and created liquidity pools are nearly identical. Among the 162,000 liquidity pool creators, only 113 issued more than 10 tokens to the exchange. This does not imply that these 113 individuals are responsible for fraudulent tokens, while the rest are "honest". In fact, fraudsters often use an address only once before creating a new one.

### *4.4. Uniswap Growth*

Before selecting the data for study, decentralized exchanges were analyzed to determine where fraudulent tokens are most actively traded. Trading volume, the number of transactions for each exchange, and the number of tokens traded were obtained. It is hypothesized that due to the existing commission system, it is more profitable for fraudsters to create tokens on

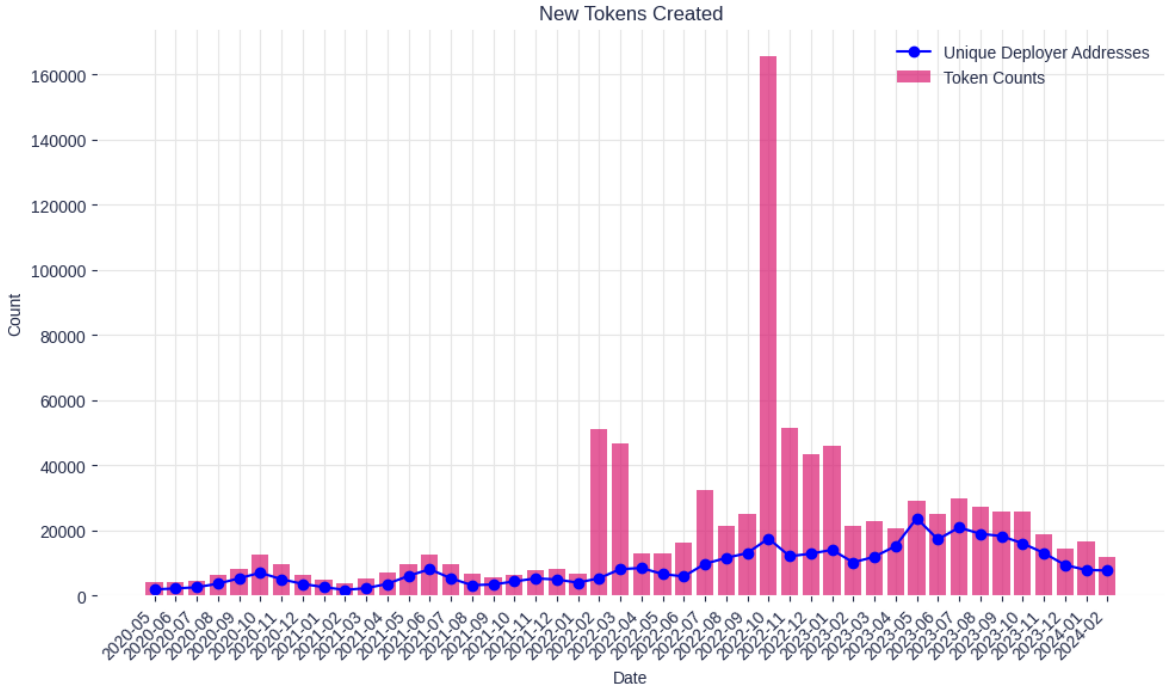



Figure 3: New Tokens Created Over Time

Uniswap V2 rather than the third version of the protocol. This is primarily due to the protocol mechanics: Uniswap V3 the focus is on managing concentrated liquidity, and in the case of fraud the price spread is extremely high, making this approach inefficient. Additionally, Uniswap V3 does not permit token trading where the buy/sell commission is included in the smart contract.

An analysis of trade data from different versions of the Uniswap protocol, aggregated by month (see Figure 4), reveals significant market changes. The year 2022 was particularly unfavorable for cryptocurrencies, often referred to as "Cryptowinter 2022," associated with rising global inflation, which led investors to sell risky assets. Key events in May (the collapse of Luna and TerraUSD projects) and November (the collapse of FTX) had substantial impacts on the cryptocurrency industry and continue to influence it, particularly regarding regulatory measures.

Among the data collected on all token transactions across various decentralized exchange protocols for February 2024, Uniswap dominates with 98.1% of the market, compared to 1.9% of transactions on other exchanges (see Figure 5). The next most popular exchanges are Balancer V2, PancakeSwap V3, and Zerox Exchange V4.

Filtering transactions to include only new tokens (with a lifecycle of less than 14 days) shows that 99.9% of these tokens are traded on Uniswap, predominantly on the second version of the protocol. Figure 6 shows that the proportion between the protocol versions is not maintained, which means that its greater activity cannot be attributed solely to its popularity. Among the remaining exchanges, Balancer v2 accounts for three-quarters of the market.

### *4.5. Liquidity Pools*

When a token is issued to an exchange, the creator adds liquidity to Uniswap by creating a pool consisting of two tokens. Although various pairings are possible, WETH (wrapped ether token, an ERC-20 protocol token with a 1:1 representation of ether) is the most commonly used. WETH has the greatest liquidity and is more resistant to price fluctuations, which enhances the accuracy of the study. Therefore, the analysis focuses exclusively on tokens traded on the exchange paired with WETH.

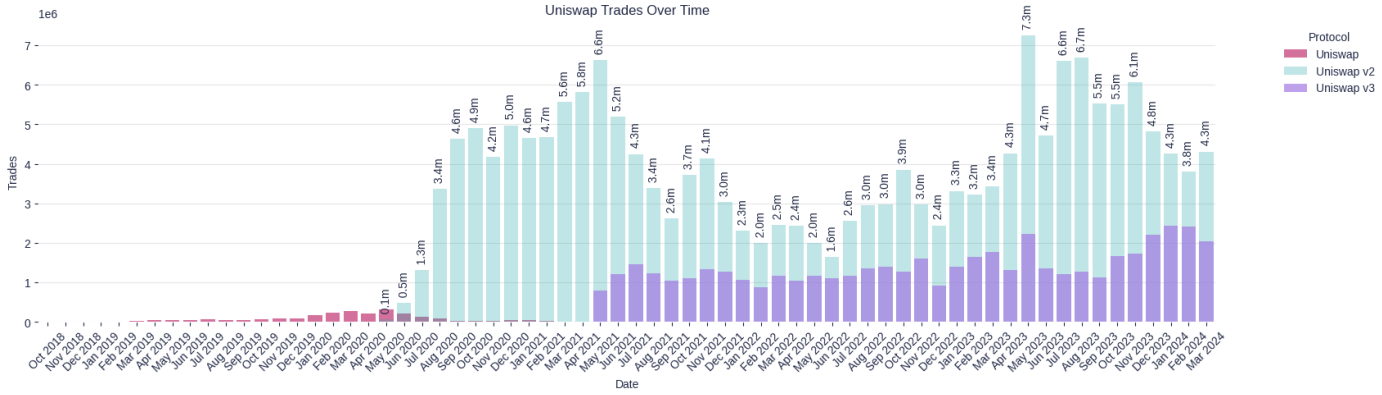



Figure 4: Uniswap Daily Trades Over Time

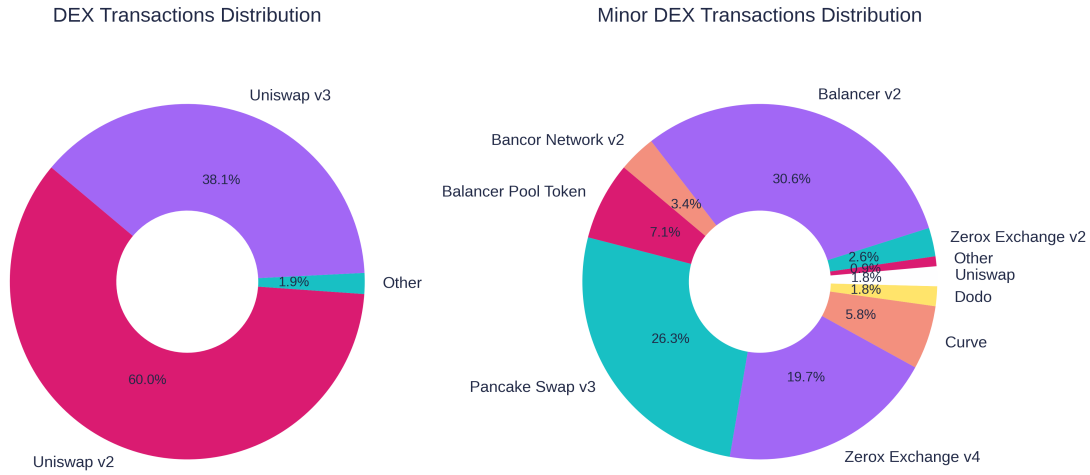



Figure 5: DEX Transactions Distribution

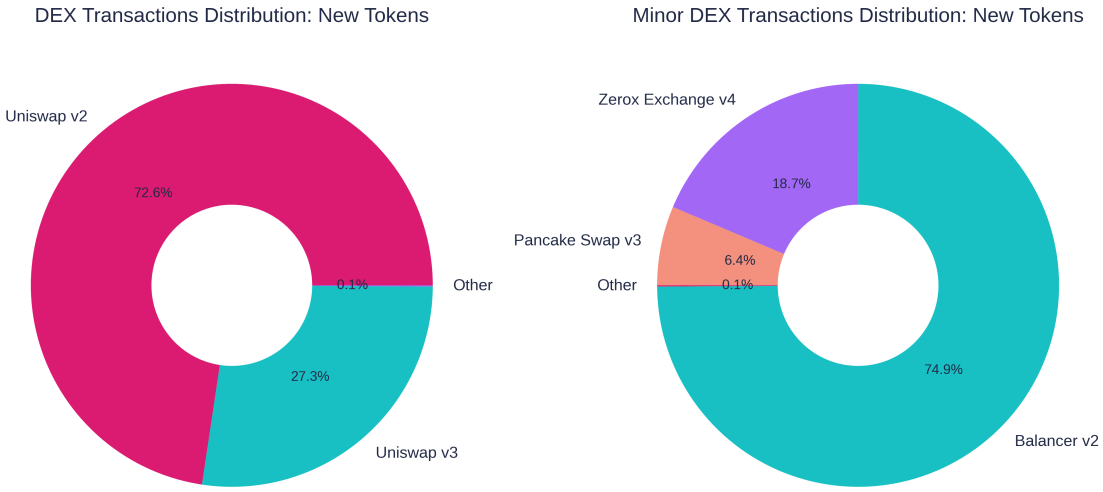



Figure 6: New Tokens Distribution

## 5. Experiment

The next section details the machine learning methods employed and compares the different models developed to address the problem.

### *5.1. Machine Learning Model Problem*

The primary task is not to determine whether a token is a rug pull, as over 98% of tokens have been identified as fraudulent based on maximum drawdown criteria [21]. The maximum drawdown is defined as $\texttt{MD} = \frac{X_{\min} - X_{\max}}{X_{\max}} < \varepsilon$, where $X_{\min}$ and $X_{\max}$ are the minimum and maximum liquidity/price correspondingly, and $\varepsilon = 0.01$ is a threshhold. Instead, the relevant challenge is to determine the time interval in which a potential rug pull may occur. One approach to this problem involves developing a machine learning model to predict the onset of a rug pull. This requires solving a binary classification problem where the target variable is 1 if the rug pull occurs within a specified time interval (e.g., within the next hour) and 0 otherwise. An activity-based approach is used to determine what constitutes a rug pull, assuming that a token that has been inactive for a period of time is flagged as suspicious. This approach does not impose restrictions on sharp price spikes of new tokens, given the high volatility of the cryptocurrency market in general. The model will enable investors to more accurately predict the lifetime of assets in their portfolio and assess risks when investing in new tokens.

### *5.2. Dataset Description*

The model input comprises a dataset with 30 features, described in Table 2, collected from November 2023 to February 2024. An external constraint is the launch of the Banana Gun tool in December 2023, with its first successful transaction on December 4. Consequently, the final dataset contains information about 7,633 tokens.

### *5.3. Data Preprocessing Techniques*

The following steps were taken to pre-process the data:

| Time interval, min | Percentage of rug pulls, % |
|---|---|
| 60 | 41.8 |
| 120 | 45.7 |
| 180 | 47.8 |
| 240 | 49.7 |
| 300 | 51.0 |
| 360 | 52.1 |
| 420 | 53.2 |

Table 3: Class balance for different time intervals

- **Correlation analysis**
  The correlations between the input features were examined, and a qualitative analysis of the data was conducted. Highly correlated features can lead to data redundancy, negatively affecting the model's performance.

- **Scaling of the data**
  The dataset contains values spanning a large range (e.g., the initial price set by the liquidity pool owner can vary by several orders of magnitude for different tokens). MaxAbsScaler was employed to scale the data, preserving relative relationships within the features.

- **Resampling**
  Although the sample is fairly balanced, resampling techniques can enhance the algorithm's accuracy and provide a better representation of each class in the training sample. Random Over-Sampling was used to increase the size of the original sample by randomly resampling elements of the smaller class.

## 6. Numerical Results

### *6.1. Classification*

Applying Recursive Feature Elimination (RFE) resulted in a slight improvement in the metrics, achieving an accuracy of 87.89%. This algorithm uses a recursive iterative process, each time training on a subset of features, selecting the least important ones for the model and eliminating them. In this case, the algorithm identified the following featuresfor elimination: creation_month_cos, is_pool_creator, and std_rsi.

In addition, the application of SMOTEEN 5 (Synthetic Minority Over-sampling Technique

| Metrics | Decision Trees | Random Forest | Gradient Boosting | AdaBoost | Extreme Gradient Boosting |
|---|---|---|---|---|---|
| Accuracy, % | 82.35 | 87.31 | 84.98 | 79.31 | 87.60 |
| Recall, % | 87.17 | 90.27 | 89.28 | 81.66 | 90.69 |
| Precision, % | 79.64 | 85.33 | 82.31 | 78.14 | 85.51 |
| F1 Score, % | 83.23 | 87.73 | 85.66 | 79.86 | 88.02 |
| ROC AUC Score, % | 82.33 | 87.30 | 84.95 | 79.29 | 87.58 |
| Best parameters | criterion: gini, max_depth: 27, min_samples_leaf: 1, min_samples_split: 2 | bootstrap: True, max_depth: 20, min_samples_leaf: 1, n_estimators: 200 | learning_rate: 0.5, max_depth: 5, min_samples_leaf: 1, n_estimators: 200 | learning_rate: 1, n_estimators: 200, | gamma: 0, learning_rate: 0.1, max_depth: 7, n_estimators: 200 |

Table 4: Comparison of metrics of applied models

| Metric | Over-Sampling | SMOTEEN | SMOTEEN full dataset performance |
|---|---|---|---|
| Sample size | X_train: 6630 X_test: 1658 | X_train: 2431 X_test: 608 | X_test: 7633 |
| Accuracy, % | 87.60 | 91.32 | 78.67 |
| Recall, % | 90.69 | 95.85 | 98.63 |
| Precision, % | 85.51 | 91.69 | 66.74 |
| F1 Score, % | 88.02 | 93.72 | 79.61 |
| ROC AUC Score, % | 87.58 | 88.87 | 81.36 |
| SMOTEENN settings | SMOTE(sampling_strategy=0.9, k_neighbors=5) EditedNearestNeighbours(sampling_strategy='auto', n_neighbors=3) | | |

Table 5: Using SMOTEEN in the Extreme Gradient Boosting model

with Editing), an Under-Sampling method, was considered. SMOTEEN combines SMOTE (Synthetic Minority Over-sampling Technique) and ENN (Edited Nearest Neighbors). This approach first generates synthetic elements of the smaller class and then removes noisy instances that differ from the majority of their neighbors. Despite the model's excellent performance on the out-of-sample data, the generalizing ability of the model trained with SMOTEEN on larger dataset was average. However, this model excelled in the recall metric, which is useful when identifying all fraudulent tokens is crucial, even if the number of false positives is higher than desired.

The Extreme Gradient Boosting model, trained and tested for different time intervals, yielded the highest F1-score. As depicted in Figure 7, the metric values decrease over longer time intervals, likely due to the easier identification of fraudulent tokens at the initial stage.

### *6.2. Key Features*

Identifying the characteristics of a new token that are most indicative of potential fraud is one of the goals of this paper. By calculating these features for a token that has just entered a DEX, the model can be used to predict how the token behaves in the market several hours ahead. Figure 8 shows the key features that had the most influence on the Extreme Gradient Boosting model. For example, the most significant feature for the model is the feature showing how much WETH was spent in all transactions collected in the 5 minutes of the token's existence. The 8b graph shows that the greater the turnover of WETH traded in a pair, the less likely it is to be fraudulent. The same conclusion can be drawn about the time of token release to the exchange. If the team announced the release of the token after it was created, did some work with the public or some other positive event that led to a delay in releasing the token to the exchange, then such a token is less likely to be fraudulent. The figures show

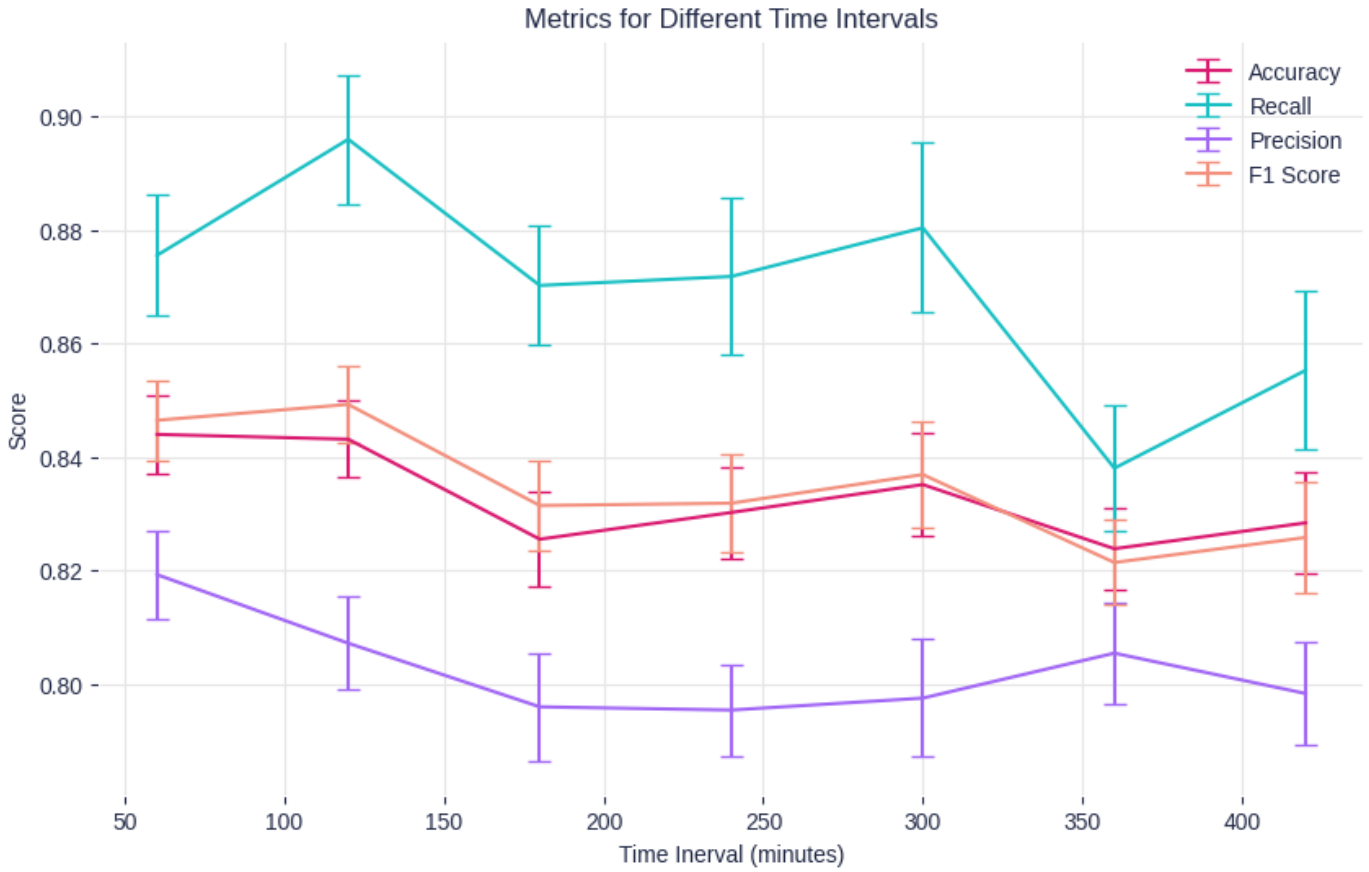



Figure 7: ML Scores for Different Time Intervals (Extreme Gradient Boosting)

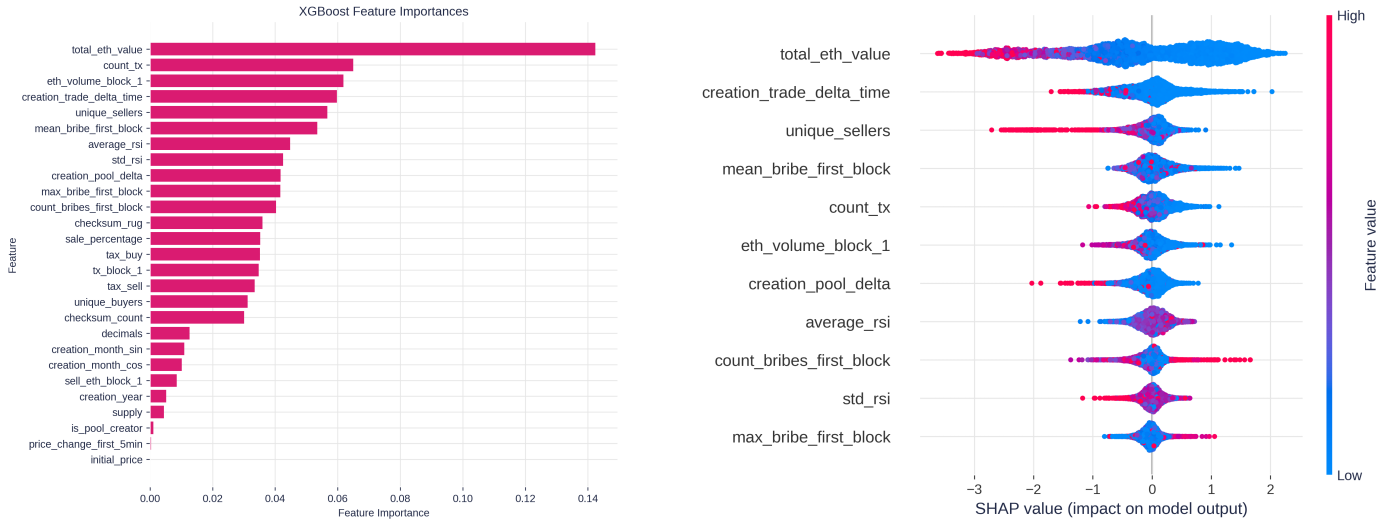
that fraudulent tokens are characterised by larger price jumps and a higher reward for the validator. This is most likely due to the fact that with such short-lived tokens, it is most important to get into the first block to be the first to buy and get out in time when the token price peaks. The information gathered provides a deeper understanding of which features have the greatest impact on the model and forecasts. However, it is important to note that these values were obtained for an experiment using the XGBoost model on randomly over-sampled data over an observation time interval of 3 hours, for other models the importance of the features will be different, but this does not affect the conclusions that can be drawn from the SHAP values.

### *6.3. Model Justification*

In order to assess the economic significance of the developed solution for cryptocurrency investors and the broader trading ecosystem, we propose to compare the profitability of two different investment strategies: one that involves investing in all issued tokens, and another that focuses exclusively on tokens deemed safe for investment by the model. This comparison will be an assessment of the profit and loss (PnL) of these two investment strategies on the basis of historical asset price data. The comparison of these two strategies is carried out as follows.

**Assumptions and Initial Setup:**

- We aim to invest 1000 WETH in $N$ tokens, distributing the initial investments evenly across the tokens.
- This setup results in a portfolio comprising $N$ assets, with each asset subject to the trading rules.




(a) Feature importance

(b) Shap values for top features

Figure 8: Key features in model training

**Trading Rules:**

1. **Stop-Loss Level:** A stop-loss level is set at 0.1. If triggered, all tokens are sold at the current price to minimize losses.
2. **Take-Profit Levels:**
   - At a profit level of 0.5, half of the tokens are sold, allowing the remaining tokens to continue trading.
   - At a profit level of 1.0, 75% of the remaining tokens are sold, with the rest continuing to trade.
3. **Final Sale:** All tokens are sold at the current price after $X$ hours. If a rug pull occurs before $X$ hours, all remaining tokens are considered lost.

The success of each strategy will be evaluated based on the overall profit and loss of the portfolio. By applying these rules and comparing the resulting PnL across the two strategies, we can assess the effectiveness of investing in all tokens versus selectively investing in tokens identified as safe by the model.

The PnL for two portfolios over a two-hour ($X = 2$) strategy interval was evaluated with an initial investment of 1000 WETH for each portfolio:

1. A portfolio of $N = 100$ random tokens issued between February 1, 2024, and February 10, 2024, traded on the exchange.
2. From these $N = 100$ random tokens, the model identified 89 tokens as safe for investment within the given time interval.

The results demonstrate that the strategy of investing in tokens identified for this time interval as safe by the model is 49% more profitable. The simulation results for other parameter sets are presented in Table 6.

| | Portfolio 1 | | Portfolio 2 | | | |
|---|---|---|---|---|---|---|
| N | Investment per token | PnL | Number of assets | Investment per token | PnL | Profit, % |
| 100 | 10.0 | 108.99 | 89 | 11.2 | 162.67 | 49.2 |
| 150 | 6.7 | 130.94 | 136 | 7.6 | 186.31 | 42.3 |
| 200 | 5.0 | 88.09 | 181 | 5.5 | 143.16 | 62.5 |
| 250 | 4.0 | 87.39 | 227 | 4.4 | 145.68 | 66.7 |
| 300 | 3.3 | 120.31 | 273 | 3.7 | 179.37 | 49.1 |
| 350 | 2.9 | 251.98 | 318 | 3.1 | 325.89 | 29.3 |

Table 6: Simulation results

## 7. Discussions and Conclusions

The pervasive use of social networks and messaging platforms by fraudsters to influence token prices and deceive investors echoes historical events such as the ICO bubble. Despite their vulnerability to fraudulent activities, meme coins have surged in popularity by prioritizing community engagement over utility. This study delves into the prevalence of deceptive practices within meme coins on decentralized exchanges, with a specific focus on Uniswap V2 as a key platform for new token launches.

The evolving landscape of token launches has witnessed a significant transformation, evident in the fluctuating patterns of monthly token introductions. The distinction between rug pulls and legitimate projects has become increasingly blurred, with a majority of tokens falling into the former category based on current classification standards. The central concern now revolves around predicting the timing of potential rug pulls rather than simply anticipating their occurrence. To address this paradigm shift, the study formulates a refined problem statement centered on binary classification to forecast the likelihood of a rug pull within a specified timeframe post-token inception.

Data for this investigation was meticulously sourced from Bitquery, a robust blockchain transaction analysis tool, to track ERC-20 token creation, decentralized exchange transactions, liquidity pool setups, and trading behaviors. The study primarily scrutinized tokens minted between May 2020 and February 2024, focusing on dissecting market trends by closely examining Uniswap V2 pairs and Uniswap V3 pools.

Additionally, the research delved into the impact of flash bots on acquiring newly minted tokens, with Banana Gun serving as a prominent case study. Detecting fraudulent tokens necessitated checksum calculations utilizing the TUFExtractor tool, particularly due to restricted public access to code for numerous suspicious tokens. Unique features were meticulously extracted from the dataset to predict the likelihood of fraudulent activities, with a specific emphasis on early trading behaviors observed within the initial 5 minutes post-token launch. These features were selected based on their potential influence on fraud detection, such as token sales volume and spikes in market activity coinciding with new token release dates.

Identifying an exact match in smart contract code checksums, despite variations in variable names, can serve as a red flag for potential fraudulent activities, emphasizing the critical need to differentiate between malicious tokens and those using similar contract structures. The data underscored a prevalence of matching checksums in rug pull scenarios.

The model analyzed a comprehensive dataset comprising 30 features collected between November 2023 and February 2024, encompassing data on 7,633 tokens following the implementation of the Banana Gun tool in December 2023. Data pre-processing involved correlation analysis, data scaling using MaxAbsScaler, and resampling through Random Over-Sampling to bolster algorithm accuracy.

Notably, the classification results showcased an impressive accuracy rate of 87.89% post RFE, which effectively identified and eliminated less significant features. The model's performance with SMOTEEN for handling imbalanced data excelled in recall metrics but displayed average generalization on a larger dataset. The Extreme Gradient Boosting model emerged with the highest F1-score across various time intervals, with diminishing values over prolonged periods possibly attributed to easier fraud identification at the initial phase.

Key findings highlighted the significance of WETH turnover in initial token transactions and the timing of token releases. Analysis indicated that tokens with lower WETH turnover and delayed releases are less likely to be associated with fraudulent activities. Furthermore, fraudulent tokens tended to exhibit substantial price fluctuations and higher validator rewards, potentially linked to swift buying and selling strategies. A nuanced understanding of these characteristics proves instrumental in enhancing model predictions and fortifying fraud detection mechanisms.

Furthermore, an evaluation of the economic impact of our model on cryptocurrency investors revealed stark differences between investment strategies. Comparing two approaches showcased the potential economic gains facilitated by classifiers, contrasting with scenarios devoid of machine learning insights that proved unprofitable.

Based on our findings, the following directions are worth exploring for future investigations:

- Delve deeper into investor behavior patterns post-token launch to identify early warning signs of potential fraudulent activities.
- Incorporate sentiment analysis from social media platforms to gauge investor sentiment and its impact on token prices and fraud detection.
- Explore real-time model updating techniques to adapt to evolving fraud strategies and enhance predictive accuracy.
- Extend the study to analyze fraudulent activities across multiple decentralized exchanges beyond Uniswap V2, considering different platform dynamics.

This study sheds light on the deceptive practices surrounding meme coins and the prevalence of fraudulent activities within decentralized exchanges. By leveraging advanced machine learning techniques and blockchain data analysis, we have made significant strides in predicting rug pulls and identifying potential fraudulent tokens. The high accuracy rates achieved underscore the effectiveness of our model in distinguishing between legitimate projects and malicious tokens.

As the cryptocurrency landscape continues to evolve, it is imperative to remain vigilant against fraudulent activities and adopt proactive measures to safeguard investors. By further exploring the suggested research directions, we can enhance our understanding of fraudulent behaviors within the crypto space and develop robust frameworks for fraud detection and prevention.


## Acknowledgments

The authors express their gratitude Bitquery Inc. (`https://bitquery.io/`) for the use of their API product, which facilitated access to the data required for this research. Bitquery Inc. is an API-first product company dedicated to power and solve blockchain data problems using the ground truth of on-chain data.

The authors express their gratitude to the anonymous crypto enthusiast Osoi Otoko for sharing valuable insights on meme coins and for engaging in fruitful discussions.


## References


[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org (2008) 1–9.
URL `https://bitcoin.org/bitcoin.pdf`

[2] V. Buterin, Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform, Ethereum (January) (2014) 1–36.
URL `https://github.com/ethereum/wiki/wiki/White-Paper`

[3] R. Huang, J. Chen, Y. Wang, T. Bi, L. Nie, Z. Zheng, An overview of Web3 technology: Infrastructure, applications, and popularity, Blockchain: Research and Applications 5 (1) (2024) 100173. `doi:10.1016/J.BCRA.2023.100173`.

[4] E. Meyer, I. M. Welpe, P. Sandner, Decentralized Finance—A systematic literature review and research directions, in: ECIS 2022 Research Papers, Elsevier BV, 2021, pp. 1–25. `doi:10.2139/ssrn.4016497`.

[5] CoinMarketCap, Today's Cryptocurrency Prices by Market Cap (2023).
URL `https://coinmarketcap.com/`

[6] DAO Community and Friends, The DAO Whitepaper (2016).
URL `https://github.com/the-dao/whitepaper`

[7] E. Bischof, A. Botezatu, S. Jakimov, I. Suharenko, A. Ostrovski, A. Verbitsky, Y. Yanovich, A. Zhavoronkov, G. Zmudze, Longevity Foundation: Perspective on Decentralized Autonomous Organization for Special-Purpose Financing, IEEE Access 10 (2022) 33048–33058. `doi:10.1109/ACCESS.2022.3161392`.
URL `https://ieeexplore.ieee.org/document/9739690/`

[8] O. Rikken, M. Janssen, Z. Kwee, The ins and outs of decentralized autonomous organizations (DAOs) unraveling the definitions, characteristics, and emerging developments of DAOs, Blockchain: Research and Applications (2023) 1–26`doi:10.1016/j.bcra.2023.100143`.

[9] W. Metcalfe, Ethereum, Smart Contracts, DApps, Vol. 77, Springer Singapore, 2020, pp. 77–93. doi:10.1007/978-981-15-3376-1_5.
URL http://link.springer.com/10.1007/978-981-15-3376-1_5

[10] F. Vogelsteller, V. Buterin, EIP-20: ERC-20 Token Standard (2015).
URL https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

[11] V. Davydov, A. Gazaryan, Y. Madhwal, Y. Yanovich, Token Standard for Heterogeneous Assets Digitization into Commodity, in: Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, ACM, New York, NY, USA, 2019, pp. 43–47. doi:10.1145/3376044.3376053.
URL https://dl.acm.org/doi/10.1145/3376044.3376053

[12] M. di Angelo, G. Salzer, Tokens, Types, and Standards: Identification and Utilization in Ethereum, in: 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), IEEE, 2020, pp. 1–10. doi:10.1109/DAPPS49028.2020.00001.
URL https://ieeexplore.ieee.org/document/9126009/

[13] S. A. Lee, G. Milunovich, Digital exchange attributes and the risk of closure, Blockchain: Research and Applications 4 (2) (2023) 100131. doi:10.1016/j.bcra.2023.100131.
URL https://linkinghub.elsevier.com/retrieve/pii/S2096720923000064

[14] S. Dos Santos, J. Singh, R. K. Thulasiram, S. Kamali, L. Sirico, L. Loud, A New Era of Blockchain-Powered Decentralized Finance (DeFi) - A Review, in: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE, 2022, pp. 1286–1292. doi:10.1109/COMPSAC54236.2022.00203.
URL https://ieeexplore.ieee.org/document/9842637/

[15] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, Tech. rep. (2023).
URL https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

[16] Chainalysis, The Chainalysis 2023 Crypto Crime Report, Tech. rep., Chainalysis (2023).
URL https://go.chainalysis.com/2023-crypto-crime-report.html

[17] R. Falcone, S. Conant, New shameless commodity cryptocurrency stealer (westeal) and commodity rat (wecontrol) (2023).

[18] S. T. Howell, M. Niessner, D. Yermack, Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales, The Review of Financial Studies 33 (9) (2020) 3925–3974. doi:10.1093/rfs/hhz131.
URL https://academic.oup.com/rfs/article/33/9/3925/5610546

[19] A. Stencel, What is a meme coin? dogecoin to the moon! (12 2023).
URL https://hal.science/hal-04360574https://hal.science/hal-04360574/document

[20] D. A. Zetzsche, D. W. Arner, R. P. Buckley, Decentralized Finance (DeFi), SSRN Electronic Journal (2020). doi:10.2139/ssrn.3539194.
URL https://www.ssrn.com/abstract=3539194

[21] B. Mazorra, V. Adan, V. Daza, Do Not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection, Mathematics 10 (6) (2022) 949. doi:10.3390/math10060949.

[22] H. Adams, Uniswap Whitepaper (2018).
URL https://hackmd.io/@HaydenAdams/HJ9jLsfTz

[23] H. Adams, N. Zinsmeister, D. Robinson, Uniswap v2 Core (2020).
URL https://uniswap.org/whitepaper.pdf

[24] L. LAMPORT, R. SHOSTAK, M. PEASE, The byzantine generals problem, ACM Transactions on Programming Languages and Systems 4 (3) (1982) 382–401.

[25] R. De Prisco, B. Lampson, N. Lynch, Revisiting the paxos algorithm, in: Distributed Algorithms: 11th International Workshop, WDAG'97 Saarbrücken, Germany, September 24–26, 1997 Proceedings 11, Springer, 1997, pp. 111–125.

[26] L. Oliveira, I. Bauer, L. Zavolokina, G. Schwabe, To token or not to token: Tools for understanding blockchain tokens, in: International Conference on Information Systems 2018, ICIS 2018, 2018, pp. 1–17.

[27] H. Benedetti, G. Rodríguez-Garnica, Tokenized Assets and Securities, The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges (2023) 107–121doi:10.1108/978-1-80455-320-620221008.

[28] CoinMarketCap, Today's Cryptocurrency Prices by Market Cap (2024).
URL https://coinmarketcap.com/

[29] S. Dowlat, M. Hodapp, Cryptoasset market coverage initiation: network creation, Satis Group (Satis Group) (2018).

[30] S. Srifa, Y. Yanovich, A. Salehi S., R. Vasilyev, T. Rupasinghe, V. Amelin, Scam Token Classification for Decentralized Exchange Using Transaction Data, SSNR (2023).
URL https://ssrn.com/abstract=4582918orhttp://dx.doi.org/10.2139/ssrn.4582918

[31] A. Elsts, Liquidity Math in Uniswap v3, SSRN Electronic Journal (2021) 1–8doi:10.2139/ssrn.4575232.

[32] D. Liebau, P. Schueffel, Crypto-currencies and icos:

Are they scams? an empirical study, SSRN Electronic Journal (01 2019). doi:10.2139/ssrn.3320884.

[33] M. Tiwari, A. Gepp, K. Kumar, The future of raising finance - a new opportunity to commit fraud: A review of initial coin offering (icos) scams, Crime, Law and Social Change: an interdisciplinary journal 73 (4) (2020) 417–441. doi:10.1007/s10611-019-09873-2.

[34] T. Chiu, V. Chiu, T. Wang, Y. Wang, Using textual analysis to detect initial coin offering frauds, Journal of Forensic Accounting Research 7 (1) (2022) 165–183.

[35] L. Hornuf, T. Kück, A. Schwienbacher, Initial coin offerings, information disclosure, and fraud, Small Business Economics 58 (04 2022). doi:10.1007/s11187-021-00471-y.

[36] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, Y. Zhou, Detecting ponzi schemes on ethereum: Towards healthier blockchain technology, in: Proceedings of the 2018 World Wide Web Conference, 2018, pp. 1409–1418.

[37] M. Bartoletti, S. Carta, T. Cimoli, R. Saia, Dissecting ponzi schemes on ethereum: identification, analysis, and impact (2019). arXiv:1703.03779.

[38] M. Vasek, T. Moore, There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams, in: R. Böhme, T. Okamoto (Eds.), Financial Cryptography and Data Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015, pp. 44–61.

[39] R. Ji, N. He, L. Wu, H. Wang, G. Bai, Y. Guo, Deposafe: Demystifying the fake deposit vulnerability in ethereum smart contracts, 2020, pp. 125–134. doi:10.1109/ICECCS51672.2020.00022.

[40] T. Durieux, J. F. Ferreira, R. Abreu, P. Cruz, Empirical review of automated analysis tools on 47,587 Ethereum smart contracts, in: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, ACM, New York, NY, USA, 2020, pp. 530–541. doi:10.1145/3377811.3380364.
URL https://dl.acm.org/doi/10.1145/3377811.3380364

[41] C. Sendner, L. Petzi, J. Stang, A. Dmitrienko, Vulnerability scanners for ethereum smart contracts: A large-scale study, arXiv preprint arXiv:2312.16533 (2023).

[42] D. Twomey, M. Mann, Fraud and manipulation within cryptocurrency markets, in: Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation, Wiley, 2020, pp. 205–250.

[43] P. Xia, H. wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, G. Xu, Trade or trick? detecting and characterizing scam tokens on uniswap decentralized exchange (2021). arXiv:2109.00229.

[44] P. Xia, B. Zhang, R. Ji, B. Gao, L. Wu, X. Luo, H. Wang, G. Xu, Characterizing cryptocurrency exchange scams (2020). arXiv:2003.07314.

[45] M. H. Nguyen, P. D. Huynh, S. H. Dau, X. Li, Rug-pull malicious token detection on blockchain using supervised learning with feature engineering, in: Proceedings of the 2023 Australasian Computer Science Week, 2023, pp. 72–81.

[46] C. Li, H. Yang, Will memecoins' surge trigger a crypto crash? evidence from the connectedness between leading cryptocurrencies and memecoins, Finance Research Letters 50 (2022) 103191.

[47] E. Lansiaux, N. Tchagaspanian, J. Forget, Community impact on a cryptocurrency: Twitter comparison example between dogecoin and litecoin, Frontiers in Blockchain 5 (2022) 829865.