Short Paper: DeFi Deception – Uncovering the prevalence of rugpulls in cryptocurrency projects

Sharad Agarwal[1], Gilberto Atondo-Siu[2], Marilyne Ordekian[1], Alice Hutchings[2], Enrico Mariconti[1], and Marie Vasek[1]

[1] University College London
{sharad.agarwal, marilyne.ordekian.21, e.mariconti, m.vasek}@ucl.ac.uk
[2] University of Cambridge
{jga33,ah793}@cl.cam.ac.uk

Abstract. DeFi has attracted legitimate investors and scammers alike. The paper presents an empirical investigation into the prevalence of rugpulls, a scam where cryptocurrency project developers exit without fully delivering and leave investors in the wind. Using forum data, 101 rugpulls from 6 different types of DeFi services are documented. ICOs form the majority of the rugpulls, most of which were active for less than six months before scamming out. ICOs rugpulled in 2021 were active for a much longer time than those that were rugpulled later on, perhaps pointing to new entrants intending to pull the rug. Through qualitative thematic analysis, we discover that these schemes primarily use authoritative and financial lures at the announcement stage of the project to mimic legitimate projects.

1 Introduction

With the rise of many types of cryptocurrency projects, it has become increasingly difficult for ordinary consumers to assess the validity of any particular project. With decentralized finance (DeFi) becoming increasingly popular, more and more consumers are brought to the cryptocurrency ecosystem. In turn, scammers have capitalized on investment scams, using consumers' lack of knowledge and the relative lack of consumer protections to earn millions of dollars.

Exit scams are scams where project developers abandon the project and run away with investors' funds. Unlike Ponzi schemes, these do not offer ludicrous rates of returns as a whole. Rather, they promise a good or service that they do not deliver. **Rugpulls** are exit scams in DeFi.

Exit scams, more broadly, are quite profitable – Chainalysis found that 37% of scam revenue in 2021 was from exit scams [1]. In 2021, operators of a Turkish cryptocurrency exchange, Thodex, ran away with $2 billion after closing overnight. In March 2022, the US Department of Justice charged two people in a rugpull NFT scam that they anticipated would earn around $1.5M [15].

Our work investigates the incidences of rugpulls over time across different categories of projects in DeFi. To measure this comprehensively across these different categories, we use reports of rugpulls from a discussion forum to create

a list of 101 different services which were rugpulled, mostly from 2020-2022. We provide the following contributions:

- We detail our comprehensive methodology that identifies rugpulls across six different categories of projects over more than two years in §3.
- We show the variety of types of rugpulls in §4. We relate this back to other occurrences in the ecosystem during this time to decipher why this happens.
- Using qualitative thematic analysis, we work towards understanding the lures when the projects are first announced in §5. This helps explain how scam projects draw in victims.

2 Related Work

There exists a burgeoning research direction in measuring exit scams on blockchains. Mazorra et al. [8] and Xia et al. [17] both detect over 10,000 rugpull scam tokens on the Uniswap platform, which defrauds users out of millions of dollars.

Mackenzie analyzes cryptocurrency scams through a criminological lens and divides rugpulls into two types: slow and fast [7]. Slow rugpulls are scams where the organizers start, e.g., an Initial Coin Offering (ICO), premine a large sum of the currency, and then slowly sell off their stock of coins. This contrasts with fast rugpulls of the sort that Mazorra et al. and Xia et al. uncover, which exploit quick liquidity hits on DeFi platforms like Uniswap. Xu et al. formalizes fast rugpulls [20]. Our work collects information on primarily the slower type.

Others have explored different areas in the cryptocurrency ecosystem and showed the impact of exit scams. Soska and Christin showed the impact of exit scam behavior both by exchange operators and on individual vendors on the reputation of the dark net market ecosystem [12]. In 2020, Xia et al. found that many COVID-influenced ICOs ended up performing exit scams [18]. Oosthoek and Doerr and Moore et al. separately analyzed security behavior on cryptocurrency exchanges and considered (but did not independently measure) exit scams [11][9]. This work fits broadly into the literature on cryptocurrency scams [19][16][4].

3 Methodology

In this section, we describe our approach to collecting our rich dataset on reported rugpulls.

3.1 Quantitative methods

Collecting Rugpulls Rugpulls are a relatively new form of cryptocurrency fraud, and no comprehensive list of these exists. To curate a more diverse listing of these scams, we use the discussion forum, `bitcointalk.org`. This forum, started by Satoshi themself, has historically been used to talk about cryptocurrencies more broadly. Currently, it remains a source for cryptocurrency beginners and often attracts scammers (and then talks about scams). This source is by no means

comprehensive, but it does yield an insight into scams particularly targeting new users. We evaluated other open source listings of rugpull scams and could not find another set of listings of not just large rugpulls that make the news, but also smaller ones that influence not just new users' wallets, but also their trust in the community.

We use the Google Custom Search API[3] and identify all posts between Jan 2018 and Sept 2022 which include the keywords "rug pull" or "rugpull." We find 551 pages consisting of 335 distinct threads. For each thread, we fetch a local copy of all the posts in that thread.

Rugpull is a relatively new term and many users used it out of context, increasing the number of false positive threads. For instance, some threads speculate if a particular project will rugpull in the future, new users ask advice on various identification strategies for a rugpull, and investment advertisements claim to be 'rugpull proof.' Therefore, we manually review all the 335 distinct threads and identify 101 unique rugpulled projects. By inspecting the related threads and archived versions of the linked project websites, we categorize them into six different service categories. Table 1 shows an overview of the collected information.

Service Type	Definition	Obs.
Initial Coin Offerings (ICO)	Raising money to create a new ERC20 token	73
Yield farms	Lending crypto assets to earn interest on the loan	16
Exchanges	Platforms for users to buy/sell cryptocurrency	5
Non-Fungible Tokens (NFT)	Unique, non-interchangeable digital asset that can be bought and sold	5
Initial Dex Offerings (IDO)	Similar to ICO, but on a decentralized exchange	1
Cloud mining	Fractional shares of a mining operation	1

Table 1. DeFi service types by quantity of observed rugpulls ($N = 101$).

Collecting Supplementary Data To find the corresponding start date of each project (since many projects did not exist on third-party aggregator websites), we collect the dates when the services were first introduced on the forum. These project announcements, aka ANN threads, are threads where people announce their upcoming projects. Users often link the ANN threads in the same thread where the rugpull was reported. Other times, rugpull report thread is an ANN thread where the incidence of rugpull was mentioned in a later post on the thread. For the remainder, we query the bitcointalk forum using the rugpull's name to find its first occurrence. We manually verify that the mentioned service was indeed the same. To this end, we identify 63 rugpulls' first occurrence date.

To supplement our data on rugpulled services, we collect data on ICOs, the most common identified rugpull. We collate 2177 ICOs introduced between 2014 and September 2022 from the aggregator website `coincodex.com`. We omit 57 without a start date. We augment this with the available listings on `coinmarketcap.com`, resulting in 2227 total ICOs. Additionally, we use the historical data for the price of Bitcoin and Ethereum in USD from `coincodex.com`.

[3] `https://developers.google.com/custom-search/v1/overview`

3.2 Qualitative thematic method

Cybercriminals use social engineering techniques to attract and deceive investors. It is essential to understand these techniques so investors can detect and avoid falling prey to fraudulent schemes. Therefore, we perform a qualitative thematic analysis [5] of project announcements in bitcointalk before they are reported to be rugpulled. We extract the content of posts identified as rugpulls and perform a manual thematic categorization of the text used in the announcement of these projects. We compare this to an analysis of an equal number of project announcements, selected from similar date ranges, that were not claimed to have been rugpulled. We use one coder to classify the data following a "concept-driven"[5] approach and adapt Stajano and Wilson's [13] scam lure principles as the framework for our analysis. We apply this framework's seven principles (shown in Table 2) as the codebook used for matching announcements; our results in §5 have been paraphrased to anonymize the source.

Lure Principle	Description
Authority	Cybercriminals aim to provide trust to investors by showing technical knowledge and making references to legitimate entities.
Dishonesty	Fraudsters invite users to participate willingly and knowingly into a fraudulent scheme.
Distraction	Scammers aim to confuse users by giving many unrelated details.
Financial	Cybercriminals leverage users' 'greed' and offer attractive monetary benefits, so users make an investment.
Herd	Scammers encourage investors to not miss out on opportunities by relating to the popularity of the scheme.
Kindness	Fraudsters leverage the willingness of people to help others.
Time	Scammers pressure users to make decisions quickly.

Table 2. Description of lure principles adapted from Stajano and Wilson [13]

Ethical Considerations: We constructed our study design and data collection to minimize harm to forum participants. We did not store potential PII. We went through the ethics oversight process at the university and received approval.

4 Quantitative Findings

While almost every cryptocurrency platform has had scam services confusing potential customers, scams tend to concentrate on specific sectors based on the scam type. Rugpulls are, by definition, related to DeFi services which naturally limits their scope. However, we wish to uncover which services disproportionately fall prey to this scam and if this trend changes as new technology in the DeFi space is released over time or if other factors, such as the price of Ethereum, change the incentives for scammers to decide to pull the rug at a given time.

Rugpulls vs. Exit Scams The word "rugpull" is a relatively new term whose usage can overlap colloquially with the word "exit scam" since rugpulls are a subset of exit scams that particularly refer to DeFi projects. Here we contextualize

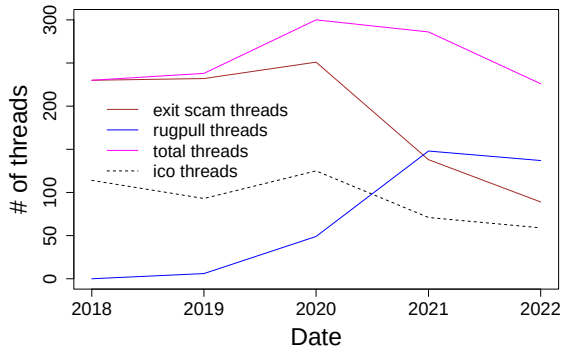

Fig. 1. Bitcointalk forum threads containing the keywords 'exit scam' ($N = 940$) and 'rugpull'/'rug pull' ($N = 340$) and the subset of these that mention 'ico' ($N = 462$).

our work on rugpulls by comparing the data to a similar dataset but on exit scams and show how exit scams have existed for a longer time and seem to cover different sorts of scams. Using the same methodology described in §3.1, we collect the posts on bitcointalk using the keyword "exit scam" and find 940 unique threads between 2018 and 2022. We also consider threads that contain the keyword "ICO" both in the exit scam and the rugpull data collections, since we hypothesized ICO scams could possibly be a dominant player here.

We observe how the keywords: "exit scam" and "rugpull" have evolved in Fig. 1. We find that while mentions of exit scams vastly predate mentions of rugpulls, the total mention of either of these terms is relatively stable over time. The increasing number of rugpull threads since 2020 motivates us to look deeper into the rugpull services in further subsections.

4.1 Rugpulls over Time and by Service

We start by understanding how reports of rugpulls have evolved. There were four reported rugpulls before mid-2020: one exchange and three ICOs. However, the start of this phenomenon really kicks off starting the second half of 2020, as shown in Fig. 2. This follows the rise of DeFi services; scammers enter the market after its popularity increases, and new services (which might have otherwise failed) "cash out" using this scam.

Yield farming services suddenly gained attraction in the summer of 2020 [2]. We see a peak in yield farm rugpulls in March 2021 after fifteen such scams were reported in a single thread on the forum. We only observed one other occurrence of rugpulls of yield farming services beyond this. This is likely an artifact of our data – bitcointalk tends towards less sophisticated users. For instance, an aggregator website of yield farming scams[4] lists 41 different scams (ranging from fake air drops to rugpulls) from Oct 2020 through Jan 2021.

To understand the number of days between the projects being announced and subsequently rugpulled, we analyze the distribution of their lifetime as seen in

[4] `https://defiyield.info/yield-farming-scam-database`

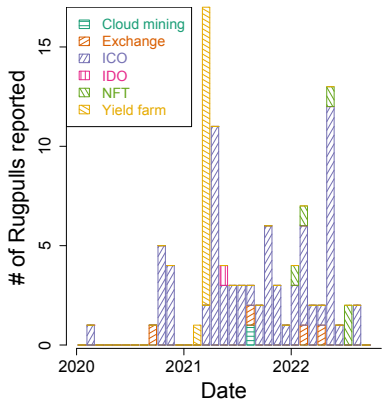

Fig. 2. Rugpulls reported between Jan 2020 and Sept 2022 ($N = 98$), split by type of service.

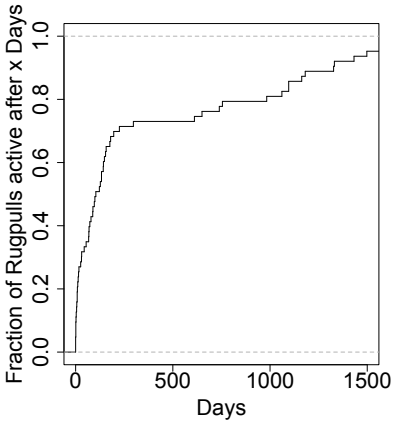

Fig. 3. Cumulative distribution for the number of days rugpull services were active ($N = 63$).

Fig. 3[5]. While 68% of the rugpulled projects were active for less than six months, 23.8% were active for more than two years. We hypothesize that the longer-running projects wait for a reasonable ETH exchange rate before pulling the rug. We observe this in Figure 5. The positive Spearman's correlation coefficient between the monthly price of Ethereum and the monthly frequency of rugpull projects supports this hypothesis ($r_s = 0.606, p < 0.001$).

We also find that the projects rugpulled before September 2021 were active for a long time (median 384 days): the most long-lasting project was active for 2551 days. However, in 2022, rugpulled projects were active for only a short time (< 180 days, median 110.5 days). This likely demonstrates that these products started to engage in a rugpull scam after seeing the earlier success of their pre-2022 analogues. For instance, 'WX Coin' started in 2018 with some reputation mechanisms like a GitHub repo and whitepaper, but after 3 years, were possibly tempted by financial gains and rugpulled. On the other hand, 'Squid Coin,' based on a famous TV show in Oct 2021, was designed to attract investors and then rugpull within days once the token's price dramatically increased [14].

4.2 Rugpulls in ICOs

ICOs form the majority of the rugpulls in our data. Most of these are considered in the literature to be slow rugpulls [7], where the scam is rolled out over periods of months or years rather than hours. However, this term used to discuss token ICOs is relatively new, and ICOs are becoming less frequent with time.

To understand this interaction, we compare the number of ICOs introduced with ICOs rugpulled over time. We find that the increase in rugpulled ICOs

[5] We only consider those that we have start dates for. See §3.1.

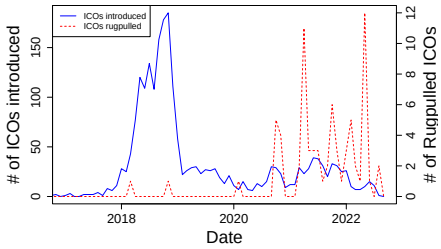

Fig. 4. Comparison of ICOs introduced ($n = 2227$) over time with the number of rugpulled ICOs ($N = 73$).

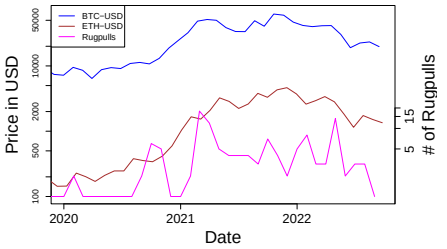

Fig. 5. Exchange rate of Bitcoin and Ethereum compared to rugpulls ($N = 98$) between Jan 2020 to Sept 2022.

broadly follows the increase in ICOs introduced, as seen in Fig. 4. We observe that while the peak in ICO announcements occurred in October 2018, rugpulls started to peak two years later. Part of this is a term definition issue: we did not use "rug pull" until around 2020 and we likely missed out on earlier ICO projects which pulled the rug. This could also be due to the lifetime of a legitimate ICO – it takes time for projects to turn a product and similarly, scammers can then accept money for longer periods of time. We also hypothesize this could be due to companies that started with legitimate, but perhaps overhyped and underresourced ideas, and ended up selling to scammers to get out.

We find that the number of rugpulled ICOs has decreased since the second half of 2022. This is likely due to the decrease of the popularity of ICOs waning with time with scammers and legitimate project owners moving other to new DeFi attractions like IDOs and NFTs. This could also be due to volatility.

5 Qualitative thematic analysis

As mentioned in §4.2, many rugpull projects are associated with ICOs, which use marketing tools to attract investors and provide credibility. ICO rugpulls also aim to follow these processes, at least to some extent, to convince potential victims of their purported legitimacy.

We identify the authority principle being used in some of these projects. Our dataset includes schemes that provide details of their corresponding founders, proposed algorithms, and links to code in GitHub repositories. Many include this information in whitepapers, some of which turn out to be plagiarized [10]. For example, one project claims to provide a better consensus protocol. Another project claims to be sponsored by reputable fund providers. We found similar examples of legitimate projects that provide analogous information when they are introduced in the forum. This shows the difficulty that investors might have to differentiate scams from legitimate projects when scammers use this principle.

We also uncover the financial principle in rugpulled projects. For instance, one promises an outstanding rate of passive return on a guaranteed and effortless basis. We discover a combination of the time and herd principles used in some other projects. For example, one of the schemes encourages users not to miss an

opportunity to see their tokens' price increase, which will happen if more people join the project. We did not find these types of strategies used to advertise legitimate projects. Therefore, these examples provide some indications of the warnings that investors should be aware of to avoid falling prey to rugpulls.

Our analysis shows that investors should be skeptical of projects that employ financial, time, and herd principles to lure investors since these are not frequently found in legitimate projects. We do not observe the use of dishonesty, distraction, or kindness principles in the rugpulled project announcements. This fits into the work of Jahani et al. on discussions about "less serious" coins on `bitcointalk` where users hype up the coin rather than seeking for truth about it [6].

6 Conclusion

We have presented the dynamics of rugpull scams using a mixed method approach, with the aim of empirically analyzing the phenomena. While the early rugpull scams were using services that have been active for a long time, the later peaks have consisted of very new services. This indicates that, while at the beginning rugpull scams were perhaps not planned but rather opportunistic, more recent scams were likely planned and operated with malicious intent due to the easy earnings. This highlights not only how users flock to invest in DeFi after particular types of services are hyped, but also how scammers follow the money.

In this paper, we have established the prevalence of rugpull scams during the prolonged regulatory void. However, the situation is expected to change with the upcoming MiCA (Markets in Crypto-Assets[3]) regulation which is set to harmonize rules for cryptocurrencies across the EU. The framework intends to alleviate existing uncertainties in many ways, including the enhancement of consumer protection and bringing those such as token issuers under a proper form of standards. In particular, the rules will require issuers to be legal entities that draft, notify, and publish a detailed whitepaper that not only includes clear and transparent information about the project and the marketing communications[6], but also on the issuers/offerors themselves (art. 4,5,6,7,8). MiCA will also grant consumers[7] the right to withdraw their funds or even be reimbursed when possible (art. 12). Consequently, it will be harder for scammers to run and get away with schemes such as rugpulls.

In the interim, our qualitative analysis highlights how criminals use the promise of financial gain (financial principle) and the unmissable opportunity (time principle) to lure investors and scam them. Note that these principles are of differing effectiveness as some savvy investors highlight these lures as suspicious behavior. We encourage those operating platforms for beginning investors, such as those moderating discussion forums to alert novices to these potential lures and exercise caution.

[6] Marketing must also follow the notification and publication process where applicable.
[7] The right to withdraw and reimbursement only applies to retail holders and not to qualified investors.

References

1. Chainalysis: The biggest threat to trust in cryptocurrency: Rug pulls put 2021 cryptocurrency scam revenue close to all-time highs. https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/
2. Cousaert, S., Xu, J., Matsui, T.: Sok: Yield aggregators in DeFi. In: 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 1–14 (2022)
3. European Commission: Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
4. Foley, S., Karlsen, J.R., Putniņš, T.J.: Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies **32**(5), 1798–1853 (2019)
5. Gibbs, G.: Analyzing qualitative data. The SAGE qualitative research kit, SAGE, London (2007)
6. Jahani, E., Krafft, P.M., Suhara, Y., Moro, E., Pentland, A.S.: Scamcoins, s*** posters, and the search for the next bitcoin^{TM}: Collective sensemaking in cryptocurrency discussions. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–28 (2018)
7. Mackenzie, S.: Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. The British Journal of Criminology (2022)
8. Mazorra, B., Adan, V., Daza, V.: Do not rug on me: Leveraging machine learning techniques for automated scam detection. Mathematics **10**(6) (2022)
9. Moore, T., Christin, N., Szurdi, J.: Revisiting the risks of bitcoin currency exchange closure. ACM Transactions on Internet Technology **18**(4), 50:1–50:18 (Sep 2018)
10. Morin, A., Vasek, M., Moore, T.: Detecting text reuse in cryptocurrency whitepapers. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 1–5 (2021)
11. Oosthoek, K., Doerr, C.: From hodl to heist: Analysis of cyber security threats to bitcoin exchanges. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 1–9. IEEE (2020)
12. Soska, K., Christin, N.: Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In: Proceedings of the 24th USENIX Security Symposium. pp. 33–48. Washington, DC (Aug 2015)
13. Stajano, F., Wilson, P.: Understanding scam victims: seven principles for systems security. Communications of the ACM **54**(3), 70–75 (2011)
14. Stokel-Walker, C.: How a Squid Game crypto scam got away with millions. https://www.wired.co.uk/article/squid-game-crypto-scam
15. US Department of Justice: Two defendants charged in non-fungible token fraud and money laundering scheme. https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0
16. Vasek, M., Moore, T.: There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In: Financial Cryptography and Data Security. pp. 44–61. Springer (2015)
17. Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X., Xu, G.: Trade or trick? Detecting and characterizing scam tokens on Uniswap decentralized exchange. Proceedings of the ACM on Measurement and Analysis of Computing Systems **5**(3), 1–26 (2021)

18. Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., Xu, G., Huang, G., Liu, X.: Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams. In: 2020 APWG Symposium on Electronic Crime Research (eCrime). pp. 1–14. IEEE (2020)
19. Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., Xu, G.: Characterizing cryptocurrency exchange scams. Computers & Security **98**, 101993 (2020)
20. Xu, J., Paruch, K., Cousaert, S., Feng, Y.: SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. `https://arxiv.org/abs/2103.12732` (2021)