5th International Conference on Advanced Research Methods and Analytics (CARMA2023)
Universidad de Sevilla, Sevilla, 2023
DOI: http://dx.doi.org/10.4995/CARMA2023.2023.16428

On the involvement of bots in promote-hit-and-run scams – the case of Rug Pulls

Dietmar Janetzko[1], Jonas Krauß[1], Frederic Haase[2], Oliver Rath[2]
[1]Stockpulse GmbH, Germany, [2]University of Cologne, Germany

Abstract

Many social media frauds related to finance can be summarized under what we consider promote-hit-and-run scams. Examples include rug pull scams also known as exit scams, pump-and-dump schemes or bogus crypto currency trading platforms. For scams of this kind *to work they must be publicly advertised as lucrative investment opportunities. Social media are key in this promotion. Here, fraudsters find platforms to persuade others investing into what later turns out to be a scam. Via social network analysis of Twitter screen names and their first-level contacts, our work investigates rug pulls. It examines social media communication around them with a special focus on the deployment of bots. Repeatedly bots have been identified in social media campaigns (Orabi et al., 2020). Bot deployment in the context of rug pulls, however, has not been studied yet. Our analysis of social data of 27 rug pulls reveals for the first time massive bot activity coordinated within and between rug pulls mainly targeting established finance news outlets, e.g., Bloomberg, Reuters. Among the conclusions of our work is that bot deployment may prove an early indicator for rug pulls and other promote-hit-and-run scams.*

Keywords: *Bots; social media; rug pull; crypto currencies; fraud; twitter*

The work described in this paper has been partially financed by the AFFIN Project funded by the German Federal Ministry of Education and Research (BMBF).

Editorial Universitat Politècnica de València

1. Introduction

Financial fraud in social media comes in various forms (e.g., Mirtaherie et al, 2021 Nghiemet et al. 2021). Many of them share a similar pattern: fraudsters entice people into actions that promise high gains, but which eventually translate into losses to the victims. We summarize swindles implemented around this pattern under the category of promote-hit-and-run scams. Examples include rug pull scams, pump-and-dump schemes or enticements to bogus crypto currency trading platforms. Most of them are initiated by coordinated social media campaigns on platforms such a Telegram, Reddit or Twitter (Orabi et al., 2020; Sharma et al, 2021; Tardelli et al., 2020). The digital traces fraudulent campaigning leaves gives us a handle to identify them. The work in this paper investigates Twitter activities related to rug pulls (Solidus, 2022, Scharfman, 2023). Rug pulls are examples of promote-hit-and-run scams usually connected to crypto currencies whereby the developers take the assets of investor and disappear. Negligible before 2020, rug pulls now spread at a staggering speed. Platforms like Twitter, Reddit or Telegram are among the most popular communication channels for rug pull promotion. The importance of communication for the success of rug pulls invites a comparison with other campaigns that rely on communication on social media, e.g., pump-and-dump (Mirtaheri et al., 2021) or in politics (Murthy et al., 2016). In those and many other areas communication on social media is often affected or even orchestrated by bots. To the best of our knowledge, however, possible bot involvement of social media communication related to rug pulls has not yet been investigated.

In sum, public communication is indispensable to promote rug pull projects. Details on the involvement of bots as an essential element of this type of fraudulent communication are largely unknown, however. Against the background of this research gap, the overall question addressed in this paper is: Are there social media indicators of bots activity related to crypto investments that were later rug pulled? We break this question down into two more specific objectives: Firstly, to find out whether and in which way bot activity is reflected in historical social data of rug pulls, we compare screen names co-occurrence across 27 of them. We secondly identify screen names involving a rug pull and their contacts and set up a social network with screen names as vertices and interactions (replies, retweets) between them as directed edges. We then examine whether social network metrics like in- and out-degree centrality and their relation to bot probability scores (Yang et al, 2020) allow us to identify the deployment of bots in rug pulls. Our paper is organized as follows. The next section looks into recent work on bot activity around finance-related topics in social media, which is followed by an outline of the methodology used. Next, the studies corresponding to our research objectives are presented. The paper concludes with a discussion of our results.

2. Related Work

Social Bots (or simply bots) are automated programs that deceitfully act like humans on social media. Though bots are a widespread phenomenon (Orabi et al., 2020, Aljabri et al., 2023) there are only a few studies on bots in relation to crypto currencies and to their role in financial markets in general (Mirtaheri et al., 2021; Schuchard et al 2019; Tardelli et al., 2020). Of particular interest to our work is the work by Mirtaheri et al., 2021. The authors found a large number of Tweets related to crypto currencies generated by bots. Increased Twitter bot activity was observed during the time of pump-and-dump frauds. Though pump-and-dump schemes share some similarities with the rug pulls, they are not necessarily the same. For instance, a rug pull involves completely new tokens. Thus, it can be expected that in rug pulls more effort has to be put into the trust building. This can hardly work in a short time span and may require a strong visibility on social media. It cannot be ruled out that various types of bots are deployed to achieve these goals. Examples include the follower-bots that increase the sheer number of accounts following another account or commenting bots that post comments.

3. Method

Data on the rug pulls studied was made available by Stockpulse's archive of historical and current social media messages.[1] It covers historical and current social media communication analytics for, e.g., Twitter, Telegram, Reddit, Discord over up to 12 years. From Stockpulse's archive, Tweet data on each of the following 27 rug pulls was analyzed:

Africrypt, AnubisDAO, Baby Musk Coin, BabyEth, BankSocial, Billionaire Dogs, BitConnect, CryptoZoo, DeFi100, Dink Doink, EthereumMax,Freeway Token,Green Satoshi, Kronos DAO, MILF Token, Mango Token, RapDoge, SafeMoon V1, Snowdog DAO, Snowflake DeFi, SolFire, Squid Game, StableMagnet, TeddyDoge, Terra Classic, Thodex, Yummy Token

For our studies we selected medium to large rug pulls executed between Feb 15, 2016 – Feb 6, 2023. The time of the communication sourced was essential to increase the likelihood of catching bot activity. Therefore, we collected Tweets exchanged after the introduction of the coin to the public associated with each rug pull examined, but before its public exposure

[1] Stockpulse is a data analytics company based in Bonn (Germany) offering advanced AI-driven data and signals for financial institutions and regulators.

as a scam via an authoritative source that flagged up the fraud.[2] The data-collection is broken down into two steps:

Step 1. Using the interval-based method described above we sourced messages referring to one of the 27 rug pulls and preprocessed them into key variables including screen name and time. This resulted in 27 seed lists of screen names, which is just a list of Twitter addresses of account connected to a rug pull. The 27 seed lists ranged between 23 (Snowdog DAO) and 200,566 (Squid Game) unique screen names.

Step 2. For each screen name of the 27 seed lists, a list of its friends (contacts) was sourced with 2 screen names (source, target) per data row. Again, 27 lists resulted. In contrast to the seed lists of step 1, the contact lists qualify as relational data as it reflects communication links between source-target pairs of screen names.

4. Studies and Results

Study 1 proceeds on the assumption that Twitter screen names overlap across otherwise unrelated rug pulls suggesting that the same group of bots are being deployed across different rug pulls. To examine screen name overlap we considered all 351[3] pairwise intersections of screen names that could be generated from the 27 rug pulls studied.

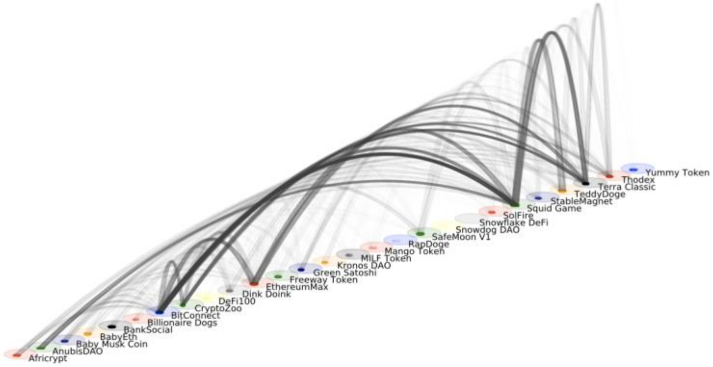

Figure 1. Screen Name Co-Occurrence across Rug Pulls

Fig. 1 visualizes screen name co-occurrence between different rug pulls. It highlights that in a number of rug pulls the same screen names occur. Differences in thickness of the bended

[2] Authoritative sources include government agencies, private or public regulating bodies, established news outlets or companies focused on crypto security or trade surveillance.

[3] (27*27-27) / 2 = 351

connecting lines expresses that rug pulls are affected to a different extent by screen name co-occurrence. Squid Game, Bitconnect, and Terra Classic stand out here. They are rug pulls that show high co-occurrence values in pairwise rug pull comparisons (thickness of bended connecting lines). They also come with the highest number of co-occurrences with other rug pulls (number of bended connecting lines).

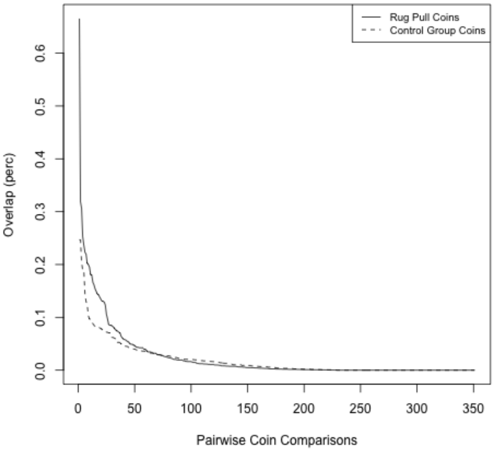

Figure 2. Screen Name Co-Occurrence across Rug Pull and Coins of a Control Group

Fig. 2 shows the screen name overlap across 27 rug pulls and across 27 coins of a control group. The figure plots on the x-axis all pairs of coins against the relative frequency of the screen name co-occurrence found for each of them. The resulting negative exponential distribution (solid line) reveals that rug pull coins share up to 66% of screen names (and possibly participants) with each other. At the same time, the long tail of the distribution suggests that many rug-pulls seem to be largely disjoint in terms of screen name overlap. The dashed line shows the comparison values of a control group of crypto currencies[4]. Here, the screen name co-occurrence ranges between 0.09% and 26%. Testing the differences between both distributions with a two-sample Kolmogorov-Smirnov test revealed a significant difference (D=.160, p<0.001). Clearly, high proportions of identical screen names showing up in pairwise comparisons of rug pulls is suspicious. But in itself it is not hard evidence for bot activity. The results of study 1 alone cannot rule out alternative

[4] The control group of coins was made up of the top 27 coins found on coinmarketcap.com on Feb 10, 2023 (ADA,APT,ATOM,AVAX,BCH,BUSD,CRO,DAI,DOGE,DOT,ETC,FIL,HBAR,LDO,LEO,LINK,LTC,MATIC,OKB,SHIB,SOL ,TON,TRX,TUSD,UNI,WBTC,XLM,XMR,XRP). The top three coins (BTC, ETH, USDT) were not included as the sheer volume of those coins made them unlikely matches for the rug pull coins studied.

explanations of the findings, e.g., that humans and not bots have created the screen name overlap spotted.

Study 2: The open questions of study 1 prompted a second study to find out more about overlapping screen names leveraging social network analysis (SNA). We examined the 25 screen names (Twitter accounts) with the highest in-degree and out-degree centrality, respectively, found in three largest rug pulls examined.[5] In our study, the out-centrality for a screen name reflects the number of retweets or replies actively *sent*. By contrast, the in-degree centrality is a measure of the number of retweets or replies that a screen *received*.

Table 1: Mean Bot Probability of Top 25 Senders and Receivers for 3 Major Rug Pulls

Rug Pull	messages	mean *p* in-centrality	mean *p* out-centrality
Squid Game	200,566	0.102	0.863
Terry Classic	36,062	0.296	0.581
Bitconnect	11,463	0.122	0.901

Table 1 has results of study 2 that connected centrality scores with bot probabilities. For each of the 3 × 2 × 25 screen names we collected its Botometer score, viz., its probability of being a bot (Yang et al, 2020). For the 25 nodes with the highest in- and out-degree centrality we averaged this score. We found the mean bot probability (Botometer Score) to be consistently higher for screen names with high out-degree centrality and vice versa. The findings offer answers to the questions that remained open after study 1. They suggest that in the networks analyzed the communication is mainly driven by bots and not by humans (Fig. 3. left) and that the bots are not non-tweeting follower-bots as they are actively targeting popular accounts, e.g., those of influential news outlets (Fig. 3. right).

[5] In-degree and out degree centrality are metrics provided by social network analysis. A node in directed graph on which many other nodes are pointing has a high in-degree centrality. In social network based on Twitter data such a node is a typical receiver. Vice versa, a node in directed graph that points massively onto other nodes has a high out-degree centrality. In an actor network based on Twitter data such a node is a typical sender.

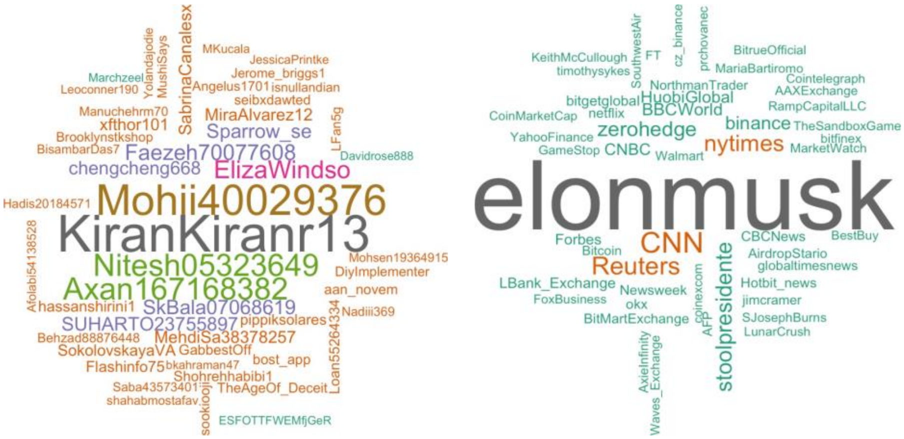

Figure 3. Twitter Screen Names with high out-degree Centrality (left) and with high in-degree Centrality (right)

5. Discussion

Bots are strongly involved in rug pulls and our explorative study identified distinctive patterns of bot deployment both within a single and also across several rug pulls. Furthermore, out work suggests that bot activity is significantly stronger in rug pulls than in other crypto currencies. *Within one rug pull*, we found strong evidence that bots drive the communication by the sheer number of messages and their specific targeting. The large number of messages sent out was reflected by a high out-degree centrality. Their specificity became evident when we looked at the receiving Twitter accounts. Here, we often find popular sites, many of them news outlets, e.g., Reuters, CNN or Bloomberg. It is tempting to conjecture that bots may repeatedly reply to Tweets of an established site in order to build up trust simply by what is known in psychology as a mere-exposure effect (Zajon, 1968). *Bot deployment across rug pulls* could be identified via screen name co-occurrence identifiable across multiple rug pulls. Together with aforementioned results it suggests that often the same bots are being used across rug pulls. This finding raises questions and concerns. It obviously reflects professional coordinated efforts to defraud investors possibly via bot net services. We did not study the actual effects bots have on humans. But it can be reasonably expected that bot activities identified in our studies create a false sense of interest in a project, making it difficult for investors to distinguish between genuine interest in a project and artificially generated buzz/hype. In our analysis we harnessed historical data. Follow up research is required to find out whether bot activity patterns can actually predict future rug pulls. Further research is required to study those effects and whether the patterns found also characterize other promote-hit-and-run scams.

References

Aljabri, M., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, D. M. (2023). Machine learning-based social media bot detection: a comprehensive literature review. *Social Network Analysis and Mining*, *13*(1), 20.

Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Ver Steeg, G., & Galstyan, A. (2021). Identifying and analyzing cryptocurrency manipulations in social media. *IEEE Transactions on Computational Social Systems*, 8(3), 607–617.

Murthy, D., Powell, A. B., Tinati, R., Anstead, N., Carr, L., Halford, S. J., & Weal, M. (2016). Automation, algorithms, and politics| Bots and political influence: A sociotechnical investigation of social network capital. *International Journal of Communication*, *10*, 20.

Nghiem, H., Muric, G., Morstatter, F., & Ferrara, E. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*, 182, 115284.

Orabi, M., Mouheb, D., Al Aghbari, Z., & Kamel, I. (2020). Detection of bots in social media: a systematic review. Information Processing & Management, 57(4), 102250

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer Nature.

Schuchard, R., Crooks, A., Stefanidis, A., & Croitoru, A. (2019). Bots in nets: empirical comparative analysis of bot evidence in social networks. In *Complex Networks and Their Applications VII: Volume 2 Proceedings The 7th International Conference on Complex Networks and Their Applications COMPLEX NETWORKS 2018 7* (pp. 424-436). Springer International Publishing.

Solidus, I. (2022). The Rug Pull Report. New York. Retrieved from https://www.soliduslabs.com/reports/rug-pull-report

Tardelli, S., Avvenuti, M., Tesconi, M., & Cresci, S. (2020). Characterizing social bots spreading financial disinformation. In G. Meiselwitz (Ed.), Social computing and social media. design, ethics, user behavior, and social network analysis (pp. 376–392).

Yang, K. C., Varol, O., Hui, P. M., & Menczer, F. (2020, April). Scalable and generalizable social bot detection through data selection. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 34, No. 01, pp. 1096-1103).

Zajonc, R. B. (1968). Attitudinal Effects of Mere Exposure. Journal of Personality and Social Psychology, 9, 2, 1–27.