Selected Papers of #AoIR2023:
The 24th Annual Conference of the
Association of Internet Researchers
Philadelphia, PA, USA / 18-21 Oct 2023

EXPLORING THE DARK SIDE OF CRYPTOCURRENCIES ON FACEBOOK AND TELEGRAM: UNCOVERING MEDIA MANIPULATION AND "GET-RICH-QUICK" DECEPTIVE SCHEMES

Massimo Terenzi
University of Urbino

Introduction

New technologies such as blockchain and cryptocurrencies decentralize transactions while introducing new vulnerabilities and "exposing the economy to threats unprecedented" (Dipietro et al. 2021, p. 66). In particular, when it comes to cryptocurrencies, scholars argue that the risks associated with cryptocurrencies are still unclear. Particularly, in the era of social media, the so-called information-based manipulation, perpetuated through spreading false rumors or information, can be conducted through numerous sources of information. One recent case that has garnered widespread attention is the GameStop short squeeze (Jetty et al. 2022). In January 2021, a group of Reddit users gathered in the subreddit R/WallStreetBets to drive up the stock price of GameStop, a struggling video game retailer. The coordinated effort caused significant financial losses for established hedge funds that had bet against the company's success. This incident highlights the power of coordination on social media in shaping financial markets and its potential to disrupt traditional investment strategies. However, it also raises questions about the ethical implications of manipulating public sentiment through media channels. While it is true that many of these Reddit users urge a shifting of power from the financial establishment into the hands of ordinary people, other news stories have revealed the great risks that these broader movements involve. For example, in 2022, the collapse of FTX, the third-largest cryptocurrency exchange by volume, caused hundreds of thousands of small investors to lose billions, in what has been defined as a "fraud of epic proportions" by US federal prosecutors (Sorkin et al. 2022).

Some preliminary works investigate discussions on platforms such as Reddit (Glenski et al. 2019), Twitter, Discord, or Telegram (Nizzoli et al. 2020; Feder et al. 2018; Mirtaheri et al. 2019) with the aim of mapping both the ecosystem cryptocurrencies and possible forms of manipulations. Nonetheless, the research still lacks a clear and comprehensive picture of how widespread the phenomenon is, its actors, venues, and strategies of

Suggested Citation (APA): Terenzi, M. (2023, October). Exploring The Dark Side Of Cryptocurrencies On Facebook And Telegram: Uncovering Media Manipulation And "Get-Rich-Quick" Deceptive Schemes. Paper presented at AoIR2023: The 24th Annual Conference of the Association of Internet Researchers. Philadelphia, PA, USA: AoIR. Retrieved from http://spir.aoir.org.

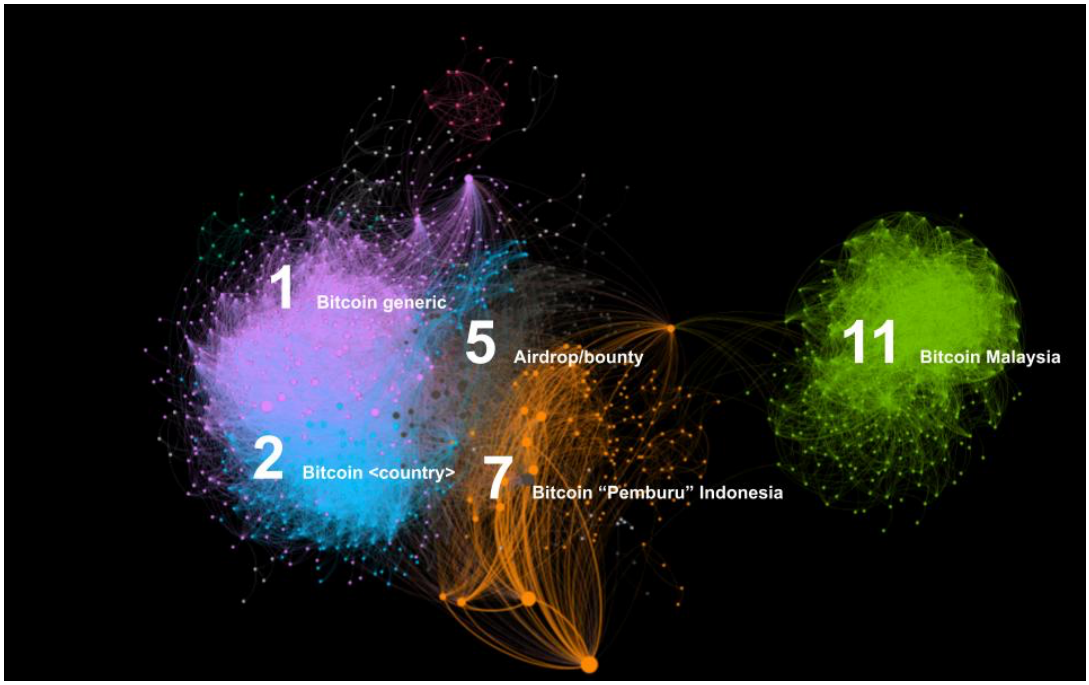
media manipulation (Donovan, 2020) in the context of financial markets and throughout the whole ecosystem. Moreover, the question of evaluating the impact of such illegal manipulative practices on mainstream social media platforms still remains unanswered.

To fill this gap, this work focuses on Facebook, as a venue for possible manipulative practices or scams related to cryptocurrencies. In this regard, it is useful to refer to the concept of coordinated inauthentic behavior: the activity of some people who employ groups of social accounts to carry out coordinated actions for the dissemination of content on social media, with manipulative purposes. Specifically, Coordinated Link Sharing Behaviour (CLSB) is a strategy for boosting the reach and distribution of links by using coordinated activities performed by Facebook accounts that repeatedly share the same content in a very short period from each other (Giglietto et al., 2020a). This is done through bots and automatic systems (Cresci 2020), fake or compromised accounts, which take on the appearance of real users, that is, with behavior that is perfectly plausible in the eyes of the platforms. For the latter, therefore, it becomes increasingly difficult to distinguish the activity of real users from that of bogus accounts, created ad hoc (Acker 2018, p. 4).

Methods

The CooRnet library, based on the R software environment, was used to identify networks of coordinated link-sharing accounts on Facebook (Giglietto et al., 2020b). CooRnet uses social media data to detect such coordinated networks of accounts that repeatedly share the same links in a very short amount of time. CooRnet has been widely used and increasingly adopted by scholars and research centers specializing in the detection and analysis of coordinated behavior on social media and disinformation, providing results capable of linking coordination to the dissemination of political information and disinformation during electoral and other circumstances (e.g. Ayers et al., 2021; Broniatowski, 2021; DFRlab, 2020; Giglietto et al., 2019; Giglietto et al., 2020b).

This work stems from a broader investigation into disinformation in Africa (Giglietto et. al 2022) where we identified different clusters of Facebook entities that shared content related to the world of cryptocurrencies in a coordinated way. One of these clusters appeared to be particularly relevant, being made up of 152 groups, with 521 shared domains (521 full domains, with 477 parent domains).



These signs of coordination allowed us to formulate our first research question, which guided our investigation into the intersection between Facebook and the crypto ecosystem:

RQ1a: to what extent the content circulated by the crypto-cluster on Facebook can be deemed as problematic content?

RQ1b: how many of the circulated links are presently active and how many are inactive?

RQ2: what types of crypto initiatives emerge?

To analyze this cluster related to cryptocurrencies, we collected through CrowdTangle 100,000 posts produced by the cluster itself, and extracted the links present in the posts of our dataset for a total of 12,033 URLs, calculating the sum of the interactions of the posts that linked to the same URLs. We, therefore, selected the 1,052 URLs that scored the most interactions. Then, to measure the relationship between problematic and non-problematic content (RQ1a), we verified how many of the links in our sample were active (RQ1b), through the automatic bulk check of the HTTP response status codes of the sampled URLs dataset.

Results

We found that a significant part of the links checked was inactive, and found that the absolute most widespread domain among the links of our sample was that of Telegram, a noteworthy 47%. Namely, links were related to Telegram bots, channels, groups, or profiles. We then manually checked all the Telegram links to better understand their status and found that a large part of the accounts was

labeled by the platform as "scams".

Lastly, to answer RQ2 we analyzed the remaining part of active Telegram channels, bots, and groups. The accounts displayed names, usernames, or descriptions referring to the possibility for users to receive free cryptocurrency sums. Cryptocurrencies were allegedly distributed to users as a reward for performing certain actions, such as clicking on social media or sending users' data. In some cases, users were promised to earn cryptocurrencies by watching advertisements, or by playing so-called "bot games". A minimum threshold is often required for the withdrawal of the accumulated rewards and the instantaneousness of the payment of the rewards is almost always mentioned, as well as the reliability of the bots ensured.

Some bots referred to the so-called "Airdrops", perhaps the most ephemeral category but also the most representative of all the operations we have observed, and the theme of the attention economy itself. Airdrops refer to short crypto-events in which small amounts of cryptocurrency are distributed completely free of charge. Airdrops represent an effective marketing strategy carried out by those who launch new crypto-projects, to achieve wider adoption of the new cryptocurrency, since the presence of mass adoption is considered a good metric. Conversely, Airdrops could also give a false impression of growth to users, that is, an inauthentic amplification, that is, letting users believe that the cryptocurrencies that are launched are much more widespread than they are.

This paper explores the overlap between the cryptocurrency community and social media, analyzing how crypto-related projects are disseminated as a new type of problematic content on Facebook and Telegram.

References

Acker, A. (2018), “Data Craft: The Manipulation of Social Media Metadata”, in Data & Society, Retrieved from: https://datasociety.net/wp-content/uploads/2018/11/DS_Data_Craft_Manipulation_of_Social_Media_Metadata_.pdf

Ayers, J. W., Chu, B., Zhu, Z., Leas, E. C., Smith, D. M., Dredze, M., & Broniatowski, D. A. (2021). Spread of Misinformation About Face Masks and COVID-19 by Automated Software on Facebook. JAMA internal medicine, 181(9), 1251–1253. https://doi.org/10.1001/jamainternmed.2021.2498

Broniatowski, D. A. (2021). Towards statistical foundations for detecting coordinated inauthentic behavior on Facebook, https://iddp.gwu.edu/sites/g/files/zaxdzs3576/f/downloads/Coordinated%20Behavior%20On%20Facebook;%20Broniatowski.pdf

Cresci, S. (2020), A decade of social bot detection, Communications of the ACM (Forthcoming)

DFRlab (2020). Why the debunked COVID-19 conspiracy video “Plandemic” won’t go away https://medium.com/dfrlab/why-the-debunked-covid-19-conspiracy-video-plandemic-wont-go-away-c9dd36c2037c

Dipietro, R., Raponi, S., Caprolu, M., & Cresci, S. (2021). New Dimensions of Information Warfare. In New Dimensions of Information Warfare (pp. 1-4). Springer, Cham.

Donovan, J. (2020). The lifecycle of media manipulation. In C. Silverman (Ed.), Verification handbook for disinformation and media manipulation. European Journalism Centre.

Feder, A., Gandal, N., Hamrick, J. T., Moore, T., Mukherjee, A., Rouhi, F., & Vasek, M. (2018). The economics of cryptocurrency pump and dump schemes (No. 13404). CEPR Discussion Papers.

Giglietto, F., Righetti, N., Marino, G., Rossi, L. (2019). Multi-Party Media Partisanship Attention Score: estimating partisan attention of news media sources using Twitter data in the lead-up to 2018 Italian election. Comunicazione Politica, n.1/2019, pp. 85-108. DOI: 10.3270/93030

Giglietto, F., Righetti, N., & Rossi, L. (2020a). CooRnet. Detect coordinated link-sharing behavior on social media. http://coornet.org

Giglietto, F., Righetti, N., Rossi, L., & Marino, G. (2020b). It takes a village to manipulate the media: coordinated link sharing behavior during 2018 and 2019 Italian elections. Information, Communication and Society, 1–25.

Giglietto, F., Olaniran, S., Mincigrucci, R., Marino, G., Mottola, S., & Terenzi, M., Blowing on the Fire: An Analysis of Low Quality and Hyper Partisan News Sources Circulated by Coordinated Link Sharing Networks in Nigeria (July 13, 2022). Available at SSRN: https://ssrn.com/abstract=4162030 or http://dx.doi.org/10.2139/ssrn.4162030

Glenski, M., Saldanha, E., Volkova, S., (2019) Characterizing speed and scale of cryptocurrency discussion spread on Reddit, in The 28th International Conference on World Wide Web (WWW'19), pp. 560–570

Jetty, S., Chen, T., & Mirza, R. (2022), Meme war: the Gamestop short squeeze campaign that gamed the financial algorithm, The Media Manipulation Casebook, Retrieved from: https://mediamanipulation.org/case-studies/meme-war-gamestop-short-squeeze-campaign-gamed-financial-algorithm

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.

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., & Ferrara, E. (2020). Charting the landscape of online cryptocurrency manipulation. IEEE Access, 8, 113230-113245.

Sorkin, A.R., Mattu, R., Warner, B., Kessler, S., Gandel, S., De La Merced, M.J., Hirsch, L., & Livni, E. (2022), The New York Times, Retrieved from: https://www.nytimes.com/2022/12/23/business/dealbook/sbf-ftx-epic-fraud-lawsuit.html