The Conspiracy Money Machine: Uncovering Telegram's Conspiracy Channels and their Profit Model.

Vincenzo Imperati
imperati@di.uniroma1.it
Sapienza University of Rome

Massimo La Morgia
lamorgia@di.uniroma1.it
Sapienza University of Rome

Alessandro Mei
mei@di.uniroma1.it
Sapienza University of Rome

Alberto Maria Mongardini
mongardinia@di.uniroma1.it
Sapienza University of Rome

Francesco Sassi
sassi@di.uniroma1.it
Sapienza University of Rome

Abstract

*

In recent years, major social media platforms have implemented increasingly strict moderation policies, resulting in bans and restrictions on conspiracy theory-related content. To circumvent these restrictions, conspiracy theorists are turning to alternatives, such as Telegram, where they can express and spread their views with fewer limitations. Telegram offers channels—virtual rooms where only administrators can broadcast messages—and a more permissive content policy. These features have created the perfect breeding ground for a complex ecosystem of conspiracy channels.

In this paper, we illuminate this ecosystem. First, we propose an approach to detect conspiracy channels. Then, we discover that conspiracy channels can be clustered into four distinct communities comprising over 17,000 channels. Finally, we uncover the "Conspiracy Money Machine," revealing how most conspiracy channels actively seek to profit from their subscribers. We find conspiracy theorists leverage e-commerce platforms to sell questionable products or lucratively promote them through affiliate links. Moreover, we observe that conspiracy channels use donation and crowdfunding platforms to raise funds for their campaigns. We determine that this business involves hundreds of thousands of donors and generates a turnover of almost $66 million.

1 Introduction

Conspiracy theories have been an integral part of human history, offering alternative interpretations for complex events [100]. The most common definition, which we use in our work, is that a conspiracy theory is a belief that an event or situation is the result of a secret plan made by powerful people [40]. A notorious example is the Flat Earth theory [36]. Despite centuries of scientific evidence proving the Earth's roundness, the theory continues to be discussed and promoted by several communities [47, 72]. Throughout history, several conspiracy theories have emerged on a wide range of topics, like the Moon Landing Hoax [46], JFK Assassination [109], Holocaust Denial [66], Elvis Presley's Faked Death [34], and 9/11 Conspiracy Theories [93].

Nowadays, with the advent of the Internet and social media, conspiracy theories have found new outlets to spread and gain traction [44, 82]. A notable example is the Pizzagate conspiracy theory, which originated and spread on online bulletin boards in 2016 [99]. In 2017, online forums acted as a catalyst for QAnon conspiracy theories [39], which alleged that a global cabal of malevolent elites was involved in heinous activities. The advent of the COVID-19 pandemic has sparked various online conspiracy theories, including claims that the virus is a bio-weapon for population control [56], and that 5G technology is somehow linked to the spread of the virus [8]. Finally, on January 6, 2021, a pro-Trump mob stormed the U.S. Capitol building, disrupting the certification of the 2020 presidential election results [74]. These incidents led the major social media platforms to implement content moderation to curb the dissemination of these theories [18]. In response, conspiracy theorists are flocking to less moderated platforms to freely share their views. Anecdotal evidence from various news sources [4, 20, 103] underscores Telegram, one of the most popular instant messaging applications, as one such platform. This is not surprising, as Telegram offers a permissive content policy and channels—virtual rooms where the admins can broadcast messages to large audiences.

In our work, we perform a large-scale study of Telegram to shed light on its ecosystem of conspiracy channels. We propose a novel approach to identify channels related to conspiracy theories by examining the URLs they share. In particular, we leverage previous scientific work on conspiracy theories to build the Conspiracy Resource Dataset, which contains a list of online resources (*e.g.,* YouTube videos, Reddit posts) linked to conspiracy theories. Then, we use the TGDataset, a public dataset of over 120,000 Telegram channels, to find channels sharing conspiracy-related URLs with their subscribers. Then, we utilize a community detection algorithm

*Published in the Proceedings of the XXX (XXX 2025). Please cite accordingly.

to analyze Telegram communities, finding that conspiracy-related channels are clustered in four specific communities. We characterize these communities by analyzing their language and most influential channels. We refer to the channels contained in these communities as the Conspiracy Channel Dataset. The analysis of the Conspiracy Channel Dataset highlighted the presence of channels actively seeking to profit from their subscriber. We characterize and quantify this phenomenon, focusing on three monetization strategies: donations, crowdfunding campaigns, and affiliate programs. First, we focus on analyzing donation and crowdfunding platforms. While we could not extract information about donation URLs, we find several insights about crowdfunding campaigns. Indeed, crowdfunding projects sponsored by conspiracy channels collected millions of dollars donated by over 900,000 backers. Moreover, analyzing the top-funded campaigns, we find they are linked to far-right support, COVID-19 restriction opposition, and truth-revealing documentaries against governments and powerful individuals. Finally, we also find fake charity campaigns that are outright scams. Then, we find that conspiracy theorists exploit the lenient product policies of eBay, Teespring, and Etsy to promote questionable items to their subscribers, such as 5G shields, EMF stone protectors, and healing wands. Moreover, they exploit Amazon's tolerant book content policies to self-publish and profit from books claiming to "reveal the truth" about several topics. Our work makes the following contribution:

- **Conspiracy Datasets.** We release two datasets. The first one is the Conspiracy Resource Dataset, a collection of conspiracy-related web resources gathered through an extensive literature review. The second is the Conspiracy URLs Dataset, a list of 198,818 resolved unique URLs shared by conspiracy theory-related channels. We believe these datasets can enable further studies on identifying and characterizing conspiracy communities on other platforms and determining their activities.

- **Conspiracy Detection and Analysis.** We propose an approach to identify conspiracy communities on Telegram, finding four large communities comprising 17,829 channels. We characterize each community by analyzing their language and their most influential channels.

- **Conspiracy Monetization.** Finally, we identify the potential strategies that conspiracy theorists can employ to generate revenue from the subscribers of Telegram channels. We find that the most popular approaches involve donations, crowdfunding campaigns, and affiliate programs. We discover 123K URLs linked to donation platforms and more than 24K URLs related to crowdfunding campaigns. Quantifying the amount of money raised with projects sponsored by conspiracy channels, we discovered that they amassed almost $66M donated by over 906K backers.

2 How Telegram works

Telegram is one of the most prominent instant messaging application platforms, with over 700 million active users in 2023 [3]. Like most instant messaging applications, Telegram provides one-to-one messaging. Indeed, Telegram users can easily engage in conversations by exchanging text messages, multimedia content, and files. Moreover, users can also create and join groups—chats where any member can post content. This feature allows users to create communities around shared interests for discussions, event planning, and coordination.

Channels. One of the core features of Telegram is channels, chats designed to provide one-to-many messaging. Indeed, the only user who can send messages into a channel is the admin. Other Telegram users can freely join a channel and read its posts but cannot send messages. This feature allows the admin to share content with a huge number of subscribers, making Telegram channels a prime broadcasting medium for disseminating news and announcements. Channels on Telegram are identified by unique usernames, have a title, and may include a description and a chat picture. Moreover, while group members can see which users are in their group, only a channel admin can access the list of subscribers.

Message forwarding Another core functionality for distributing content within Telegram is message forwarding. Indeed, users (or admins of a channel) can easily forward a message from one chat to another. The forwarded message displays the original message's author, serving as a bridge between groups, channels, and private chats.

3 Related work

Telegram has recently gained substantial attention, with several prior studies investigating questionable activities on the platform Weerasinghe et al. [107] studied "pods", organized groups created to artificially boost Instagram popularity. Other studies have explored Telegram's use in cryptocurrency market manipulations like pump and dump [59, 64] and Ponzi schemes [78]. Additionally, researchers have noted its misuse by terrorist organizations for propaganda and recruitment [27, 108, 110]. Research on conspiracy theories on Telegram is limited, with most studies focusing on other social media platforms. Here is a report on these studies.

Telegram. Hoseini et al. [55] examined 161 QAnon groups on Telegram, analyzing their toxicity and performing topic modeling to understand the QAnon narrative in multiple languages. Garry et al. [49] focuses on analyzing 35 QAnon Telegram channels, discovering that they spread disinformation messages to recruit new adepts. La Morgia et al. [61, 63] analyze over 120,000 Telegram channels, focusing on detecting fakes and clones. They discovered that these channels are used to lure users into conspiracy-related channels. Unlike these studies, we examine the overall landscape of conspiracy-related channels on Telegram, propose a method to identify

their communities, and analyze their profit model.

YouTube. Leidwich et al. [65] explore whether YouTube's recommendation algorithm promotes radicalization by guiding users to increasingly extreme content. They categorized 816 channels, including 79 conspiracy ones. Clark et al. [33] leverage the dataset of [65] to find YouTube communities. They create an embedding for the channels considering the channel's subscribers. Then, they leverage cluster algorithms to reveal the YouTube communities, finding QAnon and conspiracy-related ones.

Reddit. Phadke et al. [85] analyzed conspiracy theories on Reddit using the RECRO model to study user radicalization. They examined 169 million contributions from 36,000 users, identifying four engagement trends. Papasavva et al. [79] focused on the QAnon conspiracy, analyzing 4,949 "Q drops" and their dissemination on Reddit, finding continued sharing even after QAnon subreddits were banned. Engel et al. [45] analyze the submission of 13K users in 19 QAnon-related subreddits. They discover they are active across various subreddits, often posting harmful content from low-quality sources. Phadke et al. [84] analyze 56 conspiracy communities on Reddit, creating a ground truth of 60k users to develop a machine learning model to predict if a Reddit user will eventually join conspiracy communities.

Voat. Voat, a Reddit clone, gained notoriety after Reddit banned Pizzagate and QAnon-related subreddits [101]. Papasavva et al. [80] analyzed over 150,000 posts from the largest QAnon forum on Voat, finding a focus on Trump and US politics. Mekacher et al. [71] created a dataset of over 2.3 million Voat submissions, discovering that many active subverses centered on hate speech and conspiracy theories.

4chan/8kun. 4chan [21], an image-based bulletin board, has been linked to conspiracy theories, notably the PizzaGate conspiracy [95]. Papasavva et al. [81] analyzed over 3.5 million messages on 4chan's */pol* board, finding antisemitic conspiracy theories. Similar content is found on 8kun, a platform associated with white supremacism and hate crimes [53, 54]. Aliapoulios et al. [79] discovered that 8kun QAnon threads are significantly larger than those on 4chan.

Monetization misuse and frauds. Ballard et al. [16] leverage the datasets from [33, 65] to investigate the monetization strategies of YouTube conspiracy channels. They find that these channels have a high prevalence of predatory or deceptive ads, are often demonetized, and use alternative income sources via third-party platforms. Broniatowski et al. [25] conducted a study involving 1,448 respondents and found that most are unlikely to pay for online conspiracy content. However, respondents who avoid mainstream media and rely on social media for news are more inclined to pay for such content. Chachra et al. [28] study cookie-stuffing, a technique used to divert revenue commissions in affiliate marketing networks. They highlight the fraud mechanisms and identify which categories of merchants are most targeted, noting that scammers employ a wide range of evasive techniques.

4 Methodology

To uncover the structure of channels in Telegram that are related to conspiracy theories, we build a methodology consisting of four steps: First, data collection (including the introduction of a new dataset); second, detection of "conspiracy channels;" third, identification of communities of channels linked to conspiracy theories.

4.1 Data collection

We leverage two datasets. The first one is the TGDataset [62], the largest collection of public Telegram channels, with over 120,000 channels and 400 million messages. The dataset contains all the messages shared by the collected channels until July 31, 2022. This dataset provides information about the channels (*e.g.,* their title, description, and creation date), all the messages sent with their timestamp and whether a message has been forwarded, and from which channel it originated. Then, we build a novel dataset, the Conspiracy Resources Dataset, that we describe in the following.

4.1.1 Conspiracy Resources Dataset

This dataset is a collection of conspiracy-related resources extracted from an extensive review of the previous works about conspiracy theories reported in Section 3. To construct this dataset, we focus on studies that provide explicit pointers to the sources they analyze, either within the manuscript or in dedicated repositories. In the following, we report for each platform the number of resources we find and the reference article:

- **YouTube.** We follow the approach of [16] and use two repositories of YouTube channels reported in [33, 65]. These repositories contain a list of 4,007 YouTube channels manually labeled as conspiracy-related. For each channel, we extract the complete list of their videos, resulting in a total of 1,973,439 video IDs.
- **Reddit.** We leverage the work of [45, 79, 84, 85] to collect a list of 92 subreddits identified as conspiracy-related.
- **Voat.** We consider 3 Voat subverses related to the QAnon conspiracy theory reported in [71, 80].
- **4chan/8kun.** We did not find any resource specifically related to conspiracy theories on 4chan from previous work. Indeed, the infamous */pol* discussion board is too general and discusses topics unrelated to conspiracy theories. Instead, we collect a list of 7 boards related to QAnon on 8kun from the work in [79].
- **Websites.** From the work of Aliapoulios et al. [79], we collect 6 websites that are well-known aggregators of Q drops spread by the QAnon conspiracy. Then, we use

Table 1: Summary of the conspiracy-related resources we find in previous work and related URLs we extract from Telegram.

Paper	Type	# Resources	# URLs
[16, 33, 65]	YouTube	4,007 channels	147,349
[45, 79, 84, 85]	Reddit	92 subreddits	17,889
[71, 80]	Voat	3 subverses	21
[79]	8kun	7 boards	3,787
[54, 79]	Web	128 websites	299,262

OpenSources [1] (used also to study QAnon in [54]) to extract 122 website domains linked to conspiracy theories.

Although there are other works mentioning conspiracy theories in other platforms like Parler [9, 17] or Twitter [8], they do not publicly release their data-sets or provide URLs related to conspiracy theories that we can use in our study. Tab 1 reports all the resources we find and the related papers. Moreover, we release in [15] the full dataset of extracted resources.

4.2 Conspiracy channels detection

We devise a methodology that combines the TGDataset and the Conspiracy Resources Dataset to find channels on Telegram related to conspiracy theories. The detection is performed in four steps: First, we extract and pre-process URLs from the TGDataset, then we perform the match with the resources found in the Conspiracy Resources Dataset, we use graph analysis to find clusters of conspiracy-related channels, and finally, we validate our results.

4.2.1 Data extraction and pre-processing

We parse all the messages (498,320,597) in the 120,979 TGDataset's channels and use regular expressions to extract all the URLs. In this way, we obtain 205,046,775 URLs, 84,809,578 of which are unique. A first analysis of the URLs reveals that 20.2% (17,140,343 URLs) have been shortened using URL shortener services such as *bit.ly* (2,368,953 occurrences) or *if.tt* (1,462,885 occurrences). Since our methodology for detecting conspiracy theories channels revolves around identifying URLs associated with conspiracies, we want to ensure we do not miss any of them because it has been shortened. Thus, between July and September 2023, we resolved the shortened URLs by sending HEAD requests to the shortening service using the Python Requests library [29].

4.2.2 URLs matching

Then, we extract URLs associated with the resources collected in the Conspiracy Resources Dataset. We start by using the conspiracy channels and videos' IDs in the Conspiracy Resources Dataset to search YouTube URLs related to conspiracy theories. We detect 2,446 URLs (468 unique) linking to conspiracy channels and 144,903 URLs (58,099 unique) linking to conspiracy videos. The most widely shared channel is *Fall Cabal*, a channel associated with the "Fall of the Cabal" [7], an antisemitic documentary used to recruit QAnon followers affiliated with Dutch conspiracy theorist Janet Ossebaard [70]. Instead, for Reddit, 8kun, and Voat, we extract all the URLs linking to conspiracy subreddits, boards, and subverses, respectively. We find 17,889 Reddit URLs (17,238 unique), 3,787 8kun URLs (2,542 unique), and 21 Voat URLs (11 unique). Most of the URLs we find are related to the *r/conspiracy* subreddit, the largest conspiracy theory discussion board on Reddit [85].

Finally, we extract all the URLs having the domain of the flagged websites, finding 299,262 URLs (120,463 unique) from 307 different domains. The website providing the most matches is Zerohedge, a far-right news aggregator known for spreading conspiracy theories, particularly about COVID-19 [75, 76]. The second most popular is InfoWars, well-known for promoting conspiracy theories and fake news [31, 111]. We also detect over 10k URLs linking to the *qagg.news* website, a popular repository that stores the messages of the QAnon conspiracy theory [49, 79].

In total, we find 468,308 URLs (198,818 unique) posted by 11,713 Telegram channels. We publicly release the extracted URLs in [15] to enable further studies. In the following, we will refer to this dataset as **Conspiracy URLs Dataset**. Tab. 1 succinctly reports the number of URLs collected inside the Telegram channels divided by resource type.

4.2.3 Clustering conspiracy channels

The previous analysis shows 11,713 Telegram channels that posted at least one message with a link to a conspiracy-related resource. We study how and if these channels are connected to better understand the phenomenon. To do so, we follow the approach of [63] and build the Telegram forwarding graph for the whole dataset of channels. The forwarding graph is a graph $G = (V, E)$ in which nodes in G are channels and an edge $u \rightarrow v$ in E represents the presence in u of a message forwarded from channel v. Users of channel u can follow the forwarded message and reach channel v. Thus, edges represent the possible flows through channels of users following forwarded messages.

Once we have built the graph, we identify communities—subsets of nodes within the graph that are highly connected with respect to the rest of the graph [86]. In this specific case, a community is a subset of Telegram channels that consistently forward messages among themselves and rarely forward messages from channels of the other communities. To perform community detection, we use the Leiden algorithm [97] since it is widely adopted and has proven to be effective in identifying communities in social graphs (*e.g.,* Twitter [23, 91]).

We compute the optimal number of communities with regard to modularity—a metric that measures how much the partitioning is better than a random partition. The metric ranges between 1 to -1, and we obtain a score of 0.78. With this approach, we identify 47 distinct communities of channels. Then, we analyze how the conspiracy-related channels are distributed inside these communities. To illustrate this analysis, we report the scatterplot in Fig. 1. The Figure shows a dot for each community, the number of channels in the community (x-axis), and the percentage of conspiracy channels (y-axis). It is evident that some communities (highlighted in red) stand out due to an unusually high concentration of conspiracy-related channels. In particular, one community has 86% of potential conspiracy channels, while the other 3 have more than 40%. These four communities contain 17,950 channels, almost 15% of all the channels in the TGDataset. Furthermore, a vast fraction (76.6%) of the channels containing at least one link obtained from the Conspiracy Resource Dataset belong to one of these four communities. In the following, we will refer to the channels in the four communities as Conspiracy Channel Dataset and to all the links in these channels as **Extended Conspiracy URLs Dataset**. Given the relevance of these communities for understanding the diffusion of conspiracy theories on Telegram, we will analyze them in detail.

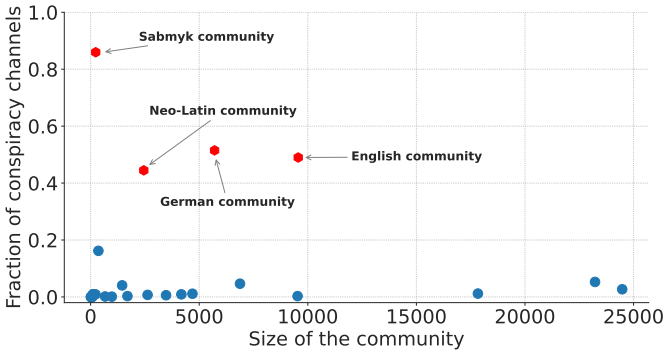

Figure 1: Each dot represents a community. The y-axis shows the percentage of conspiracy-related channels, and the x-axis represents the community size (number of channels). We highlight in red the communities that show an outstanding amount of conspiracy-related channels.

4.2.4 Clustering validation

As mentioned in the previous section, a substantial portion of channels identified by the clustering algorithm as part of conspiracy communities do not contain links from the Conspiracy Resource Dataset. Since we have less evidence that these channels are conspiracy-related, we manually validate a sample of these channels to evaluate and mitigate the presence of false positives.

To perform this task, we select the top 5% of channels by the number of subscribers, amounting to 414 channels, and perform a manual analysis to assess whether they contain conspiracy theory-related content. Three researchers independently reviewed and analyzed the content of each channel, annotating the presence of conspiracy-related content. We adopted a conservative approach, flagging only channels explicitly mentioning conspiracy theories, excluding those implying or hinting at them. Furthermore, to minimize the likelihood of false positives, a unanimous agreement among all researchers was required to classify a channel as conspiracy-related. The analysis shows that 293 channels (70.77%) are related to conspiracy theories. In the following, we discard the 121 channels not linked to conspiracy theories while we provide a detailed examination of false-positive channels in Sec. 6.

4.3 A look into Conspiracy Communities

This section offers an overview of the discovered communities, focusing on their most influential channels. We use the Hub and Authorities algorithm (HITS) [41], originally developed to identify relevant web pages [60]. The algorithm identifies good hubs as those linking to high-authority pages, and good authorities as those linked by many good hubs.

We adapt this idea to the Telegram graph, defining a channel as authoritative if many good hubs forward its messages, and as a good hub if it forwards messages from many authoritative channels. In our analysis, we are particularly interested in highly authoritative channels. Indeed, according to the definition, these channels are very influential in the community as their messages are widely forwarded. Using the HITS algorithm, we identify and analyze the top five channels with the highest authority scores in each community. Moreover, to better analyze each community, use LangDetect [38] to identify the languages used in channels. In the following, we will analyze separately each community.

English community. This is the largest community, with 9,491 channels and more than 26 million messages sent. More than 89% of these channels communicate using the English language. The most influential channel of this community is *Disclose.tv*, a website that discusses alternative viewpoints on the news and is notorious for propagating conspiracy theories [89]. Following closely in terms of authority ranking is *Tommy Robinson News*, a channel allegedly managed by Tommy Robinson, a British activist known to promote conspiracy theories, particularly those related to the threat of Islam for Western societies [35]. *RT News* is a state-funded international media company headquartered in Russia, known for its alleged bias and for disseminating information that supports the Russian government's positions [37, 106]. About the *Police frequency* channel, by searching online, we did not find evidence that this channel is associated with well-known entities or individuals linked to conspiracies. However, looking at its messages, we find that it is a far-right channel that focuses on American news about law enforcement, anti-gun

Table 2: Top channels by authority ranking in each conspiracy community.

HITS	English community	German community	Neo-Latin community	Sabmyk community
1	Disclose.tv	Fakten Frieden #FreeJanich	LA QUINTA COLUMNA TV	sabmyk
2	Tommy Robinson News	Eva Herman Offiziell	Noticias Rafapal	ChicagoReporter
3	RT News	Uncut-News.ch "Das Original"	El Investigador.org	GreatAwakeningChannel
4	Police frequency	Freie Medien	COVID-1984	CapitolNews
5	Covid Red Pills	#freejanich Oliver Janich öffentlich	DESPERTADOR DE LA MATRIX	NicolaTeslaNews

control, and anti-immigration. Finally, *Covid Red Pills* claims to unveil the truth behind the COVID-19 pandemic.

German community. The German community comprises 5,688 channels that share more than 17 million messages. Over 94% of these channels communicate in German. Among the most influential channels, three of them, *Fakten Frieden #FreeJanich* , *Uncut-News.ch "Das Original"*, and *Freie Medien*, propose themselves as alternative media that share unmanipulated and free news, emphasizing their independence from government or political parties. Instead, the other two channels feature well-known German personalities. *Eva Herman Offiziell* claims to be the official channel of Eva Herman, a former German news presenter known for promoting various conspiracy theories [48]. The final channel focuses on Oliver Janich, a prominent supporter of QAnon in Germany [102], well known for writing conspiracy books about 9/11.

Neo-Latin community. In this case, the community is not predominantly monolingual, with 58% of the channels primarily communicating in Spanish, 21% in Portuguese, and 16% in Italian. This community consists of 2,415 channels and has shared over 8.8 million messages. Similarly to the German community, the most influential channels present themselves as independent media, advocating freedom of speech and claiming freedom from government influence. Notably, three channels (*El Investigador.org* , *COVID-1984* and *DESPERTADOR DE LA MATRIX*) mostly focus on COVID-19 conspiracies, claiming that the virus is created in a laboratory, the vaccine was created to reduce the population, and the World Health Organization (WHO) is a genocidal organization.

Sabmyk community. The last community stands out, with over 86% of its 235 channels sharing URLs related to conspiracy theories. Almost the entire community (95% of channels) communicates in English. The authority scores of this community reveal a unique pattern: the *sabmyk* channel is the only true authority, with other channels primarily forwarding its messages. Searching on the web, it emerges that Sabmyk is a complex conspiracy theory proposed as a successor to QAnon [92]. This theory celebrates a new messianic figure called Sabmyk, who actively promotes conspiracy theories against COVID-19 vaccines and concerning the 2020 US elections [52].

4.3.1 Longitudinal analysis

An interesting aspect to explore is how conspiracy communities have evolved over time. We analyze this dimension in Fig. 2, which shows the number of channels created daily on Telegram. The Figure is divided into five parts: the first four charts (*a*,*b*,*c*,*d*) analyze each community, while the last one (*e*) compares the four conspiracy communities aggregated against the other Telegram communities. The chart shows that the creation of conspiracy channels is not evenly distributed over time. Instead, we find two spikes in channel creation. The first one begins around mid-March 2020, reaches a peak in May, and starts declining until June 2020. Instead, the second spike is much steeper and goes from 2021-01-06 to the middle of March 2021.

Fig. 2 (e) shows a first insight into this phenomenon. The increase in channel creation is more evident in the conspiracy communities (black line) than in the rest of Telegram (purple line). This is particularly evident in the second spike. This behavior suggests that the spike in conspiracy channel creation is not driven by overall Telegram platform growth but by specific events. Therefore, we examine the messages and descriptions of conspiracy channels created during these periods to understand their origins. The first peak can be directly linked to the stringent COVID-19 restrictions imposed in Europe during that period and is more prevalent in the German and Neo-Latin communities. We find the surge in Telegram channels offering alternative viewpoints on the pandemic. Instead, we find that the second peak is linked with the unprecedented Capitol Hill events. During this period, we observed the emergence of several pro-Trump channels, especially in the English community, that became focal points to promote alternative discussions surrounding these events.

5 Monetization

The manual review of hundreds of messages from the Conspiracy Channel Dataset during the previous phase revealed that, besides promoting conspiracy theories, some channels post messages to sell products or promote crowdfunding campaigns. This discovery raises the question of whether some conspiracy channels try to exploit their followers for financial gain. Intrigued by this aspect, we utilized a semi-automatic approach on the URLs shared by conspiracy channels to iden-

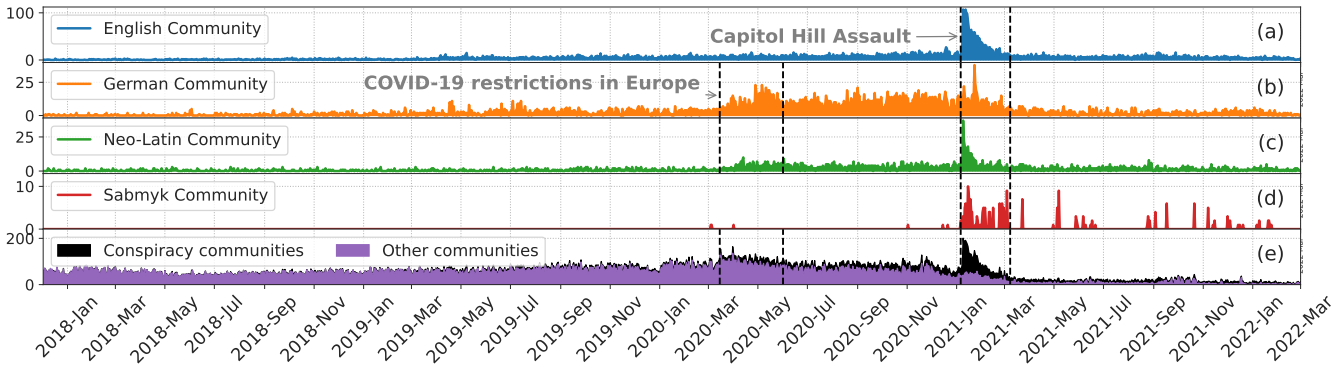

Figure 2: Channels created on Telegram over time.

Table 3: Summary of metrics about donation platforms. Gain with (*) indicates monthly earnings.

Platform	URLs	Profiles	Gain ($)	Donors
BuyMeACoffee	3,157	159	821,816	19,841
Patreon	31,041	936	259,585 *	105,692
Ko-Fi	1,475	97	88,209	5,502
SubScribeStar	2,604	134	5,947 *	5,675
Paypal/donate	83,512	1,434	-	-
DonorBox	1,550	59	-	-
Total	123,129	2,819	1,175,557	136,710

tify the possible strategies they could use to monetize. First, we extracted domains from the links and determined their frequencies. Then, we used SimilarWeb, a popular web analytics service that categorizes websites and ranks them by traffic, to exclude domains associated with social media and news platforms. Finally, we ordered the remaining domains by frequency. We inspected the remaining domains and searched online to determine whether they could be used to generate revenue for the conspiracy theory channel admin. During these operations, we observed that the inspected websites belong to three main groups: donation, crowdfunding, and affiliate programs.

5.1 Donation platforms

The first monetization strategy we analyze consists of asking the subscribers for donations to support the channel and its activity. As a first step, we identify the most popular donation platforms that can be used for this purpose. We manually collect them by analyzing the results of Google queries such as: *top donation platforms*. Given the presence of language specific communities, we conducted country-specific queries containing different languages and keywords. Moreover, to avoid search results on Google from being affected by our browsing history or geo-location, we conduct queries using a VPN. In this way, we collect 31 donation services. Then, we analyze the presence of donation platforms in the URLs shared in the Extended Conspiracy URLs Dataset.

During the exploration phase, we discover a few cases of messages sharing donation URLs with the intent to discredit genuine content creators' donation campaigns rather than promote them. To discard these cases, we analyze the content of the messages to assess the intent of the authors. For this task, we utilize the GPT-4o model via the ChatGPT API, asking the LLM to infer whether the message's author is requesting funds or is discrediting a donation project. In the Appendix, Tab. 8 reports the prompt we provided to the LLM. Of the 56,804 unique messages containing donation links, the model identifies 56,532 messages (99.52%) as promoting a donation page, while 272 are against the analyzed campaign. To evaluate the performance of the the model, we randomly sample 200 messages, 100 marked as positive (*i.e.,* the author is promoting a donation page) and 100 as negative (*i.e.,* the author is discrediting the linked donation campaign). Then, we manually label each message, obtaining a ground truth of 186 positive messages and 14 negative. Upon evaluating the model's performance, we observed that it excels at detecting negative messages, correctly classifying all 14 negative instances. However, 86 messages that initially the model classified as negative are actually positive. In other words, the model may classify promoting campaigns as messages discrediting them. Further investigation revealed that this issue is particularly evident in channels that consistently append donation links at the end of all their messages. In these cases, the model may incorrectly assume that messages with a negative tone aim to discredit the link, even when there is no actual relationship between the message content and the link. Nevertheless, considering our goal to exclude discrediting messages and the relatively small number of potentially misclassified messages (272 - 0.48%), we find the model's performance satisfactory for our purpose.

After filtering out messages classified by the LLM as discrediting the linked donation page, we identified 124,610 URLs from 15 services, shared across 5,585 channels, accounting for 31.3% of our dataset. The most used platforms

Table 4: Summary of metrics about crowdfunding platforms.

Platform	URLs	Projects	Funds ($)	Backers
Givesendgo	14,431	607	30,364,329	519,515
GoFundMe	4,314	1,070	27,688,574	284,802
Kickstarter	234	64	3,491,996	39,112
Fundrazr	184	36	2,270,651	32,981
Indiegogo	53	32	1,061,501	7,207
Fundly	299	18	717,714	14,229
DonorBox	1,073	30	191,463	4,276
Paypal/pools	4,082	392	115,455	3,513
Total	24,670	2,249	65,901,683	905,635

by number of URLs are Paypal/donate [83] with 83,512 URLs (66% of the donation URLs), Patreon with 31,041 URLs (24.5% of the donation URLs), BuyMeACoffee with 3,157 (2.5%), SubScribeStar with 2,604 (2.1%), DonorBox with 1,550 (1.2%) and Ko-Fi with 1,475 (1.2%).

To estimate the potential earnings of the Conspiracy Channel Dataset on these platforms, we create a custom crawler using the Selenium Framework [90]. We crawl all the URLs from the 6 most used donation platforms in our dataset, covering 98.9% of the URLs. * Unfortunately, PayPal/donate and DonorBox do not provide information about donation amounts and the number of donors. Thus, by scraping the web pages of these services, we could only determine the number of unique profiles still reachable. Instead, we obtained information regarding the number of donors and donated amounts for most profiles on the other services. Specifically, for Patreon and SubscribeStar, we retrieve the number of donors and the total amount of money donated in the last month. As for BuyMeACoffee and Ko-Fi, we collect data on the number of donors and the total amount of money raised by the campaigns' creators.

Tab 3 shows the number of URLs we find for the six most used services, the number of created campaigns, the amount of money donated, and the number of donors. Among the profiles we examined, the one that raised the most money through this strategy is *QAnon Anonymous* [2], which received an astonishing $87,955 from 20,103 subscribers in September 2023 using Patreon.

5.2 Crowdfunding and Fundraising services

Conspiracy channels can ask their followers to support them on a specific project by leveraging crowdfunding services. In these platforms, individuals and organizations can raise funds for projects or causes by receiving contributions, typically in exchange for rewards or incentives. We manually build a list of popular crowdfunding services performing Google queries such as *best crowdfunding services*, following the same methodology used for donation platforms. At the end of the process, we collect a list of 49 crowdfunding or fundraising websites. Looking for URLs containing the domain of these platforms in the Extended Conspiracy URLs Dataset, as for the donation links, we find evidence that conspiracy channels occasionally run misinformation campaigns against genuine projects.

Thus, we use the same approach as the previous subsection to discover these cases (Sec. 5.1), asking the GPT-4o model to determine the author's intention behind each message (prompt in Appendix, Tab. 8). Out of 7,499 distinct messages containing a URL to a crowdfunding project, the model classifies 7,319 messages (97.6%) as promoting campaigns while 180 as messages against the linked campaign. Also in this case, to validate the model, we randomly sampled 200 messages, 100 marked as positive and 100 as negative. Then, we manually label these messages as previously done in Sec. 5.1. Here, we identified 145 positive samples and 55 negative samples. Comparing the model results with the manually annotated labels, we observed the model tends to classify positive messages as negative, similar to the previous task. Specifically, the model incorrectly classified 45 messages endorsing crowdfunding campaigns as negative. After reviewing the misclassified messages, we find many authors initially discredit the GoFundMe platform, encouraging their audience not to use it, and then endorse a crowdfunding campaign on the GiveSendGo platform. This pattern was common among American far-right channels, which frequently complain about GoFundMe blocking their projects. Given that the model provides a conservative estimation and considering the relatively low number of misclassified messages (180), we used this model for our classification. Accordingly, we discarded 180 unique messages (357 including duplicates) linking to crowdfunding platforms.

As further validation, we manually examine the crowdfunding campaigns that raised more than $200K, counting 98 different projects, to determine if they are related to conspiracy theories. Three researchers independently analyzed these projects, and a campaign was labeled as related to conspiracy theories only if there was unanimous agreement. Among the 98 campaigns, we identified 51 projects (52.04%) that, despite being supported by conspiracy channels, have goals unrelated to conspiracy theories.

After this validation process, we find 24,696 URLs from 18 different platforms, shared by 3,469 channels, covering 19.5% of our dataset. The most used services are GiveSendGo with 14,431 URLs (58.4% of the crowdfunding URLs), followed by GoFundMe with 4,314 URLs (17.5%), Paypal/pools with 4,082 (16.5%), and DonorBox with 1,073 (4.3%).

Also in this case, we implemented a scraper using the Selenium Framework for each of the aforementioned platforms, covering 99.7% of all the crowdfunding URLs. This scraper allows us to collect information about each campaign's earnings and analyze their status. Indeed, a campaign can be com-

*We conducted the crawling of donation, crowdfunding, and affiliate URLs in September 2023.

pleted or ongoing. Kickstarter enables creators to access the funds only if they reach a predefined target funding at the end of the campaign. Instead, on other platforms, the campaign creator can access the funds raised while the campaign is ongoing. An exception is Indiegogo, which allows creators to choose between the two options when starting a campaign. Upon examining the campaigns' statuses, we discover eight campaigns on Kickstarter and one on Indiegogo that concluded without reaching their fundraising goal. Thus, we do not include the funds raised from these campaigns.

Tab. 4 reports the number of URLs, different projects, money raised, and number of backers for the top eight services by number of URLs. As it is possible to note, this strategy is the most remunerative, collectively funding conspiracy theorists with almost $66M. Analyzing the content of the campaigns and find that they typically fall into these categories:

Campaigns supporting far-right. We identified several fundraising campaigns for far-right projects, mainly raising funds for legal costs related to the January 6th Capitol riot. Three of these campaigns alone [57, 58, 87] collected $160,816 from 2,891 backers. We find that many of these campaigns are hosted on Givesendgo, a platform well known for promoting extremist content [6].

Campaigns about COVID-19. We also find GiveSendGo campaigns frequently linked to COVID-19, including those for the Freedom Convoy 2022 [51], a protest movement against COVID-19 policies. Similar campaigns on GoFundMe redirect to refund pages due to the platform's ban on content promoting violence [50]. Looking at the news, we discover that one of these campaigns was the biggest gainer of the platform, raising over $10 million from 120,000 donors [19]. Additionally, Indiegogo and Kickstarter host projects funding documentaries about COVID-19 [32,94,105]. These platforms have stricter content policies, but moderating pseudo-scientific claims remains challenging due to freedom of expression concerns.

Scam campaigns. We detect crowdfunding campaigns that are outright scams. An example is a Fundrazor campaign [69] falsely claiming to raise funds for starving children in Venezuela. It collected $39,500 from 602 donors before being shut down, and a banner on the page states that Save The Children has confirmed they have no association with it. Another scam [5] on Indiegogo raised over $7.4K for a portable air cleaner claiming to purify the air with a high-frequency generator before being closed as the creator claimed that Silicon Valley internet companies had hindered the project.

Campaigns against the establishment. We found campaigns raising funds to challenge government policies or influential figures. For example, a campaign [13] funded by American Education Defenders, Inc., aims to counter U.S. school indoctrination with a program called "America's 52 Videos" that promotes American values. Another campaign [26] supports a documentary series on global manipulation. Together, these campaigns raised over $37K from 477 contributors.

Table 5: Summary of metrics about e-commerce platforms.

Platform	URLs	Products	Affiliate
Amazon	63,445	19,372	34,412
Teespring	2,415	336	-
eBay	1,932	958	131
Etsy	1,082	512	-
Total	68,874	21,178	34,543

5.3 Affiliate Programs

Conspiracy channels adopting this strategy use affiliate programs from e-commerce platforms to earn a commission. Thus, as a first step, we identify the most popular e-commerce platforms they can utilize for this purpose. To this end, we leverage SimilarWeb to retrieve all the 42 services reported in the global rank for the *eCommerce & Shopping* category. Then, we extract URLs containing the domain of these platforms from the Extended Conspiracy URLs Dataset, finding 70,149 URLs from 28 platform. Among the top 4 platforms, covering 98.1% of e-commerce links, only Amazon and eBay offer an affiliate program. In this program, a participant, known as partner, can generate unique links pointing to products on the platform that embed his unique identification number. The partner earns a commission for any purchases made by users who land on the platform through his link. In particular, Amazon's partners earn a commission, between 1% and 12% depending on the categories of the product and the location of the targeted market (*e.g.,* amazon.com, amazon.de) from all the items bought in the next 24 hours from arrival through the link [10]. Similarly, on eBay, a partner earns a commission between 1% and 4% on the items purchased on the platform in the following 24 hours [43].

Overall, we find 63,445 URLs pointing to Amazon and 1,932 to eBay in the Conspiracy Channel Dataset. To detect URLs belonging to the affiliate program, we search for URLs containing the parameters *tag=* for Amazon and *campid=* for eBay. Surprisingly, we discover that 34,412 (54.2%) of Amazon's URLs and 131 (6.8%) on eBay are affiliated links granting commissions to the conspiracy channels and that 1,810 channels (10.2% of our dataset) leverage this strategy. Tab. 5 provides a summary of the metrics of e-commerce platforms.

Unfortunately, since there is no public information available about the partner programs, we can not estimate the gain of the channels with this strategy. However, we use the Selenium Framework to build a custom crawler to retrieve the type of goods sold on this platform. We obtain the item category for 50,295 of the 63,445 Amazon URLs, representing 17,163 different products. Interestingly, we discover that more than half of the advertised products are books. The remaining goods fall into various categories, such as Electronic Devices (*e.g.,* , torches, GPS devices, power supplies) and Health & Personal

Table 6: Number of channels for each monetization strategy.

Community	Donation	Crowdfunding	Affiliate
English	2,086	1,930	390
German	2,769	1,233	1,224
Neo-Latin	728	305	168
Sabmyk	2	1	28
Total	5,585	3,469	1,810

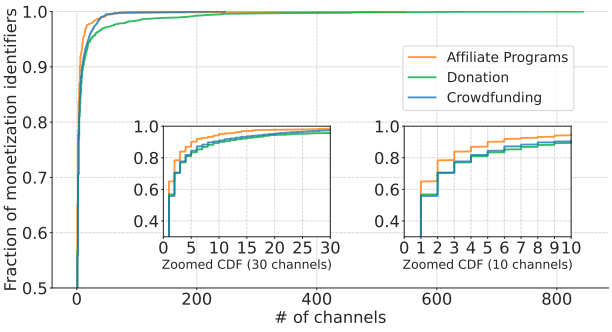

Figure 3: Distribution monetization projects in channels.

Care (*e.g.,* , vitamins, proteins, disinfectants). These items are marketed as essential for surviving in post-apocalyptic scenarios caused by the side effects of vaccines and 5G radiation. Tab. 9 in the appendix reports the number of URLs and the items found for each category. Instead, in Sec. 6, we discuss the danger behind promoting these goods and the reason for the significant presence of books among the links.

5.4 Monetization Analysis

Tab. 6 shows the number of channels in each community that use the three monetization strategies. As we can see, most German and Neo-Latin channels predominantly use the donation strategy rather than crowdfunding and affiliate programs. In contrast, English channels use crowdfunding significantly more frequently than other communities. This observation is consistent with previous analyses showing that crowdfunding campaigns often concentrate on events like the Capitol Hill Riot and the Freedom Convoy, arguably more significant for English-speaking communities. Moreover, German channels use the affiliate strategy more commonly than other communities. This phenomenon is largely explained by a specific group of channels we will explore in the following paragraph. Finally, we find that Sabmyk shares almost no monetization links. A closer examination reveals that Sabmyk primarily monetizes by directing users to the website of the creator of the movement to promote and sell his artworks. Analyzing the affiliate links promoted within the Sabmyk community, we find they are shared across 28 channels using the same referral ID, highlighting a high level of coordination.

Monetization links promoted by multiple channels. The analysis of Sabmyk affiliate links highlights the sharing of the same referral link by multiple channels. To study this phenomenon in more depth, we conducted a broader analysis that also includes donations and crowdfunding projects. Fig. 3 shows the cumulative distribution function (CDF) depicting the fraction of referral IDs (orange), crowdfunding (blue), and donation projects (green) shared in channels. The main plot provides an overview of the entire distribution, while two subplots show two different levels of zoom. By examining the zoomed CDFs, we can observe that most referral links, donation projects, and crowdfunding projects are typically shared by only a few channels. Specifically, we find that 65.4% of affiliate IDs, 56.8% of donation projects, and 55.8% of crowdfunding projects are shared by only a single channel. The figure also highlights that affiliate links are shared by fewer channels than donation and crowdfunding projects, with almost 80% of referral links shared by at most two channels. This can be expected as, while affiliate links are primarily beneficial to the channel owner, crowdfunding and donation projects may sometimes support broader causes and may be shared by channel owners even if they are not the direct beneficiaries of the funds received. Looking at the tail of the overall distribution, we find other interesting insights. Examining crowdfunding projects, we find that the most widely shared is a highly popular project supporting the Freedom Convoy, promoted on GiveSendGo [104]. This project is shared by 247 conspiracy channels and has raised $9.7 million. For donation projects, we identified a donation link that was shared by 844 channels. This link is associated with the *Corona_Fakten* channel, which focuses on disseminating news and controversial theories about COVID-19. The channel frequently includes the donation link in its posts, and because its content is widely shared and forwarded by many other channels, the donation link has spread across hundreds of channels. What is more surprising instead, is the presence of a group of over 549 channels promoting Amazon products using the same affiliate ID. Our analysis reveals this group of channels is entirely located in the German community and is actively involved in promoting various conspiracy theories, predominantly related to COVID-19.

Table 7: Monetization strategies used by channels.

	# of monetization strategies used by channels		
Community	0	1	2+
English	80.9% (7,680)	15% (1,426)	4.1% (385)
German	73.8% (4,196)	20.9% (1,187)	5.4% (305)
Neo-Latin	79.0% (1,909)	17.1% (414)	3.8% (92)
Sabmyk	99.6% (234)	0.4% (1)	0% (0)
Total	78.6% (14,019)	17% (3,028)	4.4% (782)

Channels using multiple monetization strategies. Finally, Tab. 7 shows the number of monetization strategies used by

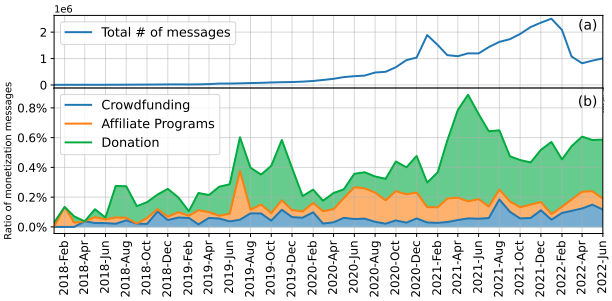

Figure 4: Total number of messages and fraction of monetization messages over time.

channels divided by community. We exclude from this analysis links contained in forwarded messages to avoid the cases, of news websites reporting donation links that are extremely widespread and are instead not a monetization strategy of the considered channel. Interestingly, we find that the majority of channels in all the communities do not use monetization strategies. Among the channels that monetize, most use only one strategy, with 4.4% employing two or more strategies.

Monetization trends over time Fig. 4 shows the total amount of messages sent by conspiracy channels (a) and which percentage of these messages are related to monetization (b). Monetization messages are divided according to the type of monetization in crowdfunding (blue), affiliate programs (orange), and donation (green). We observe that monetization messages are generally not extremely common, reaching a maximum of 0.8% in early January 2021. However, the phenomenon has clearly evolved from barely existing in 2018 to achieving relative stability of almost 0.4% of all messages in 2022. From chart (a), we can notice that the total number steadily decreased after January 2022, but instead, the ratio of monetization messages remains stable. It is also interesting to note that monetization strategies were almost equally divided before 2021, but then the donation strategy became much more prevalent. A possible explanation could be that crowdfunding platforms have implemented increasingly stricter policies to counter questionable projects, an aspect that we will explore in the following paragraph.

Shift in platform usage. Fig. 7 and Fig. 8, in the Appendix, show, respectively, the proportion of donation and crowdfunding platforms used by each community monthly. Examining donation platforms, we observe distinct preferences across different linguistic communities. The German community predominantly uses PayPal. In contrast, Patreon has been the most used platform in the Neo-Latin community over the last year. The English community initially used Patreon and PayPal most frequently, but in the past 18 months, there has been a significant diversification, with multiple platforms being utilized. For crowdfunding, PayPal Pools was the dominant platform among both the German and Neo-Latin communities. However, its popularity decreased until it was discontinued in September 2021, replaced by GoFundMe. The English community displayed a different trend. GoFundMe was consistently the preferred platform, as PayPal Pools was never widely adopted. Around October 2020, GiveSendGo began to rise in popularity, accounting for 75% to 90% of all URLs shared by the English community monthly. This shift may be attributed to GoFundMe stricter policies, as GiveSendGo promotes itself as having no moderation. We find evidence of this transition in the messages of the English community.

5.5 Other Strategies

In addition to the previously analyzed monetization strategies, we find conspiracy channels can exploit other sources of revenue.

Other Amazon features. The first one is related to the Amazon Influencer Program [12]. This program enables Influencers to create an Amazon web page with some selected products, earning commissions on sales. These pages are easily detectable because they contain the */shop/* string in their URL. Looking for this pattern in our dataset, we find 25 different shops. Another possibility is using Amazon's wish lists, essentially lists of products a user desires. These lists can be private (visible only to the creator) or public. In the latter case, anyone with access to the wish list link can gift a product to the list's creator. To identify wish lists in our dataset, we extract URLs containing the */wishlist/* string in their path. This process led us to 119 URLs, pointing to 32 distinct public lists. The inspection of these lists revealed that 12 are no longer accessible, and the others contain a wide variety of products, including underwear, vitamins, survival kits, and prepaid cards.

Blockchain addresses. In our analysis, we discover conspiracy channels asking for cryptocurrency donations in their descriptions. We use regular expressions to extract wallet addresses of the most popular blockchains (Bitcoin and Ethereum), as well as the prominent privacy-preserving blockchains (Monero and Zcash). We identified these blockchains' addresses in 40 channels, and through manual verification, we confirmed that 29 of them are used for donations. Analyzing the BTC wallets, we find they received 115 transactions, totaling 0.5 BTC ($\approx \$13,000$). Performing the same analysis on Ethereum, we find that the wallets received 42 transactions, amounting to 5.5 ETH ($\approx \$9,000$).

Custom websites. Analyzing the URLs and examining messages within the conspiracy channels, we observed frequent promotion of custom e-commerce sites or personal websites. Inspecting these websites, we discover that many of them feature dedicated donation sections with blockchain addresses or various payment options. Thus, we perform a raw analysis to estimate the magnitude of the phenomenon. In particular, we look for URLs containing the words: *shop, products, store, produkt, collections, donate, donations or support* as third-level domain or that have these words in the URL's

path. As a result, we find 152,680 URLs (24,980 unique) matching our definition. Unfortunately, we can not validate or analyze this huge amount of websites since it requires a heavy manual effort or to build custom parsers.

Drive traffic to video hosting services. The URLs analysis also revealed that conspiracy channels share a considerable number of links to popular video hosting services such as YouTube (3,656,171 URLs) or BitChute [98] (276,513 URLs). While some channels may share videos as a resource to confirm their theories, it is also well known from previous work [16], that some of them leverage such platforms to monetize their content through Partner Programs (*e.g.,* YouTube Partner Program [30]). These programs allow content creators to earn money by placing advertisements in their videos and paying them proportionally to the time they are viewed. While the in-depth analysis of this phenomenon falls outside the scope of this work, we believe that the dataset we release can be a valuable resource for future research in this area.

Channel ads. Finally, conspiracy channel administrators could also monetize by publishing sponsored messages to their subscribers. There are mainly two methods to implement this strategy. The first relies on a feature recently introduced on Telegram, the Sponsored Messages [96]. This functionality enables channel owners to share sponsored messages to receive a share of the advertising revenue. However, it is worth noting that this feature is relatively new and still in the beta phase. The second approach involves using external services like *telega.io*, which act as intermediaries between channel administrators and advertisers or establish private deals directly between advertisers and channel administrators. However, this kind of sponsored message is likely impossible to detect when products are deceptively promoted into the content and storyline of the channel.

6 Discussion

Impact of the time gap. Messages in the TGDataset range from October 2015 to July 2022, while we retrieved monetization information between September and October 2023. We analyzed the impact of this gap to determine if it could affect our estimation of money raised. Concerning the crowdfunding platforms Kickstarter, Indiegogo, and PayPal/pool, the time gap has no impact. Kickstarter and Indiegogo campaigns can run for up to 60 days, while PayPal/pool, discontinued in November 2021, allowed campaigns to run for only 30 days. Conversely, projects on other platforms can run indefinitely. Therefore, we examine the distribution of donations over time by extracting all available donations from platforms that run campaigns without time constraints. From GiveSendGo, we retrieved complete donation data, while on GoFundMe, we had access only to the most recent 1,000 donations and the top 1,000 highest donations for each project. Finally, we could not extract Fundrazr data, since the platform hides the amount users contributed. While these limitations prevent us from obtaining a complete picture, the available data still offer valuable insights. Our analysis revealed that 76.3% of campaigns closed or had their last donation by July 2022. Moreover, we found that, on average, each campaign raises 34.2% of its total funds within the first 7 days, 65% after one month, and 74.4% after three months. Therefore, since most of the money is raised within the first three months from the launch, the time gap has a limited impact.

False positive channels. Validating channels present in the detected communities Sec. 4.2.4, we classify 121 out of 414 channels as false positives. In particular, we identified 28 channels associated with the American far-right or supporting the former Brazilian president Bolsonaro. Although the messages on these channels do not explicitly endorse or promote conspiracy theories, they often share a similar underlying narrative. Additionally, the relationship between conspiracy theories and the American far-right [88] or Bolsonaro [73] is well established. Furthermore, 24 channels cover topics related to religion and self-improvement. According to social and psychological scientific works [22, 24, 42], there exists a connection between these topics and conspiracy theories. Indeed, conspiracy theories often provide a sense of belonging to a community and the perception of control over complex and seemingly chaotic events. Moreover, some conspiracy theories, like QAnon, incorporate seemingly religious elements such as beliefs in a secretive satanic elite, apocalyptic prophecies, and the involvement of divine or demonic forces. Surprisingly, 15 channels are linked to cryptocurrency. This seemingly unusual connection is backed by a recent study, which reveals that cryptocurrency holders often exhibit strong anti-establishment sentiments and a pronounced tendency to believe in conspiracy theories [67, 68]. Lastly, there are 13 channels dedicated to alternative news. These channels provide unconventional viewpoints that often challenge traditional narratives.

Detecting new monetization techniques. In this work, we focus on three main monetization methods used by conspiracy channels and mention other methods we've observed. However, new techniques may appear in the future. Based on our experience, we suggest the following ways to identify potential new techniques. Using the monetization messages collected in this study, an LLM can be fine-tuned to detect these messages more effectively than the standard ChatGPT we used. By monitoring the links these channels share and analyzing the most frequently shared ones with the fine-tuned model, it will be possible to identify new platforms used for monetization. Finally, many monetization strategies used by conspiracy channels are similar to those used by web content creators. Therefore, if web content creators start using new strategies, it is worth checking if conspiracy channels are also adopting them.

The risks of conspiracy narratives. Our analysis reveals a clear distinction between the products promoted by conspiracy theory channels on Amazon compared to other online

marketplaces. Indeed, while Amazon features standard products like books, masks, and water filters, we find a range of questionable products (*e.g.,* 5G shields, EMF stone protectors, and healing wands) on eBay, Etsy, and Teespring. The distinction is likely attributed to the different content policies of these platforms. Indeed, Amazon upholds a more rigorous content policy compared to the other services. Nevertheless, it is important to emphasize that these products are not inherently harmful. Indeed, the concern lies in the narratives and promotions associated with these items. For example, ordinary substances like Sodium Chloride and Chlorine Dioxide, commonly found in pharmacies, are promoted in four channels as essential components to prepare the so-called "Miracle Mineral Supplement", which is reported as a miraculous cure for various diseases, including cancer and HIV. Similarly, we discover 35 channels sharing links to buy seemingly innocuous white pine needles at an exorbitant price of $150 on Etsy. The concern lies in the accompanying message, which presents a guide for COVID-19 survival. This guide discourages seeking medical care in hospitals and suggests homemade remedies, including tea prepared with the costly pine needles mentioned above.

Marketplace policies. Although Amazon has a rigorous policy about the items sold and actively operates to ban QAnon merchandising [77], it has a less strict policy about book content. Quoting Amazon policies: *As a bookseller, we believe that providing access to the written word is important, including content that may be considered objectionable.* [11]. The combination of this less strict policy and the simplicity of self-publishing on Amazon allowed conspiracy theorists to spread their ideas and monetize through book sales. Indeed, nearly 50% of the links point to books and almost half of them include an affiliate tag. Looking at the most frequently occurring authors of books promoted using non-affiliate links, we discover three relatively obscure German writers: VEIBZ (3,091 occurrences), MERKSAM (1,492 occurrences), and EBURD (813 occurrences). Their books explore several conspiracies with the goal of revealing the truth on subjects such as: "NASA & Elon Musk – They lie & cover-up," "CERN & its satanic roots," "HAARP & CERN use Alien Tech." Fig. 5 shows the cover of the three most shared books.

Concerning the promoted items, there are also problems related to the transparency of the activity and compliance with the referral programs. Indeed, according to the partnership agreement of Amazon and Ebay [10] [43], a partner—a participant that can generate referral links and earn commissions—has to clearly disclose their partnership. Moreover, near each affiliated link should be a disclosure such as *"(paid link)," "#ad," or "#CommissionsEarned"*. This information is needed to inform the customers that a conflict of interest exists on the promoted item.

Figure 5: The covers of the three most shared books by conspiracy channels available for sale on Amazon.

7 Mitigation

To address the concerns highlighted in the previous section, we developed two tools: The Channel Checker Bot and the ConspiracyAlert plugin. These tools assist users in identifying channels that spread questionable content, information potentially harmful to their health, and crowdfunding campaigns that may support conspiracy theory groups.

The Channel Checker Bot. It is a Telegram Bot implemented in Python3. It receives a channel name from the user and provides detailed information about that channel. The bot uses a database containing channels identified during our research and information such as questionable content, advertised products, and dubious fundraising campaigns. When a user inputs a channel name, the bot searches the database for a match. If the channel is found, the bot provides the user with the existing information from the database. Instead, if the channel is not in the database, the bot initiates a headless Telegram client, joins the channel via Telegram APIs, and retrieves all shared content. Then, it extracts all shared links and checks them against the conspiracy resource dataset and the monetization links collected during this research. After the analysis, the bot updates the database with the new channel and its associated information. Finally, the bot presents the analysis result to the user. Fig. 6 displays an instance of a chat with the Channel Checker Bot. Therefore, the Channel Checker Bot serves a dual purpose: It provides users with detailed information about channels and continuously updates the database with new conspiracy channels.

ConspiracyAlert: A Browser Plug-in. Although the Channel Checker Bot serves as a warning system for Telegram users navigating the platform, it does not help users who browse the web and land on questionable products or crowdfunding campaigns. To address this gap, we developed the ConspiracyAlert browser plug-in. This plug-in, compatible with Chrome and Firefox and written in TypeScript, monitors the user's web navigation. Once a webpage is fully loaded, the plug-in captures the URL and transmits it to a remote server. Then, the server checks the URL against both the Conspiracy Resource dataset and the URLs dataset identified in Sec. 4.2.2. If the server finds a match, it generates an informative mes-

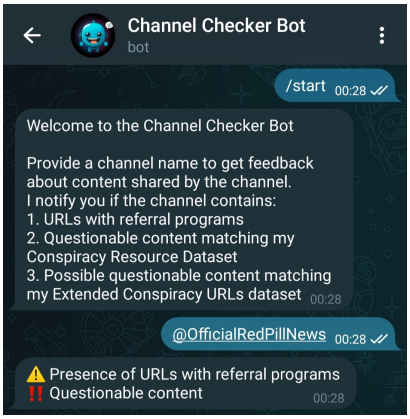

Figure 6: An instance of the Channel Checker Bot chat.

sage, which the plug-in displays to the user.

The source code for both tools and additional technical implementation details are publicly available on GitHub [14]. Notably, we designed both tools to maintain user privacy by not retaining user information (*e.g.,* IP addresses) or details that could later associate a request with a user (*e.g.,* timestamps, Telegram client versions, or browsing history). The system only stores information about the analyzed channels.

8 Limitations

As mentioned in Sec. 4.2, we build the *Conspiracy Resources Dataset* gathering information from previous work focused on conspiracy theories. However, most of the scientific literature focuses on analyzing English content. This limitation could introduce a bias, as conspiracy communities operating in other languages, such as Russian or Indian, might evade detection due to their use of non-English sources. Moreover, other platforms not considered in our study (*e.g.,* Parler [17]) are known to host conspiracy-related content. Unfortunately, we could not find works providing conspiracy-labeled datasets suitable for our study.

This study primarily utilizes link analysis to uncover monetization techniques and estimate the amount of money raised. However, this approach does not provide insight into monetization campaigns conducted through media content. For example, we observed various images shared on the channels promoting self-published books, paid events (*e.g.,* conferences), or training courses conducted by self-proclaimed gurus. In Sec. 5.2, we analyzed campaigns that collected more than $200,000 and found several that, despite being endorsed by conspiracy channels, do not show evidence of being connected to conspiracy theories. This suggests that other similar campaigns may exist among those we considered in this study. Understanding why these campaigns are endorsed by conspiracy channels raises intriguing questions: Are they shared only to support the conspiracy narratives? Are their topics intentionally unrelated to conspiracy theories to appeal to a broader audience? Or are the administrators paid to promote these campaigns?

Throughout our investigation, we do not attempt to infer the direct link between the channel's administrator and the ultimate recipient of funds. In certain situations, this connection is clear, such as when the channel's name matches a profile on an external platform or in the case of affiliate program campaigns. However, in other instances, such as crowdfunding campaigns, it proves challenging to discern the ultimate objective of the channel's administrator. However, it is clear that someone is profiting and that the channels have a key role in fueling the conspiracy theories' money machine.

9 Ethical considerations

The dataset we analyze does not contain personal information like phone numbers or any media that could include adult content or copyrighted material. Furthermore, the channels mentioned in our study are publicly accessible and represent widely recognized public figures or entities. In our data collection process, we scraped web pages of the analyzed platforms. We adopt a careful approach to prevent flooding and ensure a minimal impact on these services by limiting the volume of requests submitted.

10 Conclusion and future work

In this work, we focused on understanding and quantifying how conspiracy theories raise funds by exploiting Telegram. We started by identifying the conspiracy theory-related channels, analyzing a novel dataset we built by collecting previously validated resources from an extensive literature review that we publicly release [15].

This study revealed the alarming finding that almost 15% of all Telegram channels in the TGDataset (17,829 channels) are linked to conspiracy theories. Then, we discover that conspiracy theory-related channels actively seek to profit from their subscribers. We categorize all the diverse monetization strategies we find in our dataset and dive into the analysis of the three most common. Our study shows that conspiracy theories raised funds for about $66 million by arranging crowdfunding campaigns.

As a future work, we believe it is interesting to conduct a more comprehensive analysis of the monetization strategies reported in Sec. 5.5 to get deeper insights into the impact of monetization. Finally, another possible direction is analyzing the channels that use the same affiliate program ID and those that share identical funding projects. This study could highlight the collaborative patterns presented by these channels and enable the identification of more fine-grained sub-communities.

References

[1] Fake news corpus. https://github.com/several27/FakeNewsCorpus, 2023.

[2] Qanon anonymous. https://www.patreon.com/qanonanonymous, 2023.

[3] Telegram faq. https://telegram.org/faq, 2023.

[4] France 24. Germany weighs ban on telegram, tool of conspiracy theorists. https://f24.my/8KcH, 2022.

[5] ADL. Antivirbag-portable air cleaner, ionizer, ozonizer. https://igg.me/at/antivirbag, 2020.

[6] ADL. Adl crowdfunding report: How bigots and extremists collect and use millions in online donations. https://www.adl.org/resources/report/adl-crowdfunding-report-how-bigots-and-extremists-collect-and-use-millions-online, 2023.

[7] Anti-Defamation League (ADL). Fall of the cabal. https://www.adl.org/glossary/fall-cabal, 2023.

[8] Wasim Ahmed, Josep Vidal-Alaball, Joseph Downing, Francesc López Seguí, et al. Covid-19 and the 5g conspiracy theory: social network analysis of twitter data. *Journal of medical internet research*, 22(5):e19458, 2020.

[9] Max Aliapoulios, Emmi Bevensee, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro, Gianluca Stringhini, and Savvas Zannettou. A large open dataset from the parler social network. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 15, pages 943–951, 2021.

[10] Amazon. Associates program standard commission income statement. https://affiliate-program.amazon.com/help/node/topic/GRXPHT8U84RAYDXZ, 2023.

[11] Amazon. Content guidelines for books. https://www.amazon.com/gp/help/customer/display.html?nodeId=201995150, 2023.

[12] Amazon. Monetize your content with the amazon influencer program. https://affiliate-program.amazon.com/influencers, 2023.

[13] Inc American Education Defenders. Help protect our kids against the raw sewage of crt and other indoctrinations. fundrazr.com/ourfuture, 2021.

[14] Anonymized. Will be disclosed after acceptance. .

[15] Anonymous. Conspiracy theory urls. zenodo, 2023.

[16] Cameron Ballard, Ian Goldstein, Pulak Mehta, Genesis Smothers, Kejsi Take, Victoria Zhong, Rachel Greenstadt, Tobias Lauinger, and Damon McCoy. Conspiracy brokers: understanding the monetization of youtube conspiracy theories. In *Proceedings of the ACM Web Conference 2022*, pages 2707–2718, 2022.

[17] Dominik Bär, Nicolas Pröllochs, and Stefan Feuerriegel. Finding qs: Profiling qanon supporters on parler. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 17, pages 34–46, 2023.

[18] BBC. Twitter suspends 70,000 accounts linked to qanon. https://bbc.com/news/technology-55638558, 2021.

[19] BBC. Freedom convoy: Gofundme seizes funds of canada 'occupation'. https://bbc.com/news/world-us-canada-60267840, 2022.

[20] BBC. The light: Inside the uk's conspiracy theory newspaper that shares violence and hate. https://www.bbc.com/news/uk-65821747, 2023.

[21] Michael Bernstein, Andrés Monroy-Hernández, Drew Harry, Paul André, Katrina Panovich, and Greg Vargas. 4chan and/b: An analysis of anonymity and ephemerality in a large online community. In *Proceedings of the international AAAI conference on web and social media*, volume 5, pages 50–57, 2011.

[22] Alessandro Bessi, Mauro Coletto, George Alexandru Davidescu, Antonio Scala, Guido Caldarelli, and Walter Quattrociocchi. Science vs conspiracy: Collective narratives in the age of misinformation. *PloS one*, 10(2):e0118093, 2015.

[23] Ivan Blekanov, Svetlana S Bodrunova, and Askar Akhmetov. Detection of hidden communities in twitter discussions of varying volumes. *Future Internet*, 13(11):295, 2021.

[24] Bayleigh Elaine Bond and Ryan Neville-Shepard. The rise of presidential eschatology: Conspiracy theories, religion, and the january 6th insurrection. *American Behavioral Scientist*, 67(5):681–696, 2023.

[25] David A Broniatowski, Kevin T Greene, Nilima Pisharody, Daniel J Rogers, and Jacob N Shapiro. Measuring the monetization strategies of websites with application to pro-and anti-vaccine communities. *Scientific reports*, 13(1):15964, 2023.

[26] Derek Broze. Help us finish the pyramid of power documentary series! https://fnd.us/pyramidofpowerdoc, 2021.

[27] Zhenfeng Cao, Minzhang Zheng, Yulia Vorobyeva, Chaoming Song, and Neil F Johnson. Dynamical patterns in individual trajectories toward extremism. *arXiv preprint arXiv:1706.01594*, 2017.

[28] Neha Chachra, Stefan Savage, and Geoffrey M Voelker. Affiliate crookies: Characterizing affiliate marketing abuse. In *Proceedings of the 2015 Internet Measurement Conference*, pages 41–47, 2015.

[29] Rakesh Vidya Chandra and Bala Subrahmanyam Varanasi. *Python requests essentials*. Packt Publishing Birmingham, UK, 2015.

[30] Xu Cheng, Fatourechi Mehrdad, Xiaoqiang Ma, Cong Zhang, and Jiangchuan Liu. Understanding the youtube partners and their data: Measurement and analysis. *China Communications*, 11(12):26–34, 2014.

[31] Miyoung Chong. Discovering fake news embedded in the opposing hashtag activism networks on twitter:# gunreformnow vs.# nra. *Open Information Science*, 3(1):137–153, 2019.

[32] Robert Cibis. Corona.film. indiegogo.com/projects/corona-film?create_edit=true, 2020.

[33] Sam Clark and Anna Zaitsev. Understanding youtube communities via subscription-based channel embeddings. *arXiv preprint arXiv:2010.09892*, 2020.

[34] Steve Clarke. Conspiracy theories and conspiracy theorizing. In *Conspiracy Theories*, pages 77–92. Routledge, 2019.

[35] Jamie Cleland. Charismatic leadership in a far-right movement: an analysis of an english defence league message board following the resignation of tommy robinson. *Social Identities*, 26(1):48–60, 2020.

[36] CNN. The flat-earth conspiracy is spreading around the globe. does it hide a darker core? https://www.cnn.com/2019/11/16/us/flat-earth-conference-conspiracy-theories-scli-intl, 2019.

[37] Rhys Crilley, Marie Gillespie, Bertie Vidgen, and Alistair Willis. Understanding rt's audiences: Exposure not endorsement for twitter followers of russian state-sponsored media. *The International Journal of Press/Politics*, 27(1):220–242, 2022.

[38] Michal Mimino Danilak. langdetect. https://pypi.org/project/langdetect/, 2023.

[39] Daniel De Zeeuw, Sal Hagen, Stijn Peeters, and Emilija Jokubauskaite. Tracing normiefication: A cross-platform analysis of the qanon conspiracy theory. *First Monday*, 2020.

[40] Cambridge Dictionary. Conspiracy theory definition. https://dictionary.cambridge.org/dictionary/english/conspiracy-theory, 2023.

[41] Chris HQ Ding, Hongyuan Zha, Xiaofeng He, Parry Husbands, and Horst D Simon. Link analysis: hubs and authorities on the world wide web. *SIAM review*, 46(2):256–268, 2004.

[42] Karen M Douglas, Robbie M Sutton, and Aleksandra Cichocka. The psychology of conspiracy theories. *Current directions in psychological science*, 26(6):538–542, 2017.

[43] eBay. Global rate card. https://partnernetwork.ebay.com/our-program/rate-card, 2023.

[44] Adam M Enders, Joseph E Uscinski, Michelle I Seelig, Casey A Klofstad, Stefan Wuchty, John R Funchion, Manohar N Murthi, Kamal Premaratne, and Justin Stoler. The relationship between social media use and beliefs in conspiracy theories and misinformation. *Political behavior*, pages 1–24, 2021.

[45] Kristen Engel, Yiqing Hua, Taixiang Zeng, and Mor Naaman. Characterizing reddit participation of users who engage in the qanon conspiracy theories. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1):1–22, 2022.

[46] Emily Fales, Lauryn Lintner, Mason Runkel, and Paola Ariza. The moon landing hoax. 2020.

[47] Philip M Fernbach and Jonathan E Bogard. Conspiracy theory as individual and group behavior: Observations from the flat earth international conference. *Topics in Cognitive Science*, 2023.

[48] Milla Frühling. The conspiracy empire of oliver janich. https://www.belltower.news/social-media-the-conspiracy-empire-of-oliver-janich-106913/, 2020.

[49] Amanda Garry, Samantha Walther, Rukaya Rukaya, and Ayan Mohammed. Qanon conspiracy theory: examining its evolution and mechanisms of radicalization. *Journal for Deradicalization*, (26):152–216, 2021.

[50] GoFundMe. Update: Gofundme to refund all freedom convoy 2022 donations (2/5/2022). gofundme.com/f/taking-back-our-freedom-convoy-2022, 2022.

[51] Todd Gordon. The freedom convoy, the resurgence of the far right, and the crisis of the petty bourgeoisie. *Studies in Political Economy*, 103(3):280–293, 2022.

[52] The Guardian. Unmasked: man behind cult set to replace qanon. https://www.theguardian.com/us

-news/2021/mar/20/revealed-man-behind-fast-growing-cult-becoming-the-new-qanon-sabmyk-network, March 2021.

[53] The Guardian. 8chan: the far-right website linked to the rise in hate crimes. https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website, 2023.

[54] Hans WA Hanley, Deepak Kumar, and Zakir Durumeric. No calm in the storm: investigating qanon website relationships. In *Proceedings of the international AAAI conference on Web and social media*, volume 16, pages 299–310, 2022.

[55] Mohamad Hoseini, Philipe Melo, Fabricio Benevenuto, Anja Feldmann, and Savvas Zannettou. On the globalization of the qanon conspiracy theory through telegram. In *Proceedings of the 15th ACM Web Science Conference 2023*, pages 75–85, 2023.

[56] Roland Imhoff and Pia Lamberty. A bioweapon or a hoax? the link between distinct conspiracy beliefs about the coronavirus disease (covid-19) outbreak and pandemic behavior. *Social Psychological and Personality Science*, 11(8):1110–1118, 2020.

[57] April Jensen. God bless america, free my j6er. givesendgo.com/G26FY, 2021.

[58] Sommer B Johnson. Stand with paul. fundly.com/stand-4-paul, 2021.

[59] Josh Kamps and Bennett Kleinberg. To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, 7(1):1–18, 2018.

[60] Jon M Kleinberg. Hubs, authorities, and communities. *ACM computing surveys (CSUR)*, 31(4es):5–es, 1999.

[61] Massimo La Morgia, Alessandro Mei, and Alberto Maria Mongardini. It's a trap! detection and analysis of fake channels on telegram. In *2023 IEEE International Conference on Web Services (ICWS)*. IEEE, 2023.

[62] Massimo La Morgia, Alessandro Mei, and Alberto Maria Mongardini. Tgdataset: a collection of over one hundred thousand telegram channels. *arXiv preprint arXiv:2303.05345*, 2023.

[63] Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Jie Wu. Uncovering the dark side of telegram: Fakes, clones, scams, and conspiracy movements. *arXiv preprint arXiv:2111.13530*, 2021.

[64] Massimo La Morgia, Alessandro Mei, Francesco Sassi, and Julinda Stefa. The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations. *ACM Transactions on Internet Technology*, 23(1):1–28, 2023.

[65] Mark Ledwich and Anna Zaitsev. Algorithmic extremism: Examining youtube's rabbit hole of radicalization. *First Monday*, 2020.

[66] Deborah E Lipstadt. *Denying the Holocaust: The growing assault on truth and memory*. Simon and Schuster, 2012.

[67] Shane Littrell, Casey Klofstad, and Joseph E Uscinski. The political, psychological, and social correlates of cryptocurrency ownership. *PloS one*, 19(7):e0305178, 2024.

[68] Brett AS Martin, Polymeros Chrysochou, Carolyn Strong, Di Wang, and Jun Yao. Dark personalities and bitcoin®: The influence of the dark tetrad on cryptocurrency attitude and buying intention. *Personality and Individual Differences*, 188:111453, 2022.

[69] Team McAfee. Help team mcafee give back to savethechildren venezuela thanksgiving feast4food. https://fundrazr.com/Team_McAfee, 2021.

[70] Theo Meder et al. Online coping with the first wave: Covid humor and rumor on dutch social media (march–july 2020). *Folklore: Electronic Journal of Folklore*, (82):135–158, 2021.

[71] Amin Mekacher and Antonis Papasavva. "i can't keep it up." a dataset from the defunct voat. co news aggregator. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 16, pages 1302–1311, 2022.

[72] Shaheed N Mohammed. Conspiracy theories and flat-earth videos on youtube. *The Journal of Social Media in Society*, 8(2):84–102, 2019.

[73] Robert Muggah. In brazil, qanon has a distinctly bolsonaro flavor. https://foreignpolicy.com/2021/02/10/brazil-qanon-bolsonaro-online-internet-conspiracy-theories-anti-vaccination/, 2021.

[74] Mohd Razman Achmadi Muhammad and Noor Nirwandy. A study on donald trump twitter remark: a case study on the attack of capitol hill. *Journal of Media and Information Warfare (JMIW)*, 14(2):75–104, 2021.

[75] CBS News. Twitter bans zero hedge after it posts coronavirus conspiracy theory. https://www.cbsnews.com/news/twitter-bans-zero-hedge-coronavirus-conspiracy-theory/, 2020.

[76] NBC News. Google bans website zerohedge from its ad platform over comments on protest articles. https://www.nbcnews.com/tech/tech-news/google-bans-two-websites-its-ad-platform-over-protest-articles-n1231176, 2020.

[77] NBC News. Amazon removes qanon merchandise from its marketplace. https://www.nbcnews.com/business/business-news/amazon-removes-qanon-merchandise-its-marketplace-n1253937, 2021.

[78] Leonardo Nizzoli, Serena Tardelli, Marco Avvenuti, Stefano Cresci, Maurizio Tesconi, and Emilio Ferrara. Charting the landscape of online cryptocurrency manipulation. *IEEE Access*, 8:113230–113245, 2020.

[79] Antonis Papasavva, Max Aliapoulios, Cameron Ballard, Emiliano De Cristofaro, Gianluca Stringhini, Savvas Zannettou, and Jeremy Blackburn. The gospel according to q: Understanding the qanon conspiracy from the perspective of canonical information. In *AAAI International Conference on Web and Social Media*, 2021.

[80] Antonis Papasavva, Jeremy Blackburn, Gianluca Stringhini, Savvas Zannettou, and Emiliano De Cristofaro. "is it a qoincidence?": An exploratory study of qanon on voat. In *Proceedings of the Web Conference 2021*, pages 460–471, 2021.

[81] Antonis Papasavva, Savvas Zannettou, Emiliano De Cristofaro, Gianluca Stringhini, and Jeremy Blackburn. Raiders of the lost kek: 3.5 years of augmented 4chan posts from the politically incorrect board. In *Proceedings of the international AAAI conference on web and social media*, volume 14, pages 885–894, 2020.

[82] Pujan Paudel, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini. Soros, child sacrifices, and 5g: understanding the spread of conspiracy theories on web communities. *arXiv preprint arXiv:2111.02187*, 2021.

[83] Paypal. Donate button. https://www.paypal.com/donate/buttons, 2023.

[84] Shruti Phadke, Mattia Samory, and Tanushree Mitra. What makes people join conspiracy communities? role of social factors in conspiracy engagement. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):1–30, 2021.

[85] Shruti Phadke, Mattia Samory, and Tanushree Mitra. Pathways through conspiracy: the evolution of conspiracy radicalization through engagement in online conspiracy discussions. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 16, pages 770–781, 2022.

[86] Filippo Radicchi, Claudio Castellano, Federico Cecconi, Vittorio Loreto, and Domenico Parisi. Defining and identifying communities in networks. *Proceedings of the national academy of sciences*, 101(9):2658–2663, 2004.

[87] Jodi Reffitt. Reffitt family fund. givesendgo.com/G23DE, 2021.

[88] Kevin Roose. What is qanon, the viral pro-trump conspiracy theory? https://www.nytimes.com/article/what-is-qanon.html, 2021.

[89] Elizabeth Schumacher. Disclose.tv: English disinformation made in germany. https://www.dw.com/en/disclosetv-english-disinformation-made-in-germany/a-60694332, 2023.

[90] Selenium. Selenium automates browsers. that's it! https://www.selenium.dev, 2023.

[91] Karolina Sliwa, Ema Kusen, and Mark Strembeck. A case study comparing twitter communities detected by the louvain and leiden algorithms during the 2022 war in ukraine. In *Companion Proceedings of the ACM on Web Conference 2024*, pages 1376–1381, 2024.

[92] Joe Sommerlad. Sabmyk network: Founder of bizarre new religion targeting qanon believers 'unmasked' by hope not hate. https://www.independent.co.uk/news/world/europe/sabmyk-network-qanon-conspiracy-theories-b1820639.html, March 2021.

[93] Carl Stempel, Thomas Hargrove, and Guido H Stempel III. Media use, social structure, and belief in 9/11 conspiracy theories. *Journalism & Mass Communication Quarterly*, 84(2):353–372, 2007.

[94] Maria Susana. Crimes against humanity. indiegogo.com/projects/crimes-against-humanity?create_edit=true, 2020.

[95] Amelia Tait. Pizzagate: How a 4chan conspiracy went mainstream. https://www.newstatesman.com/science-tech/2016/12/pizzagate-how-4chan-conspiracy-went-mainstream, 2016.

[96] Telegram. Telegram ad platform. https://promote.telegram.org, 2023.

[97] Vincent A Traag, Ludo Waltman, and Nees Jan Van Eck. From louvain to leiden: guaranteeing well-connected communities. *Scientific reports*, 9(1):5233, 2019.

[98] Milo Trujillo, Maurício Gruppi, Cody Buntain, and Benjamin D Horne. What is bitchute? characterizing the. In *Proceedings of the 31st ACM conference on hypertext and social media*, pages 139–140, 2020.

[99] Marc Tuters, Emilija Jokubauskaitė, and Daniel Bach. Post-truth protest: How 4chan cooked up the pizzagate bullshit. *M/c Journal*, 21(3), 2018.

[100] Jan-Willem Van Prooijen and Karen M Douglas. Conspiracy theories as part of history: The role of societal crisis situations. *Memory studies*, 10(3):323–333, 2017.

[101] The Verge. Reddit has banned the qanon conspiracy subreddit r/greatawakening. https://www.theverge.com/2018/9/12/17851938/reddit-qanon-ban-conspiracy-subreddit-greatawakening, 2023.

[102] VICE. Germany's 'biggest qanon mouthpiece' arrested in the philippine. https://www.vice.com/en/article/n7zexk/oliver-janich-germany-philippines, 2022.

[103] VSQUARE. Telegram, the free zone for disinformation and conspiracies. https://vsquare.org/telegram-the-free-zone-for-disinformation-and-conspiracies/, 2023.

[104] W. Freedomconvoy2022. givesendgo.com/FreedomConvoy2022, 2021.

[105] W. The big reset. kickstarter.com/projects/thebigreset/the-big-reset, 2021.

[106] Charlotte Wagnsson. The paperboys of russian messaging: Rt/sputnik audiences as vehicles for malign information influence. *Information, communication & society*, 26(9):1849–1867, 2023.

[107] Janith Weerasinghe, Bailey Flanigan, Aviel Stein, Damon McCoy, and Rachel Greenstadt. The pod people: Understanding manipulation of social media popularity via reciprocity abuse. In *Proceedings of The Web Conference 2020*, pages 1874–1884, 2020.

[108] Per-Olof H Wikström and Noémie Bouhana. Analyzing radicalization and terrorism: A situational action theory. *The handbook of the criminology of terrorism*, pages 175–186, 2016.

[109] Skip Willman. Traversing the fantasies of the jfk assassination: Conspiracy and contingency in don delillo's" libra". *Contemporary Literature*, 39(3):405–433, 1998.

[110] Ahmet S Yayla and Anne Speckhard. Telegram: The mighty application that isis loves. *International Center for the Study of Violent Extremism*, 9, 2017.

[111] Jing Zeng and Mike S Schäfer. Conceptualizing "dark platforms". covid-19-related conspiracy theories on 8kun and gab. *Digital Journalism*, 9(9):1321–1343, 2021.

A ChatGPT prompt

Table 8: Prompt used to ask GPT-4o whether the author of a message containing a monetization link is requesting funds or promoting a campaign or if they are discrediting a donation or crowdfunding project.

Prompt
The input provided is a text containing one or more URLs pointing to donation or crowdfunding platform. Classify the message with 1 if the message is asking directly or indirectly for donations, or to support a project. Otherwise, return 0 if the message is discrediting or asking to report the recipient of the donation or the project.

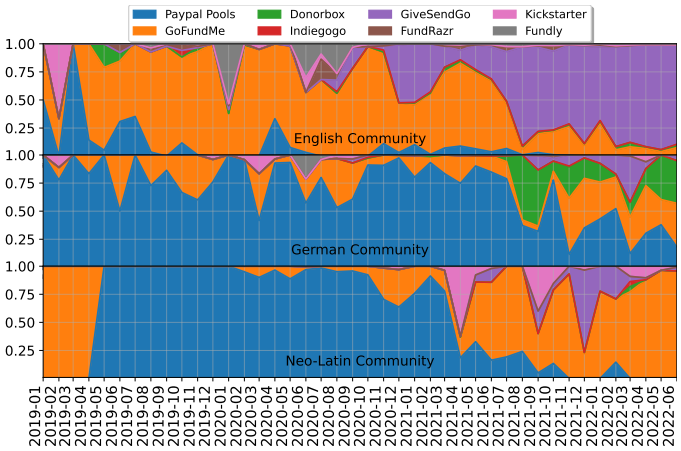

Figure 8: Crowdfunding platforms usage over time.

B Amazon content

Table 9: The five types of products most frequently advertised by conspiracy channels on Amazon.

Category	URLs	Distinct products
Books & eBooks	27,523 (54.72%)	5,213 (30.37%)
Fashion & Personal Care	7,820 (15.55%)	3,700 (21.56%)
Home & Living	6,715 (13.35%)	3,688 (21.49%)
Electronics & Technology	4,189 (8.33%)	2,358 (13.74%)
Sports & Outdoors	1,618 (3.22%)	636 (3.71%)

C Platforms usage over time

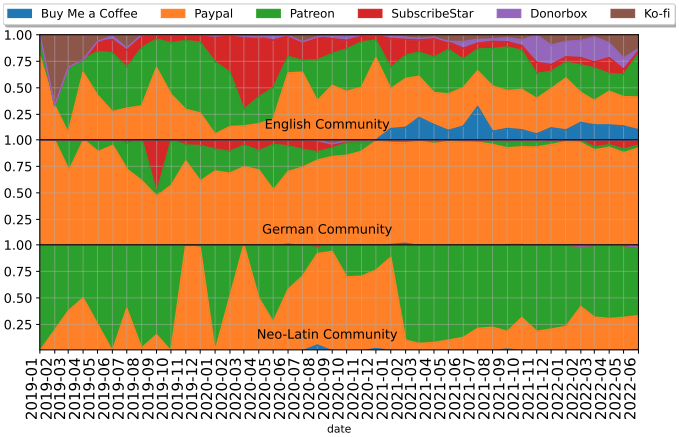

Figure 7: Donation platforms usage over time.