Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams

Xigao Li
Stony Brook University
xigli@cs.stonybrook.edu

Anurag Yepuri
Stony Brook University
ayepuri@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

***Abstract*—As cryptocurrencies increase in popularity and users obtain and manage their own assets, attackers are pivoting from just abusing cryptocurrencies as a payment mechanism, to stealing crypto assets from end users. In this paper, we report on the first large-scale analysis of cryptocurrency giveaway scams. Giveaway scams are deceptively simple scams where attackers set up webpages advertising fake events and promising users to double or triple the funds that they send to a specific wallet address. To understand the population of these scams in the wild we design and implement CryptoScamTracker, a tool that uses Certificate Transparency logs to identify likely giveaway scams. Through a 6-month-long experiment, CryptoScamTracker identified a total of 10,079 giveaway scam websites targeting users of all popular cryptocurrencies. Next to analyzing the hosting and domain preferences of giveaway scammers, we perform the first quantitative analysis of stolen funds using the public blockchains of the abused cryptocurrencies, extracting the transactions corresponding to 2,266 wallets belonging to scammers. We find that just for the scams discovered in our reporting period, attackers have stolen the equivalent of tens of millions of dollars, organizing large-scale campaigns across different cryptocurrencies. Lastly, we find evidence that attackers try to re-victimize users by offering fund-recovery services and that some victims send funds multiple times to the same scammers.**

I. Introduction

What started as a technical paper titled "Bitcoin: A peer-to-peer electronic cash system" released by a previously (and still) unknown individual named Satoshi Nakamoto in 2008 [60], has since become one of the most promising new technologies since the Internet itself. The concept of cryptocurrencies and the blockchains supporting them has attracted billions of dollars in funding and investments, innumerable new startup companies, and thousands of academic papers proposing new consensus algorithms, transaction settlement layers, and novel blockchains with entirely different properties compared to the originally proposed Bitcoin.

This increased activity did not go unnoticed by attackers who initially saw cryptocurrencies as a means of extracting payments from users, in the context of ransomware [31], [43], [44], [49] and blackmailing [11], [66]. As cryptocurrencies kept growing in popularity and kept attracting new users, attackers pivoted from just using cryptocurrencies as a payment channel to stealing cryptocurrency assets from end users. Whether through malicious software stealing users' private keys [22], [36], [39], the hijacking of accounts on online exchanges [12], [18], [34], vulnerabilities in smart contracts [10], [32], [62], or even the sale of hardware wallets with pre-set seed phrases [29], [50], [61], attackers are regularly stealing assets worth millions of dollars from end users and institutional investors.

One of the most recent attacks targeting cryptocurrency users are the so-called giveaway scams. In these scams, attackers set up professional looking websites that abuse the names and images of celebrities to advertise "giveaway" events, purportedly in order to popularize cryptocurrencies. These sites promise to double or triple the funds that users send to a specific wallet address, that is in fact controlled by the scammer. Figure 1 shows an example of a giveaway scam. Scammers then drive traffic to these websites through any means possible, most commonly by compromising popular YouTube channels and social-media accounts with hundreds of thousands of subscribers and followers. The most popular instance of this attack is likely the 2020 Twitter hack where social engineering was used to obtain access to Twitter's internal systems resulting in 130 accounts belonging to high-profile individuals all tweeting the same giveaway scam at the same time [28].

Unsurprisingly, once users are convinced to send funds to the wallet addresses listed in a giveaway scam, they will never get any funds back. Moreover, unlike traditional scams involving the charging of credit cards and bank accounts that may be reversible, the distributed and trustless nature of cryptocurrencies does not allow for the reversing of any charges. While there is a growing consensus that giveaway scams are an increasing problem on the web and some preliminary statistics on giveaway scams reported by the FTC estimate the losses in the order of millions of dollars [27], most reports are still anecdotal in nature from users who come forward after falling victim to these scams.

In this paper, we present the first systematic analysis of cryptocurrency giveaway scams in the wild. To discover as many scams as possible without relying on user reports, we propose CryptoScamTracker, a system that taps into Certificate Transparency logs and records all domains that contain one or more cryptocurrency-related keywords and were recently issued TLS certificates. These domains are then automatically crawled by multiple crawlers and those that contain tell-tale signs of giveaway scams are reported to analysts for final verification. In a six-month period starting from January 1, 2022, CryptoScamTracker recorded 10,079 giveaway scam websites hosted on a total of 3,863 domains. By analyzing the domain names that scammers registered and the hosting infrastructure supporting

Network and Distributed System Security (NDSS) Symposium 2023
27 February - 3 March 2023, San Diego, CA, USA
ISBN 1-891562-83-5
https://dx.doi.org/10.14722/ndss.2023.24584
www.ndss-symposium.org

their websites we make a number of observations including the fact that scammers tend to prefer high-cost traditional gTLDs for their domains and host the majority of their websites on hosting providers that are otherwise unpopular. We discover that 75% of scam domains are registered mere days before they are weaponized for giveaway scams and that, for some cryptocurrencies such as Ethereum and Ripple, the number of live scam websites is correlated with the price of the underlying asset (i.e. scammers deploy more scams when the asset rises in price).

Next to characterizing the infrastructure and patterns of these giveaway scam pages, we perform the first real-world analysis of stolen funds, not based on anecdotal reports, but based on all the transactions that we can extract from public blockchains, corresponding to the 2,266 wallets addresses that we identified on scam pages. Among others, we discover that, just for Bitcoin, in the six-month period of our study, scammers were able to steal a total of 940.07 BTC corresponding to more than $18M. When one considers all the scams targeting Bitcoin, Ethereum, Cardano, and Ripple during the period of our study, we calculate that scammers stole a total of $24.9M–$69.9M (using the minimum and maximum prices of all four cryptocurrencies during our study). Moreover, by further analyzing the transactions on the scammers' wallets we find evidence that users are prone to be victimized more than once (e.g. there exist users who send funds multiple times to the same scammers) and that the most prolific scammers are responsible for large-scale campaigns operating hundreds of domain names across multiple cryptocurrencies.

Overall, we make the following contributions:

- We propose CryptoScamTracker, a tool that can automatically identify likely giveaway scams in the wild and use that tool to understand the giveaway scam phenomenon over the first half of 2022.
- We collect a wealth of statistics regarding the preferences of scammers on TLDs, hosting infrastructure, content of pages, and how these can be potentially turned against them.
- We perform the first quantitative analysis of financial loses due to giveaway scams that does not use assumptions or approximations, but instead *counts* all the transactions that are available in the identified wallets of scammers.

Given the difficulty of capturing cryptocurrency scam websites and the dearth of precise data on giveaway scams, we are releasing the dataset that we curated through CryptoScamTracker at https://double-and-nothing.github.io/.

II. System Design

To collect cryptocurrency scam domains, we design CryptoScamTracker, a tool that automatically identifies websites that are likely candidates for cryptocurrency giveaway scams. CryptoScamTracker consists of three modules: a domain monitoring module, a crawl-and-detection module, and an analysis module. The overall architecture of CryptoScamTracker is shown in Figure 2.

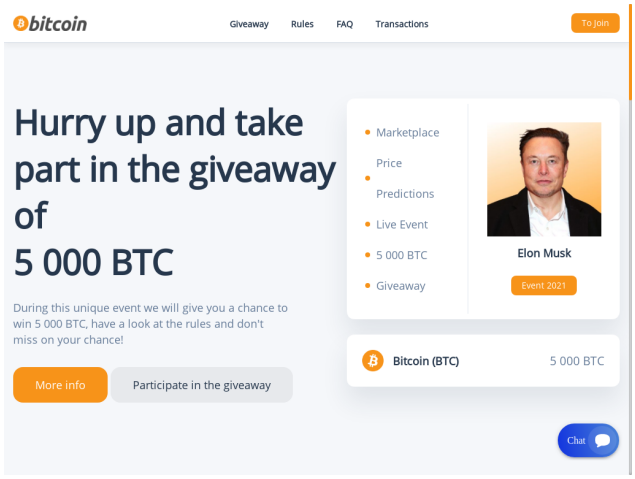

Fig. 1: *Example of cryptocurrency scam web page.*

A. Module Design

Domain monitoring module: Given the relative nascence of cryptocurrencies, it stands to reason that scams targeting cryptocurrency users must be more targeted than other types of social-engineering-based attacks, such as, phishing, technical support scams [57], and fake surveys [19], [45]. If attackers would just show cryptocurrency scams to all users indiscriminately, they would not only attract a small minority of those users (i.e. the fraction of users who have cryptocurrencies *and* are convinced by the scam) but also unnecessarily expose themselves to a wider audience leading to faster takedowns of their scam websites. As such, in order to detect cryptocurrency-giveaway scams, we require a more targeted approach compared to past works that browsed low-quality sites (such as sites offering free streaming of otherwise paid content) and then just followed ads [57], [68], [79].

To understand how users land on cryptocurrency giveaway scam websites, we read a number of anecdotal reports, both by victims of these scams, as well as by central figures in the cryptocurrency space warning people about these types of scams [1], [30], [42], [48], [56], [71]. Through this process, two main ways of targeting users emerged: compromised social media and compromised video streaming accounts. In both cases, attackers infiltrate the accounts of popular users (e.g. a popular Twitter user or a popular YouTube account) and then use these accounts to send out spam to their followers and channel subscribers. Table XIII in the Appendix lists the top 20 Google Search results in November 2022 related to "cryptocurrency giveaway scams", where almost all articles list social media and YouTube as a starting point for luring users to scam websites. Depending on the underlying platform, scammers can either use text messages (e.g. tweets) or upload cleverly-edited videos showing a cryptocurrency-related celebrity (e.g. an interview with the creator of Ethereum [23] or Cardano [17]) with links to their scam giveaway pages superimposed on these videos. A video demo of how users can stumble upon this content on YouTube is available on this URL: https://vimeo.com/775187519

In both cases, we noticed that the URLs that the compromised accounts posted were highly tailored to the cryptocurrencies being targeted. All of the domains associated with these URLs contained one or more keywords associated with a cryptocurrency (e.g. `ethereum-giveaway-2022.net`) and appeared to have been registered for the express purpose

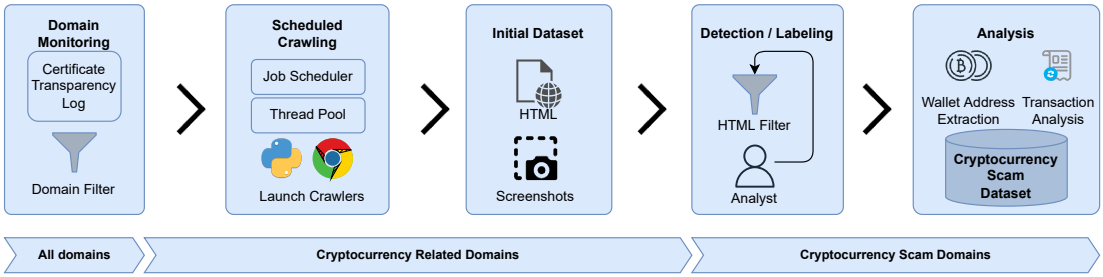

Fig. 2: *Overall architecture of CryptoScamTracker. Using the Certificate Transparency log as an input, CryptoScamTracker identifies domains that are associated with cryptocurrencies and automatically crawls them. The crawled data is then inspected by analyst to remove false positives before the final step of the analysis which involves extracting transaction information from public blockchains.*

of conducting one or more giveaway scams. Based on this observation, we opted to bypass the gateway pages that redirected users to the scam webpages (e.g. compromised YouTube and Twitter accounts) and identify the scam domains directly. In this way, CryptoScamTracker is not constrained by API limits imposed by the abused platforms (such as the number of Tweets that we can access per day) and can also identify scams that were conducted over smaller, less popular platforms.

To this end, we chose to take advantage of the Certificate Transparency (CT) log, where Certificate Authorities announce the issuance of every new certificate they create. Given the expectation of popular browsers for websites to make use of certificates with corresponding entries in CT logs, it is highly unlikely that a newly registered domain with a newly issued certificate will not present evidence of that certificate in a CT log. This is particularly true for Let's Encrypt certificates whose use has been skyrocketing, both by benign as well as malicious websites. Prior work has shown that CT logs can be successfully used to identify phishing websites targeting popular brands and institutions [8], [26], [46], [70], [72].

CryptoScamTracker taps into the constant stream of newly issued certificates and monitors the domains that the certificates correspond to. Any domains containing one or more keywords from a list that we curated based on our manual analysis of previous giveaway scams are forwarded to our crawling module that is responsible for actually visiting the website and scraping its contents. Table XI in the appendix lists the keywords used by CryptoScamTracker. Through this selective crawling, we capture domains that involve multiple cryptocurrency-related activities including giveaway scams, news sites and personal blogs related to cryptocurrencies, cryptocurrency faucets, online casinos, and investment websites.

Creating a domain name and obtaining a TLS certificate for that domain (with the corresponding entry in a CT log) does not necessarily mean that the website is accessible. To address this issue, we made use of an additional mechanism that will check back if the website is accessible every 12 hours. Whenever a website is accessible and returns an HTTP 200 response, the website is forwarded to the next module in the CryptoScamTracker pipeline.

Crawl and detection module: For domains that contain one or more cryptocurrency-related keywords, CryptoScamTracker schedules two separate crawling jobs, using a headless Python crawler as well as a fully-functional Selenium-controlled browser. The reason for performing two crawls is to be able to later identify whether a scam website uses cloaking-based evasions that are able to detect one crawler but not the other. We discuss the general effect of cloaking on CryptoScamTracker in Section V. Through these crawls, we collect the HTML code of the webpage along with a screenshot.

CryptoScamTracker extracts the text from the HTML code and attempts to match a number of cryptocurrency-related keywords against that text. We arrived at our exact list of keywords by using a form of *snowball sampling* [33]. Namely, we start with a list of keywords that we identified through our manual analysis of past scams and then analyze the domain names that are discovered using these keywords. Through this analysis, we identify more commonly-recurring keywords used by cryptocurrency giveaway scams which we then add to our list of keywords. After a few iterations of this snowball sampling method, our list of keywords stabilized and was able to support CryptoScamTracker for the entirety of this experiment. Once a website is crawled and its HTML code and screenshot has been collected, it is stored in a database for later manual verification.

CryptoScamTracker can identify multiple variations of scam websites which we further discuss in Section III-C. Early on in our experiment, we discovered that one type of cryptocurrency giveaway scam used a "fork" style where users could select their cryptocurrency of choice and then be exposed to a different cryptocurrency giveaway page (e.g. Bitcoin vs. Ethereum). For these scams, CryptoScamTracker attempts to crawl more than just the main page of the scam website, in order to be able to extract the HTML code of the actual giveaway pages which we use in our later analysis.

To establish the lifetime of these scam giveaway pages, CryptoScamTracker also conducts a liveness check for each confirmed domain. We store "live" websites into a list and periodically issue requests to each domain on the list to test whether the response code is valid. If the web server returns a valid response, we compare the content to our original capture. If the captured content matches the original content, we keep the website in the list. If the website returns an error or drastically different content (often indicative of a suspension/takedown warning by the hosting provider), we count the number of such "invalid" responses and stop scanning scam domains after three such errors.

Analysis Module: After we mark a website as a cryptocurrency scam, we extract the following types of information:

- **Domain information.** We collect the domain names and subdomains, corresponding IP address, WHOIS data, and timestamps of when it was first detected and last active.

- **Website information.** CryptoScamTracker record the HTML code of a cryptocurrency scam website along with screenshots

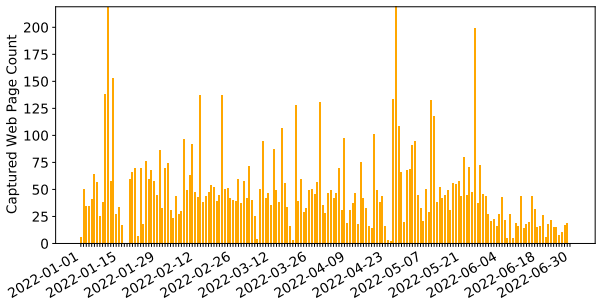

Fig. 3: *Number of daily scam websites discovered by CryptoScamTracker. On average, our tool captures* 55.7 *web pages each day.*

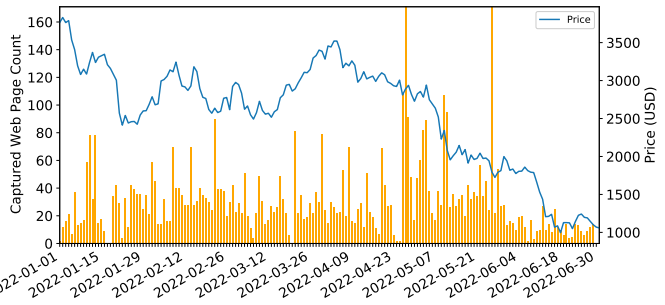

Fig. 4: *Distribution of new scam websites targeting ETH versus ETH prices.*

of the page. To understand the use of third-party services by scammers, CryptoScamTracker also records remote images and JavaScript content found in the crawled pages.

• **Blockchain information.** Using a set of regular expressions, CryptoScamTracker parses the HTML content to identify the blockchain that scammers are targeting (e.g. Ethereum vs. Bitcoin) and extract the wallet address belonging to scammers (the one where users are instructed to send funds). Given the permanent nature of the studied cryptocurrencies, we can later use their public blockchains to extract transaction information from the identified wallets.

B. Labeling Cryptocurrency Scams

To ensure the curation of a scam dataset free of false positives, we manually inspect the websites that are captured from CryptoScamTracker's pipeline. To this end, we implemented a custom web application that provides analysts a dashboard displaying screenshots of the captured websites along with labeling options. An analyst can straightforwardly identify true positives using our screenshots and extracted keywords from a website's HTML body. Given our current list of cryptocurrencies and the current levels of scam activity against them, CryptoScamTracker captures an average of 55.7 suspicious websites each day, which translate to less than 5 minutes of labeling effort per day. Due to our labeling frequency and our desire to not change the scammer ecosystem while measuring it, we chose not to report these scams in real time. Section V expands upon this decision.

III. Dataset Analysis

In this section, we provide a detailed analysis of our captured dataset collected over a 6-month period (January 1, 2022 to July 1, 2022). Overall, our dataset contains 10,079 cryptocurrency scam web pages. These 10,079 captured web pages, were served by a total of 3,863 domains, which resolved to 2,712 IP addresses. From all the cryptocurrency scam websites, we extracted 2,266 scammer wallet addresses.

A. Infrastructure of giveaway scams

Daily Captures: Figure 3 shows the number of web pages we captured over the duration of our experiment. Scammers are constantly setting up new websites which are then captured and recorded by CryptoScamTracker. On average, CryptoScamTracker identified 55.7 new cryptocurrency giveaway scams each day.

To understand whether the price of a cryptocurrency correlates with the number of scam pages targeting its users (i.e. are scammers shifting their attention *to* a cryptocurrency as its price rises), we compare daily cryptocurrency prices with the number of daily scam pages targeting it. Figure 4 shows the fluctuation of the price of Ethereum (ETH), along with the number of scams that CryptoScamTracker discovered each day. We calculated the Pearson product-moment correlation coefficients for each cryptocurrency, but we did not find a significant correlation between the price of a specific cryptocurrency and the number of scams targeting it; for example, the correlation for ETH is 0.22. The correlation between price and number of scams is less pronounced for Bitcoin, Cardano, and XRP (Figures 9–11 available in the Appendix).

TLDs, Domain names, and Hosting providers: We investigate how scam website operators choose over the hundreds of public TLDs that they could use to register their scam domain names. Table I lists the 10 most popular TLDs used by scammers, covering 89.12% of the domains in our dataset. Overall, traditional generic TLDs (gTLDs) are more favored than other more recent TLDs, with ".com", ".org", and ".net", covering more than 72.87% of all scam domains. We use the minimum price available for each TLD to calculate the total registration cost for one year for those domains. We discovered that although some recent TLDs are much cheaper than those popular TLDs, scammers still choose the expensive, traditional TLDs. The total registered cost for top 10 TLDs is more than 22,620.42 dollars, where the total cost for registering all top 3 TLDs is approximately 19,195.34 dollars. In contrast, in the latest phishing report of APWG (Q4 2021), only 60% of generic phishing is using gTLDs [9]. Given that low-cost TLDs are associated with malicious activity, scammers can sidestep any negative reputation associated with low-cost TLDs by merely paying a higher registration price. In Section IV, we show that successful scammers can steal cryptocurrencies worth hundreds of thousands of dollars, negating any small upfront domain registration and hosting costs. At the same time, as Figure 8 (available in the Appendix) shows, we did not find evidence that the cost of domain registration is correlated with the amount of funds stolen by scammer.

Next, we turn our attention to the hosting providers that scammers choose to host their cryptocurrency giveaway scams. Table II lists the top 10 hosting providers hosting 2,642 (77.95%) websites. To understand whether scammers use different hosting providers than regular websites, we crawl the top 10K websites (according to Majestic Million [54]) and determine their hosting providers. By contrasting the hosting

TABLE I: *Captured Top 10 TLDs and market prices. The minimum price is the cheapest registration price available across multiple domain registrars.*

TLD	Domain Count	Minimum register price (USD)	Total estimated cost
com	1,435	7.16	10,274.6
org	762	7.66	5,836.92
net	618	4.99	3,083.82
us	156	0.99	154.44
info	127	1.95	247.65
live	113	1.88	212.44
io	74	28.74	2,126.76
online	49	0.99	48.51
gift	42	13.24	556.08
tech	36	2.2	79.2
(Total)	3,412	-	22,620.42

TABLE II: *Top 10 hosting providers. The last column shows whether each hosting provider is also hosting popular sites (Majestic top 10K)*

Hosting Provider	Domain Count	Pct. in Dataset	Popular Hosting Provider?
CLOUDFLARENET	1,521	44.88%	✓
REGRU-NETWORK	330	9.73%	✗
DDOS-GUARD	321	9.47%	✗
NameCheap (NCNET/NAMEC)	302	8.91%	✓
SELECTEL-NET	60	1.77%	✗
NET-135-1	24	0.7%	✗
HOSTINGER-HOSTING	24	0.7%	✗
VDS-and-Dedics	20	0.59%	✗
RU-BAXET-20200402	20	0.59%	✗
Partnerllc-net	20	0.59%	✗
(Total)	2,642	77.95%	-

providers of scam sites vs. the ones of benign popular sites, we identified a number of providers that host high concentrations of scam sites yet low concentrations of popular benign sites. The most notable case is DDoS-GUARD, hosting 9.47% of all scam websites yet only 0.05% of benign top 10K websites. This discrepancy could indicate either that that hosting provider knowingly acts as a bulletproof hosting provider for scammers [7], [47], [63], or that scammers have found ways to abuse their hosting infrastructure without that company's knowledge.

For domain registrars, we discovered that scammers favor less popular domain registrars (such as reg.ru), which could again be an indication of bulletproof/mismanaged infrastructure.

Registrants and Domain Structure: Among the other information that CryptoScamTracker collects is the WHOIS data for each discovered domain. Traditionally, WHOIS data contained the names, email addresses, and addresses of the persons who registered and operated any given domain name. However, because WHOIS information was often abused for SPAM [51], [81], "private" registrations gradually became the default where the registrar hides the exact identity of the registrant and only offers an alias email address that can be used to contact the owner of a domain name without betraying their identity.

Interestingly, while the majority of emails in the WHOIS information of scam domains were of the private kind, there were still hundreds of domain names whose owners' email addresses and other information was still available. We suspect that this relates to the use of non-popular registrars by scammers, who operate in countries with fewer expectations of domain privacy. Table XII (in the Appendix) shows the top 10 most commonly occurring email addresses (which we have partially anonymized) on the scam domains that CryptoScamTracker recorded. These email addresses could be used by themselves or in conjunction with repeating wallet addresses to identify campaigns where multiple distinct scam domains are operated by the same scammer. In Section IV-B we describe our methodology for clustering individual scams into campaigns.

In terms of domain-name structure (i.e. the words that scammers choose to embed in the domains they register), we observed that scam domains tend to commonly use year-related keywords combined with cryptocurrency names, for example, `22-shib.com` and `2022-ethereum.org`. Out of a total of 3,863 TLD+1 domains, we found 1,486 (38.47%) domains contain the word "2022" or "22", where only 12 (0.31%) contain word "2021" or "21". An interpretation of this pattern is that scammers are trying to convince users of a currently ongoing and live event that is time-limited. In this way, users are encouraged to act as fast as possible, lest they miss out on the opportunity of doubling their cryptocurrencies. Similarly, another common domain-name pattern is the inclusion of a multiplier in the domain name, such as, "2x" and "3x" referring to the doubling or tripling of a user's cryptocurrencies during this "event". CryptoScamTracker discovered 1,348 (34.89%) domains containing these multiplier keywords. Lastly, other common words that appeared in the giveaway scam domain names were "events", "giveaway", and "official" further supporting the facade of a special and time-limited event which users are encourage to take advantage of as quickly as possible.

IP addresses: Given our earlier finding that scammers are not price sensitive when it comes to registering domain names for their giveaway scams, the natural next question is whether they reuse hosting across scams (i.e. is a given webserver hosting more than one giveaway scam at a time).

Among 2,712 IP addresses discovered by CryptoScamTracker, only 401 (14.79%) IP addresses are hosting multiple domains. These "multi-scam" IP addresses host an average of 4.41 domains per host. This minority of attackers who reuse hosts could indicate either scammers who were not successful with their first scam and are trying to amortize their hosting costs over multiple registered domains, or potentially scammers who prefer the simplicity of managing fewer servers and feel no need to migrate their infrastructure, given the low rates of blocklisting. Separate from whether a specific malicious server hosts one or more giveaway scams, Figure 12 (in the Appendix) shows the distribution of hosting across countries with the top countries being US and Russia (confirming our earlier finding regarding the DDOS-GUARD hosting provider), followed by the Netherlands, Brazil, and Germany.

B. Targeted Cryptocurrencies

So far, we have presented statistics about the scams that CryptoScamTracker discovered in aggregate, i.e., without placing any particular emphasis on specific cryptocurrencies. In this section, we perform a deep dive into the different types

TABLE III: *Number of scam websites and domains targeting each cryptocurrency, along with the market cap of each cryptocurrency as of July 2022. Scam websites that target more than one cryptocurrency are counted across multiple rows.*

Cryptocurrency Type	Websites	Domains	Market Cap
ETH / Ethereum	6,777	2,602	$162 Bil.
BTC / Bitcoin	5,980	2,067	$400 Bil.
XRP / Ripple	1,303	686	$17 Bil.
ADA / Cardano	818	369	$15 Bil.
BNB / Binance	816	434	$41 Bil.
SHIB / Shiba Inu	712	393	$6 Bil
DOGE / Dogecoin	447	202	$9 Bil.
SOL / Solana	132	41	$13 Bil.
USDT / Tether	90	31	$66 Bil.
TRX / TRON	64	34	$6 Bil.
DOT / Polkadot	61	27	$7 Bil.
ALGO / Algorand	19	7	$2 Bil.
HEX / HEX	18	13	$7 Bil.

of cryptocurrencies, in order to assess whether some cryptocurrencies attract more attackers than others and for what purpose.

Table III shows the number of scam websites and domains that CryptoScamTracker discovered, for each of the evaluated cryptocurrencies. The four most targeted cryptocurrencies are Ethereum (ETH), Bitcoin (BTC), Cardano (ADA), and Ripple (XRP). Together, these four cryptocurrencies attracted 90% of the websites in our dataset.

Giveaway scam websites are clearly targeting popular cryptocurrencies with large market capitalizations (the value of all currently mined coins) and a large footprint on social media. Yet market capitalization does not explain why Ethereum (with a market cap of $162 Billion as of July 2022) attracted 25% more giveaway scams compared to Bitcoin (market cap of $400 Billion) during the same period. We argue that this outsized attention from scammers has multiple plausible explanations. First, Ethereum was the first cryptocurrency to support smart contracts and Decentralized Applications (Dapps) where users have been trained to use their software wallets (e.g. Metamask) to interact with websites, other than just sending and receiving coins (as is the case in Bitcoin). It is therefore reasonable to assume that Ethereum users who are accustomed to interacting with their wallets more frequently may be more attractive targets, from the point of view of scammers. Second, given the unknown identity of Bitcoin's creator, scammers cannot create the same plausible stories as with other cryptocurrencies (such as Ethereum and Cardano) where they can abuse the recognition of key figures in the context of fake giveaway events.

Once scammers register a domain name for a giveaway scam, they can set up multiple webpages all from the same main domain. Out of 3,863 domain names discovered by CryptoScamTracker, 2,246 (58.1%) domains host multiple web pages corresponding to one or more cryptocurrency scams. The most common hosting technique we observed is creating multiple subdomains and pointing them to same content, such as `ms.coinsharedgift.live` and `ms22.coinsharedgift.live` possibly as a reaction to blocklisting. Another strategy involves hosting multiple subdirectories where each page is targeting victims. For example, `teslamuskgifts.com/eth/index.html` and `teslamuskgifts.com/btc/index.html` leads to different webpages targeting Ethereum and Bitcoin users, respectively. The latter strategy usually involves a main page offering users the option to continue to their desired cryptocurrency, similar to the style #4 listed in Table V.

TABLE IV: *Most frequent word/phrase that appeared in textual data of cryptocurrency scam webpages discovered by CryptoScamTracker.*

Rank	Top words	Presence in Web pages	Percentage
1	from/to	9,683	96.07%
2	send/sent	8,786	87.17%
3	participate/join	8,732	86.64%
4	just/just need	8,540	84.73%
5	address	8,296	82.31%
6	giveaway	8,227	81.63%
7	event	7,856	77.94%
8	x2/x3	7,583	75.24%
9	contribution	7,432	73.74%
10	rules	6,991	69.36%

C. Content of scam pages

HTML content: Scammers use specific words and phrases to convince users to send funds to their illicit wallet addresses. To understand what words are used in scam web pages, we investigated the textual data from each captured HTML source page. Table IV presents the most frequent words used in the recorded scam pages as captured by CryptoScamTracker, with similar words grouped together. For instance, CryptoScamTracker discovered 9,683 scam webpages that contain the word "from" or "to" or both. Most frequent words in HTML content are "participate/join", "giveaway", "send/sent", and "from/to". The analysis of the titles of these pages produces similar results with the addition of the names of the specific targeted cryptocurrencies (e.g. "Ethereum" and "Cardano"). Overall, in terms of their textual content, the scam pages discovered by CryptoScamTracker are highly similar. The top 500 words discovered in these pages cover 80.17% of the total words in the HTML page content.

Page Layout and Appearance: To understand to what extent scammers reuse templates across scams, we use perceptual hashing on the screenshots collected by CryptoScamTracker and use these hashes to form similarity clusters. Table V presents the results of this process. Overall, we successfully clustered 3,832 webpage screenshots to 1,198 clusters. Images in the same cluster are visually similar, which means they have similar elements, color as well as design layout.

To efficiently identify clusters, we choose those that have five or more screenshots and manually inspect the images from each cluster. Screenshots in the same cluster may have small differences in color, elements, and text but overall have similar visual styles and certain obvious common patterns, such as, the portrait of a specific celebrity or a QR code located in approximately the same position on the page. Overall, we labeled 139 clusters with 2,312 images into five visual styles.

The most common style (Style #1) of web page displays a large "Giveaway" message in the left part of page and use a

TABLE V: *Website appearance style. The web page screenshots are clustered by wavelet hashing, then manually labeled. Screenshots in the same cluster are similar in visual, color and element location, whereas clusters in the same style are only similar in visual layout.*

Style #	Style Detail	Clusters	Screenshots
1	Scam web page with celebrity portrait	44	907
2	Scam web page without celebrity portrait	22	430
3	Media article style	8	178
4	"Fork" style with two or more cryptocurrency	14	202
5	QR Code visible in first page style	2	26

portrait of celebrity related to the cryptocurrency on the right side. These web pages place the wallet address and QR code of that address towards the bottom of the page. The second variation (Style #2) is similar to the first one, but without portrait of celebrity. The web page either sets the page title in the center of the page or uses an animated cryptocurrency icon replacing the celebrity portrait.

The third variation (Style #3) is written in media article frameworks like *Medium*. The scammer does not place the wallet address or QR code in the main page, but rather uses links to redirect visitors to separate websites whose appearance matches the two aforementioned styles. Apart from setting up their own domains and webpage content, CryptoScamTracker also discovered the abuse of existing blogging platforms (such as Telegra.ph) for hosting new giveaway scams.

The fourth variation (Style #4) is different in that it aggregates multiple giveaways, allowing users to select the cryptocurrency they are interested in and subsequently redirecting them to a different URL that is targeting that specific cryptocurrency. The last variation (Style #5) shows the QR code and wallet address at the very top of the page and follows less modern aesthetics. Independent of their style, most webpages use JavaScript code to generate fake transactions that they show on the page, to convince the current user that the giveaway event is legitimate and that other users are already successfully participating in it. These transactions purport to show user wallets sending funds and receiving twice the amount, but are just randomly-generated wallet-like strings that are added to the page's DOM in regular intervals. Our aforementioned video demo shows this effect on a real cryptocurrency giveaway scam [4].

By analyzing samples of the screenshots that do not belong to the aforementioned five styles, we discovered evidence of crawler evasion where the visited page was checking our browser but never redirected CryptoScamTracker to the actual scam or in fact redirected us to an unrelated page (such as a YouTube video) because it detected that our crawler was not, in fact, a regular user. We report on the evasion scripts that we discovered later in this section. Overall, we discovered a high degree of template reuse both within a cryptocurrency but also in a cross-cryptocurrency fashion where, for example, Ethereum scams can be come Cardano scams by merely switching the celebrity portrait, the text, and wallet address of the scammer. We expect that the deployment of these pages is largely automated, allowing scammers to launch tens of new scams on new domains, on a daily basis. Our clustering results in Section IV-B support this hypothesis.

JavaScript Analysis: Since scammers are reusing templates across their scams, we investigate to what extent they also reuse JavaScript code and whether that reuse could somehow be turned into an early-detection system. To this end, we extracted the inline and third-party scripts that CryptoScamTracker recorded as part of each visited giveaway scam.

TABLE VI: *JavaScript Libraries discovered on giveaway scam pages.*

Category	Count	Library Example
JQuery	12,795	JQuery, JQuery.min
Live chat services	8,372	SmartSuppchat, Tawk.to
Animation Libraries	2,363	wow.js, aos.js, toast.js
Analytics	399	Google Analytics, Yandex Metrica
Website Obscurity	476	console-ban.js

As Table VI shows, we discover five common categories of third-party scripts on which these scam sites rely. The most common type of included resource is jQuery (either hosted on the user's server or on a CDN) which scammers use to simplify their interactions with the page's DOM. Overall, we found that 12,795 instances of JQuery on scammers' webpages.

The second most popular type of JavaScript libraries that scam websites rely on is related to live chat services. The live-chat services offer a chat-as-a-service product allowing website owners to chat, in real time, with the visitors of their web pages. Surprisingly, these types of services are commonly abused by scammers, with 8,372 giveaway websites using such a service. Given the nature of giveaway scams, we expect that these services allow scammers to interact with hesitant users in real time and convince them of the "legitimacy" of the giveaway. In terms of abused services, we observed that scammers flocked around two specific chat services, SmartSuppChat and Tawk.to which offer a free tier of service that giveaway scammers can straightforwardly abuse. Our aforementioned video demo includes our interaction with scammers over an abused chat service [4].

The third most commonly used type of JavaScript library is related to animation and visual effects library, like *wow.js*, *aos.js*, and *toast.js*. These libraries are used to make websites appear more professionally designed and aesthetically pleasing, which we expect is a requirement when trying to convince users of the legitimacy of a giveaway event. The fourth type is related to website analytics, mostly through *Yandex Metrica* and *Google Analytics*. Prior work has shown that malicious sites commonly use analytics in order to understand how many victims they reach and, depending on the analytics service being used, these analytics could be used to attribute different malicious sites back to a common operator [74].

The fifth most commonly encountered JavaScript library was related to anti-debugging [59]. Namely, the `console-ban.js` file that we encountered on 476 websites used various undocumented DOM APIs and side-channels to establish whether the Developer Tools of the visiting browser is currently visible. If it is, the library can immediately redirect the user to another webpage or rewrite the current DOM with arbitrary content. Most of the giveaway scam websites redirect users to the same default third-party URL that ships together with that library. As such, we can clearly infer that scammers are using an off-the-shelf anti-debugging library to stop the analysis of their webpages, without necessarily knowing how that library works or whether it should be customized.

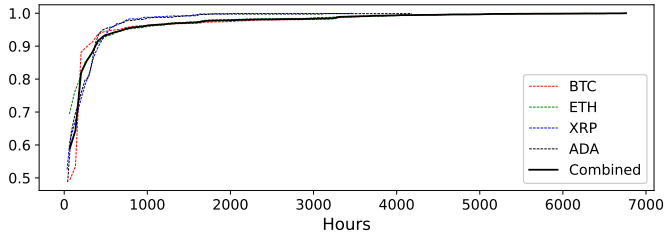

Fig. 5: *CDF of of the lifespan of giveaway scam websites. Though most websites have short lifespans, some remain reachable even at the end of our capture.*

Of all of the aforementioned types of commonly used, third-party libraries, the ones served by companies (such as live-chat services and analytics) are the best candidates for converting them into an early-detection system against giveaway scams. Namely, in the same way that contextual advertising scripts read a page's contents in order to identify the best type of ad to serve, these scripts could read the page contents in search of tell-tale signs of cryptocurrency giveaway scams. The pages that contain these signs can be flagged for manual inspection by these companies, which can then verify their nature, remove them from their list of clients, and optionally report them to blocklists. In this way, these companies can disassociate themselves from scammers while protecting the broader web ecosystem. Since their scripts are hosted remotely, scammers cannot modify them to remove the giveaway-detection logic. If scammers decide to host their own local copies of modified scripts, they will have to accept a risk of breakage where their local versions trail behind the official versions with potentially different server-side API signatures. Moreover, local copies of libraries that are meant to be remote, can itself be turned into an early-warning signal by anti-malware scanners.

D. Lifespan of scams and blocklisting

Figure 5 shows the CDF of website lifespan as established by CryptoScamTracker. We observe that half of the giveaway websites have a short lifespan of 26.18 hours. The shortest lifespan was less than 1 hour, whereas the longest lifespan 4,387.56 hours. In fact, some websites were still online at the end of our capture. When a giveaway scam domain becomes unavailable, this could be the result of a takedown by its hosting provider, the registrar, or even the scammers who delete their own websites, possibly in order to make forensic analysis more difficult after a successful scam.

Separate from the lifespan of giveaway sites, we also investigate the time between captured time and creation time. Our intuition was that these domains were registered for the express purpose of hosting one or more giveaway scams and therefore their registration time should be close to when they went "live" and were detected by CryptoScamTracker. For each domain we captured, we query its creation time from the WHOIS registry. The deltas between registration time and detection time are shown in Figure 6. Overall, 50% of the cryptocurrency scam websites have a short time delta that is less than 14.14 hours and 75% of the websites have a time delta of 195.70 hours. These findings support the notion that most giveaway-related domains are newly registered and not old domains that were repurposed for these scams. Contrastingly, Oest *et al.* [64] reported that for generic phishing, 53.3% of domains used by phishers were at least one-year old.

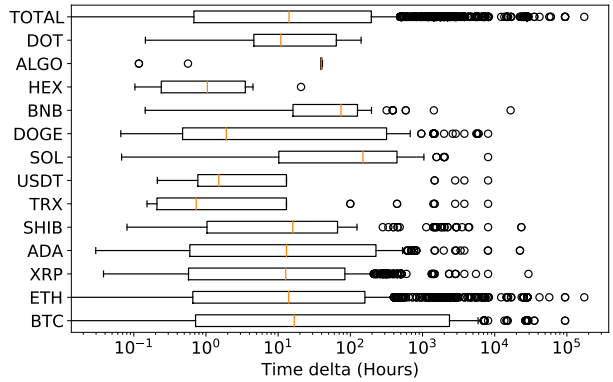

Fig. 6: *Delta between domain registration and capturing of a website by CryptoScamTracker.*

At the same time, CryptoScamTracker did discover domains used for giveaways that were significant outliers in terms of their creation date. Namely, we discovered 21 (0.54%) domains that were registered more than 10,000 hours before they were weaponized for cryptocurrency scam activities (i.e. more than a year before they were announced in CT logs and captured by CryptoScamTracker). For some of these domains, we conclude that they belong to websites that were compromised then abused for hosting scams. The earliest registration year for a giveaway scam domain was 2002, six years before Satoshi Nakamoto's paper describing Bitcoin [60]. Two domains were registered in 2015, and 11 more domains were registered between 2019 and 2020.

To better understand the reason behind these large deltas, we manually investigated some of these outliers. The domain `bigwalt.com` was registered in early 2000s (originally used to advertise a book from an author with the nickname "Big Walt") and only recently hosted a giveaway scam on the sub-domain `coinmarketcap.bigwalt.com`. Given the lack of relationship between this domain name and cryptocurrency keywords, we suspect that this domain was used mostly due to its long lifetime that imparts residual trust and can therefore evade DNS-abuse systems that penalize recently-registered domain names [53]. CryptoScamTracker identified multiple URLs with the same "coinmarketcap" subdomain which could be an indication that they are all operated by the same scammer.

Other outliers are `coin2x.me` which was registered in 2017, and `doublebitcoinfree.com` which was registered in 2018. Moreover, we found two cryptocurrency scam websites hosted on the same domain, belonging to a educational institution specializing in emergency medicine training. The cryptocurrency scam was situated on a subdomain and lasted for one week, from March 4 to March 11, 2022.

Limited coverage of domain blocklists: Modern browsers attempt to protect their users through their use of one or more blocklists (such as Google Safe Browsing). These blocklists will warn users who somehow land on a malicious page and make it difficult for them to proceed, unless they are intent on doing so. The strength of these blocklists is their attack-agnostic nature, i.e., the browser can warn users of a malicious page regardless of the type of malicious content (e.g. phishing vs. tech-support scams vs. cryptocurrency giveaways). On the other hand, these lists are by definition incomplete and cannot stop users from interacting with malicious content, until that content is added to the blocklist.

TABLE VII: *Scammer wallet transactions for the four most abused cryptocurrencies (transactions recorded on July 1, 2022). The minimum and maximum USD value is estimated using the lowest and highest price of each cryptocurrency in the experiment period.*

Cryptocurrency	#Unique Wallets	Largest Wallet Size	Average Wallet Size	Median Wallet Size	Total Cryptocurrency Amount	Total USD Value (Min. – Max)
Bitcoin (BTC)	860	204.95	1.09	0	940.07	$17.8M– $44.9M
Ethereum (ETH)	683	258.54	6.34	0.89	4,330.26	$4.31M– $16.6M
Cardano (ADA)	215	240,000.00	9,962.22	0	2,141,876.52	$1.3M– $3.43M
Ripple (XRP)	318	1,403,803.5	18,237.72	0	5,799,593.93	$1.74M– $5.08M

To assess whether popular blocklists are sensitive to cryptocurrency scam websites, we used the VirusTotal API to query all of the domains that CryptoScamTracker identified through our experiment. VirusTotal represents a best-case scenario since it integrates more than 90 different antivirus tools and blocklists. Following standard VirusTotal-labeling practices, we define a domain as malicious/suspicious if at least 3 of the 90 AV tools that VT integrates label it as such. In total, out of the 3,610 domains discovered by CryptoScamTracker, only 16.75% domains appeared in VT's blocklists. This low coverage underlines the recency of cryptocurrency giveaway scams where existing tools have not had enough time to adapt their scanning infrastructure to be able to detect them. Similar to technical support scams, giveaway scams depart from the traditional mold of malicious webpages (i.e. no HTML forms to collect user input and no offered downloads) which suggests that existing malware-detection systems are highly unlikely to detect these pages as malicious, unless they are explicitly modified to account for them.

IV. Transaction Analysis

So far, we described the infrastructure supporting cryptocurrency giveaway scams in terms of their domain names, hosting providers, and content that they use to convince users to send them funds. The techniques behind these analyses are common regardless of online malicious content and have been used in the past in the context of quantifying phishing [46], [65], domain squatting [58], [77], technical support scams [57], [73], [78], and malware C&C servers [25], [38], [52].

A key differentiator of this work compared to the aforementioned prior work is its financial component. Prior work had to make a number of assumptions in order to estimate the cost of a specific cybercrime to the community and the amount of funds that users lost due to the stealing of their private information. Contrastingly, in the context of cryptocurrency giveaway scams, the scammers' wallets are publicly accessible on their respective blockchains with an accurate ledger of all past incoming and outgoing transactions. As such, we do not have to estimate how much money was stolen or how much value was lost. We can merely sum the total transactions and arrive at a precise amount of cryptocurrencies stolen (and their corresponding dollar value).

A. Transaction Overview

As we discussed in Section III, we discovered that the four most popular cryptocurrencies attract more than 80% of the scam websites captured by CryptoScamTracker. In light of this high concentration of scams, we focus our transaction analysis on these four popular cryptocurrencies, namely Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), and Cardano (ADA). To extract the transactions of each scam wallet, we take advantage of the public nature of the blockchains supporting these cryptocurrencies and utilize publicly available API services from various cryptocurrency tracker platforms to query the transactions of each wallet address [14], [15], [24], [82]. We recorded all transactions of each wallet and summed the incoming transactions where the transaction recipient is the scammer's wallet address.

Table VII shows the results of this process. Despite having attracted fewer scams compared to Ethereum, Bitcoin is the cryptocurrency where scammers stole the most funds from users, with 860 scammer wallets having received a total of 940.07 BTC which translates to a total of $17.8M–$44.9M (based on the minimum and maximum USD price of Bitcoin during our study) stolen from victim users. For the remaining three cryptocurrencies (ETH, ADA, and XRP) scammers have stolen orders of magnitude more coins from their victims which however translate to smaller dollar amounts given the lower market caps of these cryptocurrencies. In total, just for the scam domains that CryptoScamTracker identified in the 6-month period of our study, using the minimum and maximum market rates during our study, scammers stole a total of $24.9M–$69.9M across all cryptocurrencies. Our results highlight how profitable these scams can be, despite the low adoption rate of cryptocurrencies.

Even though the most successful scammers can steal the equivalent of millions of dollars from just one giveaway scam (e.g. for Ethereum, the most successful scammer received a total of 258.54 Ethereum, translating to 990K dollars using the maximum Ethereum price during our study) not all scammers are as successful. As Table VII shows, the median transactions of all cryptocurrencies except Ethereum is zero, meaning that 50% of the wallets never received a single incoming transaction. This finding highlights the importance of driving a sufficient amount of traffic to the scammer's giveaway page under some plausible context. For example, we anticipate that compromising a YouTube channel with hundreds of thousands of subscribers and using it to drive traffic to a giveaway page will result in more funds stolen, compared to merely tweeting malicious links using a low-quality social media account. This finding highlights the importance of early detection and mitigation by large platforms which can stifle the traffic that a scammer's website receives, regardless of how long it stays online. Ethereum is the only cryptocurrency where scammers appear to be more successful on average (with a median stolen amount of 0.89 Ethereum).

B. Case Studies

Highest earning wallet address: The highest-earning wallet address recorded by CryptoScamTracker accumulated a total of 204.95 BTC, listed on a single website discovered

TABLE VIII: *Reused wallet address across targeted cryptocurrencies.*

Cryptocurrency	Reused Wallets	Max websites per wallet	Average income	Median income
BTC	79	20	0.5222	0.0247
ETH	76	13	7.5963	2.7084
ADA	24	9	10,311.07	6,815.31
XRP	35	106	63,034.81	5,037.71

by CryptoScamTracker. Yet, by inspecting the timing of the incoming transactions and correlating them with the website lifetime as recorded by CryptoScamTracker, we can conclude that the same wallet address must have been listed in additional giveaway domains. Specifically, we observe incoming transactions even after the CryptoScamTracker-discovered websites listing that specific wallet were no longer accessible. The domain names associated with these specific giveaway scams betray that this scammer used them to collect multiple cryptocurrency scams. The website listing this address contained the phrase `strategy-double.com` in its domain name and advertised multiple concurrent giveaways for BTC and ETH. Through web searches, we found additional structurally-similar websites, such as `strategy-gift.com`, advertising the same giveaway scam.

Reuse of wallet addresses: Even though the large namespace of wallet addresses allows users to generate a virtually unlimited number of wallet addresses, we discovered that some scammers reused wallet addresses across giveaway websites. Table VIII presents statistics on the levels of reuse across each cryptocurrency. Out of a total 2,266 cryptocurrency wallet addresses, there are 214 (9.44%) wallet addresses that CryptoScamTracker encountered on more than one cryptocurrency scam domains. The most widely re-used wallet address is an address of Ripple (XRP), which was listed on 106 different cryptocurrency websites. In terms of profits, we observe that reused wallet addresses attract a larger number of transactions (and total coins) across both average and median numbers. Given that address reuse makes forensic analysis and campaign clustering easier, we conclude that reuse is happening mostly as a matter of convenience allowing the attacker to automatically deploy multiple different giveaway scams without the need to manage multiple pairs of public and private cryptocurrency keys.

Fund recovery scams targeting scam victims: Several high-earning wallet addresses are listed in crowdsourced websites as "giveaway scams." Interestingly, by reading through the comments on these sites, we observed the attempt of scammers to re-victimize the victims of the initial scam. Specifically, we discovered comments left by users who claimed that a certain person or service was able to recover their stolen funds, leaving behind an email or WhatsApp number for other users to contact. Funds can only be recovered if someone obtains the private key of a scammer's wallet. Even if scammers would be hosting their stolen funds on online exchanges, the authorities would still need to be involved in order to freeze those assets. Therefore, these posts are clearly attempts by scammers (possibly different than the original scammers) to take advantage of victim users and steal additional funds from them.

Victims can be scammed more than once: One could reasonably expect that users who send money to scammers because of a giveaway scam, eventually realize that they were scammed and then never fall victim to these scams again. To understand if this holds true, we first investigate whether the same victims (as identified by the wallet addresses sending funds to scammers) send funds to more than one scammer wallet. We discovered 128 ETH and 52 XRP wallets that initiated multiple transactions to different scam wallets. Thankfully, through further analysis, we concluded that most wallet addresses belongs to online exchanges (such as Coinbase), where multiple victims can share the same outgoing address.

We also investigated whether there exist victims who send multiple transactions to the *same* wallet address. There, we unfortunately discovered 595 victims who initiated multiple XRP transactions to same scammer Ripple wallet, and 255 victims who initiated multiple ETH transactions to the same Ethereum wallet. Among them we find wallet addresses that, based on their activity level and total funds held, clearly belong to individual users (as opposed to online exchanges). For instance, one wallet address starting with "r9gJXGLi" first sent 1,033.45 XRP to the scammer's wallet and two hours later sent another 1,001.00 XRP to the same address. The only reasonable explanation for this behavior is that some users conclude that the absence of received funds must be due to some sort of error. These users can then decide to repeat their transaction, perhaps not realizing that their first transaction was successfully completed and they have now doubled their losses.

Custodial vs. Non-Custodial Wallets: One of the dimensions of cryptocurrency wallets is whether they are *custodial* or *non-custodial*. Custodial wallets are wallets that are controlled by online exchanges (such as Coinbase and Gemini) where users do not have direct access, neither to the private keys of their wallets, nor to the cryptocurrencies contained within them. Conversely, non-custodial wallets enable users to create and manage their own private keys, either in software or in hardware (known as cold-storage wallets). Custodial wallets are the easiest to setup and use, with no special requirements from users other than remembering the credentials to the exchange site. Conversely, non-custodial wallets are considered to be more secure since the assets cannot be seized or stolen, unless someone somehow obtains the user's private keys/seed phrase.

Given the technical expertise and extra steps required to manage non-custodial wallets, one may reason that the victims of giveaway scams are more likely to be using custodial wallets. Unfortunately, from the point of view of a blockchain, there is no definitive way of knowing whether a wallet address corresponds to a custodial vs. a non-custodial wallet. As an approximation, we use the number of transactions in a user's (i.e. giveaway victim's) wallet to differentiate between custodial and non-custodial wallets. This approximation hinges on the observation that, when users of exchanges send funds to other wallets, the source address of that transfer belongs to the exchange, as opposed to the individual user. This allows the exchange to pool user-transactions together and pay fewer transaction fees. As such, wallet addresses with a large number of transactions are more likely to be operated by an exchange, as opposed to an overly active individual user.

Figure 7 shows the number of transactions in all victim wallets. We exclude Ripple (XRP) from this analysis due to a limitation in the publicly available APIs that make it difficult to obtain the total number of transactions for a given Ripple wallet address. Overall, we identified a total of 15,108 victim wallets

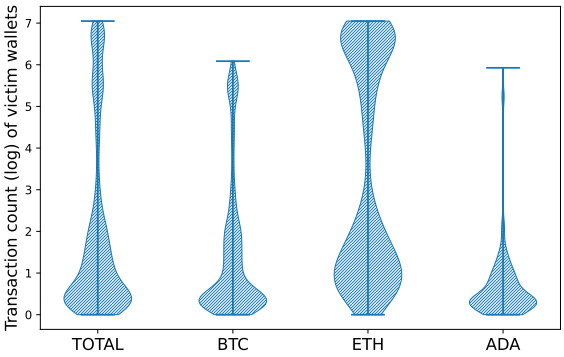

Fig. 7: *Transaction distribution of victims' wallets.*

having sent funds to scammer wallets, with 8,418 Bitcoin wallets, 4,963 Ethereum wallets, and 1,727 Cardano wallets. With the exception of Ethereum, we can observe that the vast majority of victims of BTC and ADA giveaway scams have conducted fewer than a hundred transactions, suggesting that they are using individual, non-custodial wallets. From a security point of view, this shows that even if large exchanges integrate with wallet-address blocklists, they would only protect a small minority of victims. This kind of integration would need to move into the wallet software that the users of non-custodial wallets are using.

Ethereum is the clear outlier, both in terms of the average number of transactions as well as the total number of transactions of the top half of wallets. One possible explanation is that Ethereum was the first cryptocurrency to support smart contracts and therefore NFTs and DeFi applications. This means that more users have created accounts on large exchanges and are participating in larger volumes of transactions. In this case, integrating these platforms with blocklists *does* have the potential to protect users, assuming that platforms are willing to take the risk of either denying customer transactions, or warning them before they allow them to proceed.

Lastly, we investigate the dates of the first transactions in the wallets of ETH and ADA victims. This date is the closest approximation possible to a wallet-creation date and can be used as a proxy of a user's experience with cryptocurrencies (older wallets belong to users who have involved in cryptocurrencies for multiple years). There, we find that 85.37% of ETH users and 94.43% of ADA users had their first transaction in 2021 and 2022. This is another experimental confirmation that the users who are the most vulnerable to these scams are the ones with the least experience.

CryptoScamTracker vs. Crowdsourcing: To understand the overlap between the scams that CryptoScamTracker can automatically discover and those that are voluntarily reported by users, we compared our dataset against CryptoscamDB [2] and Bitcoinabuse [3], two popular crowdsourced databases reporting the wallet addresses used in past scams. CryptoscamDB includes reports since 2017 and lists (as of July 2022) 4,478 previously reported wallet addresses. Similarly, Bitcoinabuse includes details on 288,183 previously reported wallet addresses, going as far back as May 2017. These crowdsourced databases contain reports related to a wide range of crypto-related unwanted activity, including giveaway scams, extortion, cold calls, fake exchanges, and ransomware.

We looked up the 2,266 wallet addresses captured by CryptoScamTracker in these two databases. We find

TABLE IX: *Amount of funds requested in scam pages. Average Low/Average High communicate the typical minimum/maximum amount that giveaway pages request.*

Cryptocurrency Type	Average Low	Average High	Minimum funds asked in USD
BTC	0.1143	52.91	$3,356–$7,718
ETH	0.7631	497.05	$556–$3,669
ADA	2,453.59	982,863.5	$429–$7,275
XRP	3,484.28	944,969.8	$769–$6,404

that, despite the longer data-collection horizons of these two crowdsourced databases, only 8 (0.35%) of the wallet addresses in our dataset appeared in CryptoScamDB, and 300 (14.45%) of the wallet addresses appeared in Bitcoinabuse. By focusing on the report timestamps of BitcoinAbuse, we observe that even for that small overlap, 50% of the addresses were identified by CryptoScamTracker at least 21 hours before they were reported by users. Overall, this low overlap highlights the need to supplement crowdsourced databases with data coming from automated scam-discovery tools, such as, CryptoScamTracker.

Range of requested cryptocurrency amounts: We also present a common pattern in scam web pages, where scammers often provide a range of cryptocurrency amounts that they will double, for example, 0.5 - 500 ETH. We believe this range is set up to prevent users from testing the "event" with small amounts of cryptocurrencies (e.g. before sending a large amount, users may send the equivalent of $1 to see whether they will get $2 back). We analyze our entire corpus of pages and report on the minimum and maximum range, as well as equivalent USD in Table IX. We use the same methodology as in Section IV-A involving the highest and lowest exchange rates of cryptocurrencies during the period of our study. For most cryptocurrencies, scammers asks for a minimum of approximately $500 relying on round-number quantities, such as 1.0 ETH, 3,000 ADA or 5,000 XRP. BTC is an exception with scammers requesting a minimum of approximately 3,000 USD (0.1 BTC) due to its large exchange rate. This social-engineering technique (visible in our aforementioned video demo of a real giveaway scam [4]) is unique to cryptocurrency giveaway scams, where victims essentially "choose" how much money they will lose.

Most prolific scammers: Since there are multiple indications that seemingly different cryptocurrency giveaway websites are in fact operated by the same scammer(s), in this section, we use deterministic identifiers to cluster scams into campaigns. To identify connected components which are representative of scam campaigns, we merge the domains whose WHOIS information listed the same email addresses (excluding common abuse-reporting email addresses) as well as those who shared the same cryptocurrency wallet address. The common email addresses help us group websites that present different wallet addresses, whereas common wallet addresses help us group scams whose domains were registered under different email addresses.

Table X presents the ten largest scam campaigns in our dataset. These campaigns consist of 3,586 web pages, which covered 35.58% websites in our dataset. Most of these prolific scammers targeted multiple different cryptocurrencies, ranging from popular cryptocurrencies like Bitcoin and Ethereum to more recent ones, such as, Doge or Solana. These results show that the most successful scammers are not ideologically tied

TABLE X: Top 10 cryptocurrency scam campaigns. Websites are connected to same campaign through shared emails and wallet addresses.

Campaign ID	# Sites	# Domains Involved	# Emails	# Wallet Addresses	# Cryptocurrencies Involved	Cryptocurrencies
1	1,621	3	1	2	2	ETH,BTC
2	1,360	835	46	395	10	BNB,SHIB,ADA,BTC,XRP,ETH,HEX,SOL,DOT,DOGE
3	155	69	6	21	7	BNB,SHIB,ADA,BTC,ETH,SOL,DOGE
4	116	19	1	30	6	BNB,ADA,BTC,XRP,ETH,DOGE
5	71	36	1	9	7	BNB,SHIB,ADA,BTC,XRP,ETH,DOGE
6	69	35	2	18	5	BNB,ADA,BTC,XRP,ETH,DOGE
7	63	16	4	11	3	ETH,BTC,XRP
8	45	21	2	11	3	ETH,BTC,BNB
9	45	15	2	8	5	BNB,ADA,BTC,XRP,ETH,DOGE
10	41	30	5	21	6	BNB,SHIB,ADA,BTC,XRP,ETH
(Total)	3,586	1,079	70	526	-	-

to any specific cryptocurrency. They can adjust their scam templates to match any cryptocurrency of interest and most likely rely on automation to deploy their content on hundreds of domains, pivoting from cryptocurrency to cryptocurrency as necessary and victimizing as many users as possible.

V. Discussion

Ethical Considerations. In this paper, we do not interact with end users in any way. Our one ethical consideration was whether to report the cryptocurrency giveaway domains as CryptoScamTracker is finding them, or not. While CryptoScamTracker autonomously crawls domains every day, our labeling is done asynchronously. We labeled the CryptoScamTracker matches approximately once per week (for the six months of our study). Therefore, by the time we marked an entry as a true positive, that site would typically be offline, given our lifetime calculations in Section III.

Separate from our labeling frequency (which reduces the utility of reporting) we chose not to tamper with the ecosystem while studying it, to avoid measuring artifacts of our own intervention. Had we intervened with giveaway scams, it would have been difficult to disentangle the organic evolution of this scam over the last six months, from the results of our own actions. We will be making available all of the data that CryptoScamTracker collected during our six-month analysis. We hope that this data can be of use to multiple stakeholders in the web ecosystem, from benign hosting providers who can identify that attackers are abusing them, to the operators of security crawlers who can add additional detection logic to their tools.

Limitations. Like all real-world systems, our proposed CryptoScamTracker has certain limitations regarding the discovery of cryptocurrency-giveaway scams. These limitations revolve around the i) the construction of domain names, ii) the content of the visited HTML pages, and iii) explicit detection-evasion attempts by attackers.

Given the large number of Certificate Transparency announcements, CryptoScamTracker uses a specific set of cryptocurrency-related keywords (listed in Table XI) to select which domains should be crawled. If an attacker avoids using any of these keywords, our CryptoScamTracker prototype will not crawl their website and will therefore not flag them as a giveaway scam. Similarly, if attackers set up giveaway scam pages that somehow avoid all words related to cryptocurrencies and giveaways, CryptoScamTracker may crawl that webpage but will not flag it for manual analysis. In both cases, we argue that the lists used by CryptoScamTracker can expand as necessary, whenever analysts detect that a given giveaway campaign evades the current set of words. Expanding the list of domain-level and content-level keywords will require additional computational and storage resources (for crawling and storing a larger number of webpages) and a potentially increased workload for the manual analysts who check CryptoScamTracker's reports for true and false positives.

In terms of evasions, it is well known that attackers engage in crawler evasion to increase the lifetime of their malicious pages and domains [40], [80], [83], [84]. While CryptoScamTracker does take a number of steps to avoid being evaded (e.g. using multiple user-agent headers and a combination of both a real browser as well as an HTTP-requests library) there are additional evasion techniques (e.g. waiting for users to move their mouse before revealing their content, or accepting web notifications [76]) which CryptoScamTracker does not currently handle. When CryptoScamTracker is operationalized, additional anti-cloaking capabilities can be added to it (e.g. user interaction, proxy IP addresses in residential networks, mobile and desktop crawlers, etc.) without interfering with the rest of its detection logic.

Lastly, we note that CryptoScamTracker is meant to be used with a human in the loop, i.e., an analyst that can verify true positives in CryptoScamTracker's findings, before acting upon them. Our tool does produce a small number of false positives (approximately 4%) since there exist benign webpages that happen to use the same phrases as giveaway scams, such as, gambling websites that use cryptocurrencies and crypto sites asking for donations. It is possible that supervised machine learning (using the thousands of positive examples that CryptoScamTracker has already collected) will reduce or altogether eliminate the need for manual verification of giveaway scams. We leave this investigation for future work.

VI. Related Work

To the best of our knowledge this paper is the first one to propose a tool for automatically discovering giveaway scams. The work that is the most related to ours is the advanced-fee scam analysis of Phillips and Wilder [67] as well as Bartoletti et al. [11] who presented a taxonomy of cryptocurrency scams and,

among others, looked at giveaway scams. The authors of both studies, however, limited themselves to scraping scams from existing crowdsourced websites, which, given the low overlap between the addresses that CryptoScamTracker discovered and these crowdsourced databases (Section IV-B), likely biases their findings and undercounts the size of the giveaway-scam ecosystem. Our proposed approach independently discovers giveaway scams and does not rely on blocklists and crowdsourced reports.

Taking a step back, giveaway scams belong in a long line of past and present social-engineering-based attacks that users are regularly exposed to. In this section, we provide a brief overview of other types of social-engineering attacks and draw appropriate parallels between past analyses and our work. Phishing represents the prototypical social-engineering attack where users are lured to malicious sites through the use of spam emails, instant messaging, and social networks. These malicious sites aim to trick users into divulging their credentials to sensitive websites (including email and banking) by impersonating their target sites. Given the importance and sustained success of phishing against users [21], [41], [65], phishing has attracted a wide range of research spanning multiple decades proposing systems for detecting phishing sites in the wild [5], [6], [37], [55] and helping users differentiate between authoritative and phishing sites [16], [20]. In some of the recently-proposed phishing-detection systems, researchers relied on Certificate Transparency logs to identify domain names that make suspicious use of popular trademarks [26], [46], [70], [72]. Similarly, in our work, we also relied on Certificate Transparency logs to discover domain names that included keywords associated with cryptocurrencies and automatically crawl them.

In addition to impersonating known and trusted entities, scammers are constantly devising new scenarios with believable-enough facades that convince users to provide their personal and financial information. Among others, scammers use fake surveys to collect PII from users who believe they are about to receive a reward for their participation in a survey [19], [45], as well as scams taking advantage of emergencies and natural disasters (including the recent COVID-19 pandemic [13], [35]) where users believe they are sending funds to affected populations, or are procuring goods and services that are in short supply.

Next to traditional phishing, there have been variations of social-engineering-based attacks where a malicious website impersonated a trustworthy entity to make users behave in an insecure manner. Scareware was the first popular variation of traditional phishing where websites impersonated globally-recognizable software names (like "Microsoft" and "Symantec") and pretended to scan the computers of the visiting users [69], [75]. These sites would invariably find "issues" with the machines of users, and asked users to download their software to correct the discovered problems. The downloaded malware could do anything on the user's machine, from trying to convince users to pay a software-licensing fee to repair the discovered issues, to stealing user data [25], [38], [52] and installing ransomware [43], [44].

Due to a number of interventions by browser vendors and security companies (including the treating of all unknown downloadable executables as suspicious), attackers pivoted to a variation of this attack which became known as technical-support scams. In a technical support scam, the malicious site still impersonates a popular software company and discovers "issues" on the user's machine but instructs the user to call a phone number in order to receive technical support [57], [73], [78]. Scammers then use remote-administration tools to connect to their victims' machines and then use fake diagnostic procedures to convince users to buy their support services.

Technical support scams are related to the cryptocurrency giveaway scams we investigated in this paper in that the scam crosses communication and technology mediums. In technical support scams, half of the attack is conducted over the web and the rest is conducted over the phone. In cryptocurrency giveaway scams, once users are convinced to participate in these "giveaways" they then use different technologies and platforms (such as scanning the scam QR code through their mobile software wallets or copy-pasting the scammers' wallet address in installed wallet software and online exchanges) to transfer funds to the scammers. These types of malicious pages deviate significantly from the traditional mold of social-engineering sites (they offer nothing to download and do not host any forms where a user is asked to provide information) and have proved to be hard to detect by existing phishing-detection systems. We anticipate that as users increase the number of technologies and platforms that they use in their day-to-day lives (e.g. through the ever-increasing adoption of IoT devices) that these types of cross-platform attacks will increase in frequency and in magnitude.

VII. Conclusion

In this paper, we presented the first analysis of cryptocurrency giveaway scams in the wild where scammers exploit the lack of technical expertise of users as well as the average person's desire for "get-rich-quick" solutions to steal funds from unsuspecting users.

Over a period of six months, our proposed CryptoScamTracker captured a total of 10,079 websites, with a daily average of 55.7 new websites hosted on specific hosting providers that are otherwise unpopular on the general web. We demonstrated the poor performance of existing blocklists in terms of protecting users against giveaway scams (less than 17% of the websites and 15% of wallet addresses discovered by CryptoScamTracker were available in large commercial and crowdsourced databases) and documented the reliance of scammers on third-party real-time chat services and analytics, a reliance that could be used against them in the future. In the final part of this paper, we took advantage of the public blockchains of the studied cryptocurrencies and calculated the exact amount of funds that scammers have stolen from victim users, identifying the theft of tens of millions of dollars from users.

We hope that this study will be the start of a discussion on how to best protect the users of cryptocurrencies, given the inherent decentralized nature of this technology and the expectation that there should be no trusted third parties who get to dictate transaction policies for users.

Acknowledgements: We thank the reviewers for their helpful comments. This work was supported by the Office of Naval Research (ONR) under grant N00014-20-1-2720 as well as by the National Science Foundation (NSF) under grants CNS-1813974, CNS-1941617, CNS-2126654, and CNS-2211575.

Availability. One of the main contributions of this paper is the curation of a dataset with thousands of websites, domain

names, and wallet addresses operated by cryptocurrency giveaway scammers along with their transactions. To encourage more research in this new space, we are making this dataset publicly available: https://double-and-nothing.github.io/

REFERENCES

[1] "Millions of dollars' worth of ada stolen by crypto giveaway scams every month, says charles hoskinson," https://www.gfinityesports.com/cryptocurrency/charles-hoskinson-ada-crypto-giveaway-scams-millions-of-dollars-cardano/, 2021.

[2] " Scams: CryptoScamDB ," https://cryptoscamdb.org/scams, 2022.

[3] "Bitcoin Abuse Database," https://www.bitcoinabuse.com/, 2022.

[4] "CryptoScamTracker: Video demo of cryptocurrency giveaway scam," https://vimeo.com/775187519, 2022.

[5] S. Abdelnabi, K. Krombholz, and M. Fritz, "Visualphishnet: Zero-day phishing website detection by visual similarity," in *Proceedings of the 2020 ACM SIGSAC conference on computer and communications security*, 2020, pp. 1681–1698.

[6] M. A. Adebowale, K. T. Lwin, E. Sanchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of images, frames and text," *Expert Systems with Applications*, vol. 115, pp. 300–313, 2019.

[7] S. Alrwais, X. Liao, X. Mi, P. Wang, X. Wang, F. Qian, R. Beyah, and D. McCoy, "Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 805–823.

[8] M. AlSabah, M. Nabeel, Y. Boshmaf, and E. Choo, "Content-agnostic detection of phishing domains using certificate transparency and passive dns," in *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses*, 2022, pp. 446–459.

[9] APWG, "Phishing Activity Trends Report:: Q4 2021," https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf.

[10] B. Barrett, "Security News This Week: A $320 Million Crypto Hack Sends the DeFi World Reeling," https://www.wired.com/story/wormhole-defi-hack-ransomware-security-news/, 2022.

[11] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency scams: analysis and perspectives," *IEEE Access*, vol. 9, pp. 148 353–148 373, 2021.

[12] J. Benson, "Gemini Client IRA Financial Hacked for $36M in Bitcoin and Ethereum: Report," https://decrypt.co/92950/gemini-client-ira-financial-hacked-36m-bitcoin-ethereum-report, 2022.

[13] M. Bitaab, H. Cho, A. Oest, P. Zhang, Z. Sun, R. Pourmohamad, D. Kim, T. Bao, R. Wang, Y. Shoshitaishvili *et al.*, "Scam pandemic: How attackers exploit public fear through phishing," in *2020 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2020, pp. 1–10.

[14] Blockfrost, "Blockfrost explorer api," "https://blockfrost.io/".

[15] Blockstream, "Blockstream explorer api," "https://blockstream.info/".

[16] Y. Cao, W. Han, and Y. Le, "Anti-phishing based on automated individual white-list," in *Proceedings of the 4th ACM workshop on Digital identity management*, 2008, pp. 51–60.

[17] "Cardano.org : Home ," https://cardano.org/.

[18] C. Carpenter, "Katy man out of about $17K after his cryptocurrency account was hacked," https://abc13.com/coinbase-cryptocurrency-hacked-robbed/11530402/, 2022.

[19] J. W. Clark and D. McCoy, "There Are No Free iPads: An Analysis of Survey Scams as a Business." in *LEET*, 2013.

[20] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," in *Proceedings of the 2005 symposium on Usable privacy and security*, 2005, pp. 77–88.

[21] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[22] F. Erazo, "Researchers Spot New Cryptocurrency Stealing Malware Advertised Under a Subscription Model," https://news.bitcoin.com/researchers-spot-new-cryptocurrency-stealing-malware-advertised-under-a-subscription-model/, 2021.

[23] "Home : ethereum.org," https://ethereum.org/en/.

[24] Etherscan, "Etherscan api," "https://etherscan.io/".

[25] B. Farinholt, M. Rezaeirad, P. Pearce, H. Dharmdasani, H. Yin, S. Le Blond, D. McCoy, and K. Levchenko, "To catch a ratter: Monitoring the behavior of amateur darkcomet rat operators in the wild," in *IEEE Symposium on Security and Privacy (IEEE S&P)*, 2017, pp. 770–787.

[26] E. Fasllija, H. F. Enişer, and B. Prünster, "Phish-hook: Detecting phishing certificates using certificate transparency logs," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2019, pp. 320–334.

[27] E. Fletcher, "Cryptocurrency buzz drives record investment scam losses - federal trade commission," "https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses".

[28] S. Frenkel, N. Popper, K. Conger, and D. E. Sanger, "A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam," https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html, 2020.

[29] C. Fripp, "Warning: Scammers are sending out fake gadgets to steal your money," https://www.komando.com/amazon/fake-gadgets-to-steal-cryptocurrency/795248/, 2021.

[30] G. Georgiev, "Twitter 'Free ETH Giveaway' Scams Can Rake in $50K-100K Per Day," https://bitcoinist.com/twitter-free-eth-giveaway-scam-money/, 2018.

[31] G. Gomez, P. Moreno-Sanchez, and J. Caballero, "Watch your back: Identifying cybercrime financial relationships in bitcoin through back-and-forth exploration," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, p. 1291–1305.

[32] D. Goodin, "Really stupid "smart contract" bug let hackers steal $31 million in digital coin," https://arstechnica.com/information-technology/2021/12/hackers-drain-31-million-from-cryptocurrency-service-monox-finance/, 2021.

[33] L. A. Goodman, "Snowball sampling," *The annals of mathematical statistics*, pp. 148–170, 1961.

[34] L. Greenberg, "Couple's digital Coinbase account hacked, $24,000 stolen," https://www.fox35orlando.com/news/couples-digital-coinbase-account-hacked-24000-stolen, 2021.

[35] S. Hakak, W. Z. Khan, M. Imran, K.-K. R. Choo, and M. Shoaib, "Have you been a victim of covid-19-related cyber incidents? survey, taxonomy, and mitigation strategies," *Ieee Access*, vol. 8, pp. 124 134–124 144, 2020.

[36] J. Hall, "Bitcoin stealing malware: Bitter reminder for crypto users to stay vigilant," https://cointelegraph.com/news/bitcoin-stealing-malware-bitter-reminder-for-crypto-users-to-stay-vigilant, 2022.

[37] S. Hao, A. Kantchelian, B. Miller, V. Paxson, and N. Feamster, "Predator: proactive recognition and elimination of domain abuse at time-of-registration," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1568–1579.

[38] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the underground economy: A case-study of keyloggers and dropzones," in *European Symposium on Research in Computer Security*. Springer, 2009, pp. 1–18.

[39] S. Huff, "Malware disguised as cryptocurrency wallets used to steal from iOS and Android users," https://www.androidpolice.com/malware-cryptocurrency-wallets-steal-from-ios-and-android-users/, 2022.

[40] L. Invernizzi, K. Thomas, A. Kapravelos, O. Comanescu, J.-M. Picod, and E. Bursztein, "Cloak of visibility: Detecting when machines browse a different web," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

[41] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006.

[42] P. Karter, "Cardano: "We will never give away ADA"," https://en.cryptonomist.ch/2021/09/20/cardano-never-give-away-ada/, 2021.

[43] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," in *25th USENIX Security Symposium*, 2016, pp. 757–772.

[44] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware

attacks," in *International conference on detection of intrusions and malware, and vulnerability assessment*. Springer, 2015, pp. 3–24.

[45] A. Kharraz, W. Robertson, and E. Kirda, "Surveylance: Automatically detecting online survey scams," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 70–86.

[46] B. Kondracki, B. Amin Azad, O. Starov, and N. Nikiforakis, "Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits," in *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 2021.

[47] M. Konte, R. Perdisci, and N. Feamster, "Aswatch: An as reputation system to expose bulletproof hosting ases," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 2015, pp. 625–638.

[48] "Beware of crypto giveaway scams," https://support.kraken.com/hc/en-us/articles/360057159411-Beware-of-crypto-giveaway-scams, 2021.

[49] N. Kshetri and J. Voas, "Do crypto-currencies fuel ransomware?" *IT professional*, vol. 19, no. 5, pp. 11–15, 2017.

[50] LEDGER, "Scam warning on second hand Ledger devices," https://www.ledger.com/scam-second-hand-ledger-device, 2018.

[51] N. Leontiadis and N. Christin, "Empirically measuring whois misuse," in *European Symposium on Research in Computer Security*, 2014, pp. 19–36.

[52] C. Lever, P. Kotzias, D. Balzarotti, J. Caballero, and M. Antonakakis, "A lustrum of malware network communication: Evolution and insights," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 788–804.

[53] C. Lever, R. Walls, Y. Nadji, D. Dagon, P. McDaniel, and M. Antonakakis, "Domain-z: 28 registrations later measuring the exploitation of residual trust in domains," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 691–706.

[54] "Majestic million," https://majestic.com/reports/majestic-million.

[55] E. Medvet, E. Kirda, and C. Kruegel, "Visual-similarity-based phishing detection," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, 2008, pp. 1–6.

[56] T. Meskauskas, "Do not participate in the Cardano fake giveaway," https://www.pcrisk.com/removal-guides/20380-cardano-giveaway-scam, 2021.

[57] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial One for Scam: A Large-Scale Analysis of Technical Support Scams," in *Proceedings of the 24th Network and Distributed System Security Symposium (NDSS)*, 2017.

[58] T. Moore and B. Edelman, "Measuring the perpetrators and funders of typosquatting," in *International Conference on Financial Cryptography and Data Security*, 2010, pp. 175–191.

[59] M. Musch and M. Johns, "U can't debug this: Detecting javascript anti-debugging techniques in the wild," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 2935–2950.

[60] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[61] Namcios, "Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets," https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17, 2021.

[62] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale," in *Proceedings of the 34th annual computer security applications conference*, 2018, pp. 653–663.

[63] A. Noroozian, J. Koenders, E. Van Veldhuizen, C. H. Ganan, S. Alrwais, D. McCoy, and M. Van Eeten, "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting," in *28th USENIX Security Symposium (USENIX Security)*, 2019, pp. 1341–1356.

[64] A. Oest, Y. Safei, A. Doupé, G.-J. Ahn, B. Wardman, and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2018, pp. 1–12.

[65] A. Oest, P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupé, and G.-J. Ahn, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," in *29th USENIX Security Symposium*, 2020.

[66] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, "Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem," in *Proceedings of the 1st ACM conference on advances in financial technologies*, 2019, pp. 76–88.

[67] R. Phillips and H. Wilder, "Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–8.

[68] Z. Rafique, T. V. Goethem, W. Joosen, C. Huygens, and N. Nikiforakis, "It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services," in *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS)*, 2016.

[69] M. A. Rajab, L. Ballard, P. Mavrommatis, N. Provos, and X. Zhao, "The nocebo effect on the web: an analysis of fake anti-virus distribution," in *USENIX workshop on large-scale exploits and emergent threats (LEET)*, 2010.

[70] R. Roberts, Y. Goldschlag, R. Walter, T. Chung, A. Mislove, and D. Levin, "You are who you appear to be: A longitudinal study of domain impersonation in tls certificates," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2489–2504.

[71] Satnam Narang, "Millions Of Dollars' Worth Of ADA Stolen By Crypto Giveaway Scams Every Month, Says Charles Hoskinson," https://www.tenable.com/blog/fake-bitcoin-ethereum-dogecoin-cardano-ripple-and-shiba-inu-giveaways-proliferate-on-youtube, 2021.

[72] Q. Scheitle, O. Gasser, T. Nolte, J. Amann, L. Brent, G. Carle, R. Holz, T. C. Schmidt, and M. Wählisch, "The rise of certificate transparency and its implications on the internet ecosystem," in *Proceedings of the Internet Measurement Conference 2018*, 2018, pp. 343–349.

[73] B. Srinivasan, A. Kountouras, N. Miramirkhani, M. Alam, N. Nikiforakis, M. Antonakakis, and M. Ahamad, "Exposing Search and Advertisement Abuse Tactics and Infrastructure of Technical Support Scammers," in *Proceedings of the Web Conference (WWW)*, 2018.

[74] O. Starov, Y. Zhou, X. Zhang, N. Miramirkhani, and N. Nikiforakis, "Betrayed by Your Dashboard: Discovering Malicious Campaigns via Web Analytics," in *Proceedings of the Web Conference (WWW)*, 2018.

[75] B. Stone-Gross, R. Abman, R. A. Kemmerer, C. Kruegel, D. G. Steigerwald, and G. Vigna, "The underground economy of fake antivirus software," in *Proceedings of the 10th Workshop on Economics of Information Security (WEIS)*, 2011.

[76] K. Subramani, X. Yuan, O. Setayeshfar, P. Vadrevu, K. H. Lee, and R. Perdisci, "When push comes to ads: Measuring the rise of (malicious) push advertising," in *Proceedings of the ACM Internet Measurement Conference*, 2020.

[77] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The long "taile" of typosquatting domain names," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 191–206.

[78] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn, "SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2016.

[79] P. Vadrevu and R. Perdisci, "What you see is not what you get: Discovering and tracking social engineering attack campaigns," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 308–321.

[80] D. Y. Wang, S. Savage, and G. M. Voelker, "Cloak and dagger: dynamics of web search cloaking," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011.

[81] P. A. Watters, A. Herps, R. Layton, and S. McCombie, "Icann or icant: Is whois an enabler of cybercrime?" in *2013 Fourth Cybercrime and Trustworthy Computing Workshop*. IEEE, 2013, pp. 44–49.

[82] XRPScan, "Xrpscan api," "https://xrpscan.com/".

[83] P. Zhang, A. Oest, H. Cho, Z. Sun, R. Johnson, B. Wardman, S. Sarker, A. Kapravelos, T. Bao, R. Wang *et al.*, "Crawlphish: Large-scale analysis of client-side cloaking techniques in phishing," in *2021 IEEE Symposium on Security and Privacy (SP)*.

[84] P. Zhang, Z. Sun, S. Kyung, H. W. Behrens, Z. L. Basque, H. Cho, A. Oest, R. Wang, T. Bao, Y. Shoshitaishvili *et al.*, "I'm spartacus, no, i'm spartacus: Proactively protecting users from phishing by intentionally triggering cloaking behavior," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3165–3179.

APPENDIX

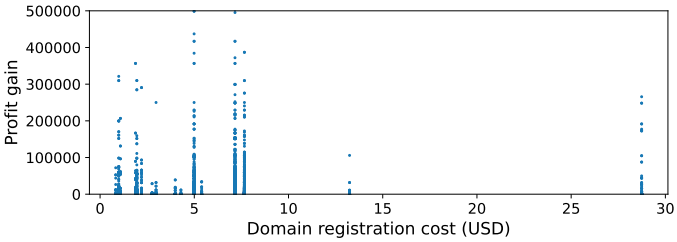

Fig. 8: *TLD registration cost versus profit gained by scammer. Each data point represents a single website. X axis represents the registration cost of the domain, Y axis represents funds stolen by the operator of that domain.*

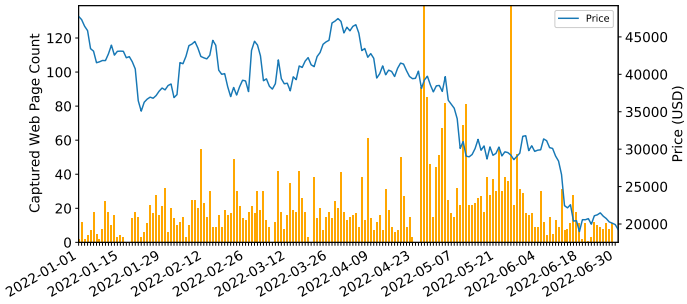

Fig. 9: *Traffic pattern for Bitcoin (BTC) with corresponding market price.*

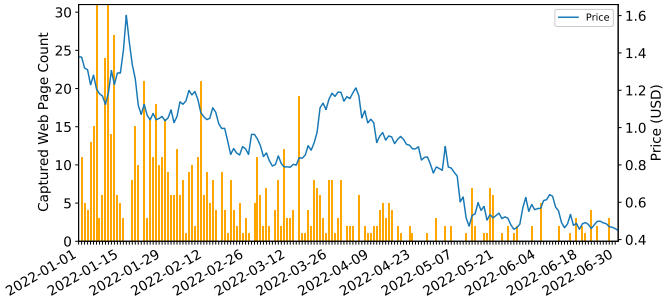

Fig. 10: *Traffic pattern for Cardano (ADA) with corresponding market price.*

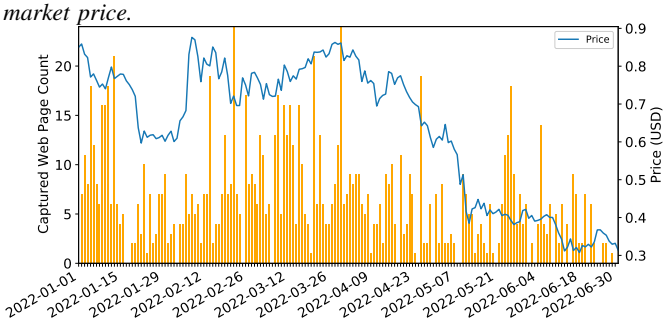

Fig. 11: *Traffic pattern for Ripple (XRP) with corresponding market price.*

TABLE XI: *Keywords used in CryptoScamTracker.*

Keyword Type	**Keywords**
URL Filter	eth(21.39%), kf(18.1%), event(11.61%), musk(9.36%), btc(9.29%), elon(8.78%), xrp(8.53%), give(8.27%), ada(6.4%), coin(6.34%), shib(5.86%), shiba(3.93%), ripple(3.3%), drop(3.22%), double(3.05%), get(2.54%), doge(1.68%), ethereum(1.5%), kefu(1.39%), bitcoin(1.31%), cardano(1.3%), solana(1.03%), vitalik(0.81%), claim(0.69%), binance(0.66%), hoskinson(0.51%), free(0.5%), charles(0.41%), algo(0.38%), usdt(0.34%), star(0.26%), polkadot(0.26%), hex(0.18%), dogecoin(0.09%), garling(0.07%), algorand(0.01%)
HTML Filter	giveaway(91.27%), participate(84.19%), send(82.91%), address(80.97%), rules(68.32%), crypto(54.03%), event(47.51%), bonus(35.89%), immediately(32.88%), hurry(9.62%)

TABLE XII: *Top 10 personal emails used in the registration of the scam domains identified by CryptoScamTracker.*

Email Address	Domain Count
dawd2ce*****@mail.ru	355
geras*****@yandex.ua	70
floyddje*****@gmail.com	50
buofnalfmachi*****@gmail.com	22
audriebalderama*****@gmail.com	19
robert-robinson*****@rambler.ru	17
lurlinedavirro*****@gmail.com	15
celiashebchu*****@gmail.com	13
aspdaxuaas*****@gmail.com	23
alfredpet*****@gmail.com	11

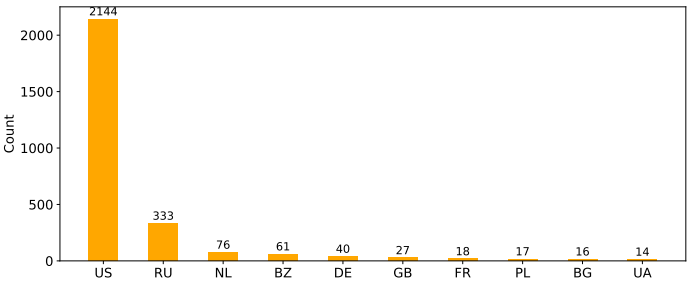

Fig. 12: *Top 10 hosting countries.*

TABLE XIII: *Top 20 Google search result for "cryptocurrency giveaway scam". All media articles are suggesting social media websites are the starting point for luring user into scams.*

Title	Source	Social Media Type	Key Paragraph
Crypto giveaway scams and how to spot them	Coinbase	Twitter/YouTube	Celebrity Twitter Impersonations:The response here is thanking Elon Musk and sharing an image that appears to be a tweet from Elon Musk about a Bitcoin and Ethereum giveaway being hosted by Tesla.
Beware of crypto giveaway scams	Kraken	Twitter/YouTube	Twitter and Youtube Giveaways:On Twitter, the fake giveaway account will sometimes have a blue verified check mark, making it appear more legitimate.
5 Social Media Crypto Scams to Avoid	Coindesk	Twitter/YouTube	In 2021, con artists used Tesla CEO Elon Musk's appearance on "Saturday Night Live" to bilk users out of $10 million through fake crypto giveaways on Twitter and YouTube.
Crypto giveaway scams continue to escalate	Helpnetsecurity	YouTube	Cryptocurrency giveaway scams are promoted on YouTube, Twitter, Facebook, and other social media platforms.
9 common cryptocurrency scams in 2023	TechTarget	Social media	Social media cryptocurrency giveaway scams:There are many fraudulent posts on social media outlets promising bitcoin giveaways. Some of these scams also include fake celebrity accounts promoting the giveaway to lure people in.
Fake cryptocurrency giveaway sites have tripled this year	BleepingComputer	YouTube/Twitch	Group-IB says that scammers abuse several video platforms to promote the fake giveaways in live streams with deepfakes of Elon Musk, Garlinghouse, Michael J. Saylor, and Cathie Wood. YouTube is first on the list, followed by Twitch.
Crypto giveaway scams continue to soar	Group-IB	Video stream	For the first time, the 24/7 Group-IB Computer Emergency Response Team (CERT-GIB) observed a sharp increase in the number of fraudulent YouTube streams "featuring" big names...
Raining bitcoin: Fake Nvidia giveaway	Kaspersky Daily	Twitter/YouTube	For example, scammers have tried to lure Twitter users to fake cryptocurrency handouts masquerading as Elon Musk, Bill Gates or Pavel Durov.
Bitcoiner loses coins worth a million in 'giveaway' scam—what are these scams all about?	CNBCTV	Twitter/YouTube	Most crypto scamsters find their victims through social media platforms such as Twitter.
Bitcoin Scams: How to Spot Them, Report Them, and Avoid Them	Investopedia	Social media	Moving down the sphere of influence, scammers also try to pose as celebrities, businesspeople, or cryptocurrency influencers.
Cryptocurrency Scams: How to Stay Safe	Morgan Stanley	Social media	These schemes often use social media posts to promote fake giveaways from actual companies or celebrities by either using forged screenshots or hacking into their accounts.
Money for nothing? Cryptocurrency "giveaways" net thousands for scammers	ProofPoint	Twitter	We frequently observed these tweets originating with fake accounts designed to generate clicks and retweets.
Avoid Scams - Bitcoin	Bitcoin.org	Social media	Unfortunately it's very easy for con-artists to create social media accounts and impersonate people.
Crypto Giveaway Scams Grow 5x in H1 2022	Cyware	Twitter/YouTube	In addition to leveraging fake YouTube streams, scammers have been found exploiting big names such as ...
YouTube Scammers Made $1.6 Million in Fake Crypto Giveaway	Bankinfosecurity	Twitter/YouTube	Researchers have found that a group of fraudsters made more than $1.6 million in 281 transactions in a massive scam using fake cryptocurrency giveaway YouTube streams attracting more than 165,000 viewers.
Scam Alert: Bitcoin / Cryptocurrency Giveaway Scams on Discord	TrendMicro	Discord	Scammers pretend to be from legitimate companies such as KFC, reaching out to users on Discord.
How to spot fake giveaways like the Ethereum giveaway	PCRisk	Twitter/YouTube/Discord	These scams are promoted via YouTube, Twitter, Discord, and other platforms.
Crypto scams: how to avoid them	RedPoints	Twitter/YouTube	Cryptocurrency giveaway scams are promoted on YouTube, Twitter, Facebook, and other social media platforms.
Bitcoin Investor Loses to Giveaway Scam, Here's Surprising Amount Lost	U Today	Twitter	There are also instances of verified Twitter accounts being hijacked and used to advertise fake giveaways intended to defraud token holders of their money.
YouTube Live Crypto Scams Made Nearly $9m in October	Infosecurity Magazine	YouTube	Tenable's researchers calculated that one subset of YouTube Live crypto scams unlawfully netted at least $8.9m in October alone.