A Sinister Fattening: Dissecting the Tales of Pig Butchering and other Cryptocurrency Scams

Marilyne Ordekian
Department of Computer Science
University College London
London, United Kingdom
marilyne.ordekian.21@ucl.ac.uk

Antonis Papasavva
Department of Security and Crime Science
University College London
London, United Kingdom
antonis.papasavva@ucl.ac.uk

Enrico Mariconti
Department of Security and Crime Science
University College London
London, United Kingdom
e.mariconti@ucl.ac.uk

Marie Vasek
Department of Computer Science
University College London
London, United Kingdom
m.vasek@ucl.ac.uk

***Abstract*—Cryptocurrency scams have risen in popularity with the mainstreaming of cryptocurrencies. People can fall victim to them because of their lack of knowledge, particularly when they gain a sense of trust in the ecosystem via a scammer. In this paper, we analyze 143 cryptocurrency scams across 11 different types mined from 133 scam narratives collated by the government of California. Most of these are pig-butchering scams (101) where attackers interact with their victims, gain their trust, and introduce them to a (scam) cryptocurrency investment opportunity. These scams vary in lure which indicates the wide variety of scams in our sample. Scammers often portray themselves as the gender opposite of their target; our results show greater financial gains using this approach. Furthermore, most scams end up communicating via messaging apps, regardless of how the scammer initially reached out to the victim. These cross-platform movements indicate a leap of faith and trust in the scammer needed to scam the victim. While many of these scams involved a fake cryptocurrency trading platform (124), we find some (33) using well-known and legitimate cryptocurrency exchanges to lend credibility to their schemes and avoid raising suspicion. To this end, we make recommendations for legitimate cryptocurrency platforms, regulators, and the community to deter and counter the prevalence of such scams.**

***Index Terms*—cryptocurrency fraud, cybercrime measurement**

I. Introduction

In the past decade, cryptocurrencies have dramatically risen in price while the market has increased in complexity. This has created a perfect storm for financial scams – the promise of riches has been realized by legitimate lucky users during times of skyrocketing prices while simultaneously, most people do not realize what they have been investing in, relying on trusted third parties for investment advice. In 2022, investment scams were the costliest scheme reported to the US Federal Bureau of Investigations [1]. Within these complaints, cryptocurrency investment fraud rose from $\$907m$ in 2021 to $\$2.57b$ in 2022.

Financial scams traditionally are aimed at an older demographic [2]. By adding a relationship component to the scam, so-called Pig Butchering scams introduce financial scams to a younger market as well as newcomers to the cryptocurrency industry writ large. This flavor of financial scam is rising to the level of the US Internal Revenue Service warning people to "Not Get Butchered" [3], reporting victim losses often in the hundreds of thousands but as high as two million. Chainalysis reports an average payment of $4,593 for these scams – the most amount lost per scam they measure – which is impressive given their interactive nature (most involve multiple money transfers between the victim and the scammer) [4].

Towards understanding this growing threat, we analyze 133 scam narratives collated by the US state of California. While the inclusion criteria is broad (cryptocurrency scams against California residents), most of the scams are interactive, relationship-building scams aka pig butchering scams (often with a romantic component). Our data source defines pig butchering as such as outlined by Table I. Other work confines pig butchering scams to romance scams – our broader definition makes sense in context of this paper, especially when victims might feel ashamed and not report the romantic component.

Our contributions are as follows:

- We add to the emerging literature on cryptocurrency pig butchering scams (§II) by analyzing newly reported scam narratives – a relatively novel method in this space.
- We hand code 143 scam incidents across 133 narratives and 11 scam types using thematic analysis (§III).
- Using these themes, we characterize these broad scams. We break down each stage of these scams which provides us insight into not just the mechanism from which the scammer extracts money from the victim, but also the other processes surrounding the scam. We uncover commonalities across scams (scammers pick a persona with an opposite gender to their victim; most scams end up in direct messaging apps) and differences (lures) (§IV). This demonstrates the wide array of scams despite the common mechanisms.

2159-1245/24/$31.00 ©2024 IEEE
DOI 10.1109/eCrime66200.2024.00016

- Third parties seem to put the onus on victims, rather than proactively managing their platforms. We make actionable recommendations to governments, cryptocurrency platforms, and the cryptocurrency community writ large towards combating these scams (§V).

II. Related Work

We survey the nascent social science literature in the growing area of pig butchering scams (§II-A). Then we preview work measuring cryptocurrency scams writ large, highlighting the diverse sets of data collected by researchers (§II-B).

A. Pig Butchering Scams

There is some existing work in pig butchering scams which bridge between investment scams and (most commonly) romance scams. Cross outlines why these scams are increasing in popularity, among other things that they allow scammers to wield a relationship to obtain trust (and therefore less red flags and more financial gains) [2]. Their interactive nature also makes them trickier to detect with current technology. Maras and Ives comb through US court cases and news articles, highlighting how organized crime groups use vehicles like shell companies or overseas components [5]. Working to discretize losses, they find that often the money lost does not end at measurable costs to the direct victim, but often reverberates out from them. Wang narrows in on the scammers behind these scams, particularly how they exploit trafficked people to purport these scams [6]. Griffin and Mei measure the proceeds from these scams using the blockchain and purport $\$75.3b$ moved into scammers' accounts [7]. We note the existing controversy surrounding this term which we use as a reflection of the terms our data source uses [8].

B. Cryptocurrency Scams

There have been a number of recent works empirically measuring cryptocurrency scams, albeit focusing on non-relationship-building scams. However, all of them have been reflections of where the data has been collected as well as the types of data that they collect.

Researchers often use scam aggregator websites curated by volunteers raising awareness about scams. Anti-scam aggregators can be noisy, but a useful reflection of what the community finds bad at a point in time. Vasek and Moore use data from scam aggregators towards finding their set of Bitcoin Ponzi schemes and other cryptocurrency scams [9]. Bartoletti et al. use similar aggregators and automate their scam detection [10]. Similarly, Xia et al. uncover cryptocurrency exchange scams via scam aggregators as well as via typosquatted domains related to legitimate cryptocurrency exchanges [11]. This use of external information is also performed by Li et al. who analyze cryptocurrency giveaway scams in depth using certificate transparency logs [12].

Others directly measure the scam using methods that victims would use to find the scam. Bawadi et al. unearth cryptocurrency scams that promise free cryptocurrency if the victim pays a small fee using programmatic searching [13]. Pump and dump scams are measured using indicators from pump and dump Telegram, Discord, and Twitter accounts [14]–[16]. Vasek and Moore studied cryptocurrency Ponzi schemes targeting new Bitcoin users on bitcointalk [17]. Nizolli et al. collected data from a wide variety of social media websites towards programmatically detecting an assortment of cryptocurrency scams [18]. Li, Lee, and Guan scraped Twitter lists to detect cryptocurrency free giveaway scams [19].

A common method unique to cryptocurrencies is to measure cryptocurrency scams using the blockchain. While other works listed above might measure profits via a blockchain, these works use the blockchain to directly discover scams. Many different researchers have used Ethereum to find and measure Ponzi schemes (e.g. [20]–[22]). Torres, Steichen, and State yielded the Ethereum blockchain towards a large scale collection of cryptocurrency honeypot scams [23]. Igarashi and Matsuura identify scam tokens by performing static analysis on smart contracts [24], similarly to how Fröwis, Fuchs, and Böhme found duplicated token contracts [25]. Many have analyzed rugpull scams (where DeFi tokens are promoted and then abandoned) using the blockchain [26]–[28].

Cryptocurrency scam narratives can be analyzed in order to uncover insights into a broader range of scams. Often qualitative researchers use these narratives to uncover themes which quantitative researchers can then use to analyze in aggregate. Childs codes narratives on Reddit towards uncovering themes and community norms around cryptocurrency scams [29]. Agarwal et al. programmatically collect narratives on rugpull scams on the Bitcoin forum, characterizing slow and fast rug pulls [30]. Anderson et al. study cryptocurrency scams on Reddit and the US FTC blog towards identifying trust relationships needed for these scams to thrive [31].

III. Methodology

In order to have a broad overview of the recent scams in the cryptocurrency ecosystem, we use the California Crypto Scam Tracker (§III-A). This allows us to have a timely and broad overview of different types of scams that were reported in a large area. We then use a variety of qualitative and quantitative methods to analyze these scams.

A. Data Source

In February 2023, the Department of Financial Protection and Innovation (DFPI) in the US State of California launched the "Crypto Scam Tracker" [32]. This contains complaints submitted by consumers and reviewed by the department. These complaints are presented as summaries (complaint narratives) describing scam indicidents. These often contain information about the victim such as gender, details about the scammer(s), how the victim was introduced to the scam, methods used by the scammer to lure and deceive the victim, and details on the amount of money lost and/or requested by the scammer. Note the DFPI does not verify the losses purported by the victims.

In addition to the complaint narrative, there is other relevant information including suspects (primary and other subjects),

Scam Type	Definition
Advance Fee	Upfront payment, promising a future service or huge return on investment.
Asset Recovery	Fee to "recover" funds lost in a prior fraudulent transaction.
Fraudulent Trading Platform	Fraudulent website or application which offers a unique investment opportunity.
Hacking	Exploits a computer system with the intent of stealing personal information.
High Yield Investment Program	Fraudulent trading platform which promises high returns in short periods of time. Similarly to mining scams, scammer presents fake dashboard with fake profits.
Identity Theft	Wrongfully obtains and uses another person's personal data towards fraud or deception.
Imposter	Wrongfully impersonates a legitimate business, government agent, or well-known figure.
Liquidity Mining	Fraudulent platform which promises passive income with crypto assets. Similarly to HYIPs, scammer presents fake dashboard with fake profits.
Livestream	Livestream event which markets a fraudulent promotion or product.
Pig Butchering	Slowly gains a victim's trust towards introducing them to a financial scam.
Romance or Social Media	Gains a victim's affection and trust towards an illusion of romance or friendship.

TABLE I: Eleven scam types and definitions paraphrased from the DFPI glossary [32].

websites involved, and the different *scam types* that are associated with each incident.

Scam Types and Definitions. The DFPI Crypto Scam Tracker provides a glossary of terminology that describes the types of scams. These definitions are not official legal definitions derived from any laws, but rather common working definitions used in the field. California laws currently do not expressly define or distinguish between all these cryptocurrency scams. The DPFI also notes that definitions often change over time as scammers do.

The glossary comprises 17 terms with corresponding definitions. Only 11 out of the 17 scam types listed in the glossary have listings in the scam tracker; the rest are proactively listed. We thus only consider these 11 types (Table I).

The continually updated website intends to offer consumers a comprehensive grasp of the most recent and emerging fraudulent activities. In line with its function in alerting and raising awareness, the website grants researchers entry to the most current variations of scams and how different people fell victim to those scams. Cryptocurrency scammers are recognized for their creativity [33], constantly devising new methods for victimizing individuals. This data source gives us a natural opportunity to analyze a diversity of scams that are affecting consumers now.

B. Data Collection

We collect the content of the website in late January 2024. At the time of retrieval, there were 133 entries.

Upon manual review, we observe inconsistencies in how incidents are documented, especially when multiple victims report the same scam. In some cases, the website consolidates multiple victims of a single scam into a single entry, while in other cases, it creates individual entries for each victim of the same scam/scammer. To address this issue, we examine these inconsistencies and implement necessary modifications to guarantee precision and homogeneity. Overall, we find 10 entries reporting more than one victim. Upon reviewing these 10 entries, we observe that each victim's experience and interaction were independent and unique, and although the scammer was the same, the scheme was different. Hence, we separate the victims of those cases and treat them as independent entries for counting and analyzing purposes. In one entry, we decide not to separate the entries because the victims were connected to each other; they were both victimized during the exact same incident dependently. This process yields 143 scam incidents across 11 scam types to analyze further.

Scam Type	Count	Gender Scammer	Gender Victim	Count
Fraudulent Trading Platform	124	Male	Female	11
Pig Butchering	101	Male	Male	6
Imposter	45	Female	Male	56
Advance Fee	16	Female	Female	12
Liquidity Mining	14	UNK	Female	8
Romance or Social Media	14	UNK	Male	27
Hacking	5	Female	UNK	0
HYIP	5	Male	UNK	0
Asset Recovery	5			
Identity Theft	3			
Livestream	1			

TABLE II: Scam count by type (as the website labels) and gender (as we code). Some scams have multiples types; some scams have varied gender groups as victims or scammers.

C. Qualitative Methods

To gain insight into *how* scams operate and *what* methods scammers employ to victimize individuals, we conduct qualitative thematic analysis on the incidents collected in §III-B [34]. Identifying patterns and understanding the strategies employed by scammers is essential for developing effective countermeasures against such crimes.

Three of the authors systematically coded and classified the data using a "concept-driven" approach, after creating a codebook [34]. After a few rounds of revisions between the coders, the final codebook comprised 19 themes; for instance, some of the themes address victim and scammer characteristics for example, while others identify and categorize the diverse range of lure techniques and the step-by-step process different scammers use. After coding and discussing 20 complaint narratives and various themes and codes, one coder adapted the extracted and thematically classified information, incorporating the Stajano and Wilson [35] scam lure principles (Table IV). We outline the adapted lure principles, along with the identified techniques used by scammers in §IV-A2.

Some of this coding was straightforward. Table II details the gender of the victims along with the portrayed gender of the scammers. Similarly, Table III outlines the messaging platforms that scammers used to contact the victims.

Category	Name of Platform/App	Frequency
Messaging App	WhatsApp, Telegram, Line, Discord, SMS, Viber, WeChat	75
Social Media	Instagram, Facebook, Twitter, and mentions of 'online' or 'Internet'	39
Dating App	Tinder, Zoosk, OkCupid, Coffee Meets Bagel, Salam, Hinge, and mentions of 'dating app'	14
Prof. Networking	LinkedIn	9
Undefined	Mentions of undefined platforms or applications	9
Email	Email	4
Phone Call	Phone calls	4
Real Life Contact	Mentions of offline discussions	4
Video Streaming	YouTube, TikTok	2

TABLE III: Name of Social Media, Platform, or App scammers used to communicate with potential victims along with the category that fits its primary objective.

Monetary Damages. Alas, some of the information provided in the complaint narratives was insufficient for coding. One specific challenge we encountered was determining the monetary losses experienced by victims. In 90 cases, the complaint narratives clearly stated the amount lost by the victim ("the victim lost 10 thousand dollars"). In 19 cases, there was no mention of monetary losses; we code these as "not applicable". The most challenging cases involved vague references to monetary losses e.g. "the victim lost millions of dollars" or "the victim invested 3 ETH" (34 records). For these, we estimate a range of money lost based on information within the complaint narrative, including initial investment amounts, supposed earnings in the victim's account, and any requested fees by the scammer. For example, "millions of dollars" is a minimum ($floor$) of $\$1m$ lost with a maximum ($ceiling$) of $\$9.9m$ lost. After coding these 34 cases, the three coders discussed and compared their estimations to reach a consensus, a process that involved three cycles.

D. Statistical Methods

We perform a variety of statistical tests on our data in line with the nature of the data. To investigate the behavioral patterns of scammers in their communication methods across various platforms, we employ a Markov Chain analysis [36]. Markov Chains are stochastic models that describe a sequence of events where the probability of transitioning from one state to another depends only on the current state and not on the sequence of events that preceded it.

In this study, we treat each communication platform category (e.g. dating app, messaging app) as a distinct state within the Markov Chain model. We analyze and estimate the transition probability of various communication platform categories between different scams in our dataset. For example, the probability that a scammer would switch from a dating app to a messaging app, etc. The Markov Chain model allowed us to capture the dynamic nature of scammers' communication strategies and quantify the likelihood of transitions between different platforms. This analysis provided insights into whether scammers tend to change their communication methods and the probabilities associated with such transitions.

E. Ethical Considerations

Our university ethics review board deemed our study exempt based on the lack of identifiable human subject features in the dataset as well as our lightweight collection method. We securely collect and store the data.

IV. Analysis

Like other scams [37], the cryptocurrency scams we study here contain four distinct phases: preparation, pre-activity, activity, and post-activity. We analyze scams using these phases to understand them more in-depth as well as provide insight into various stakeholders (victims, abused third-party services, governments) on how to disrupt scams at each stage.

A. Preparation

Before reaching out to potential victims, scammers engage in preparatory activities. These actions can aid in luring targets into the scam and establishing the credibility of the scam. Below we outline the primary preparatory work scammers engage in:

Fake persona. Creating a fake persona involves fabricating details such as gender and background (personal history). Section IV-C2 will show that scammers target the opposite gender and doing so is more financially lucrative. This indicates that gender is an integral component of the persona they construct.

Backstory. The backstory of the scammer beyond the initial persona is crucial for attracting and appealing to targets. These vary widely. Many scammers fabricate fictional scenarios and stories to portray their identity and qualifications, often claiming to have extensive experience in trading and investing. Some create tragic scenarios to build rapport with targets, such as pretending to raise funds for a humane cause. Others deceive targets with their intentions, e.g. by falsely claiming to be seeking friendships or romantic relationships.

Online presence. When scammers use social media or professional networking platforms, part of creating the fake persona involves choosing a specific platform and making a new fake profile for that persona. This is quite a popular approach (Table III) – social media apps (e.g. Instagram and Facebook) combined with professional networking platforms (e.g. LinkedIn) constitute the second most popular methods of directly contacting the targets.

Impersonation and hacking. In some instances, scammers engage in identity theft by impersonating other individuals. There are two such cases in our dataset. In the first scenario, the scammer creates a new profile of another person. In the second, they hack and gain unauthorized access to an existing account and use it to exploit friends or family.

Phishing. Some incidents involve phishing, where victims receive an email containing a link. For example, one victim received an email stating their account was closing, instructing them to sign in by clicking the provided link if they wished to withdraw their funds. The goal here is often not just directly financial, but also to obtain personal information or bank details for later use.

Co-offending. Co-offending involves multiple scammers collaborating on a single scheme. In our dataset, we identify seven cases where co-offenders are involved. However, it is possible that the appearance of co-offenders is part of the scammer's strategy and persona development. Likely, there may not be separate co-offenders but rather one scammer creating multiple personas to facilitate the deception of the target. A common scenario involves scammer A initiating contact with the target, enticing them to invest in a specific (fake) platform; when issues arise with fund withdrawals, scammer B steps in as customer support from that platform. Scammers A and B are likely the same person here.

International element. Some scammers integrate an international element into their scheme. We identify three approaches: 1. Pretending to be a naive foreigner who is new in the United States; 2. Using foreign names, especially east Asian names; and 3. Describing investment or trading platforms as companies located abroad and portraying them as legitimate and renowned companies in those foreign countries; referring to a company being foreign would likely prevent the victim from conducting due diligence about it. Pig butchering scams originated in China; the United Nations [38] and others [6], [7] have tied current operators of these scams to southeast Asia.

Fake trading/investment platform or app. Scammers not only craft fake human personas, but they also fabricate fake legal personnel such as fake companies, platforms, and apps. They intend to present these trading/investment platforms as legitimate as possible, using a company persona to instill further confidence in the victim. As part of their scheme, scammers establish websites for fictional investment or trading firms with names that often resemble those of legitimate businesses. Subsequently, these are the platforms that the scammers will later introduce to victims after successfully leading them into the scam. These websites bear a striking resemblance to other genuine platforms, making it challenging for victims to differentiate between real and fake ones.

1) Scam Co-occurrences: The other part of preparing the scam is preparing the type of scam. In this dataset, all of the scams are annotated with more than one scam type out of the 11 types found in Table I. To visualize this, we use an asymmetric scam type co-occurrence heatmap in Figure 1.

Our dataset has 101 cases of Pig Butchering Scams and 14 cases of Romance Scams. All 14 Romance Scam cases are also annotated as Pig Butchering Scams. Thus, 100% of Romance Scams are also Pig Butchering Scams, as shown in the first cell, second row of the heatmap. Only 14 of the 101 Pig Butchering Scams have been annotated as Romance Scams,

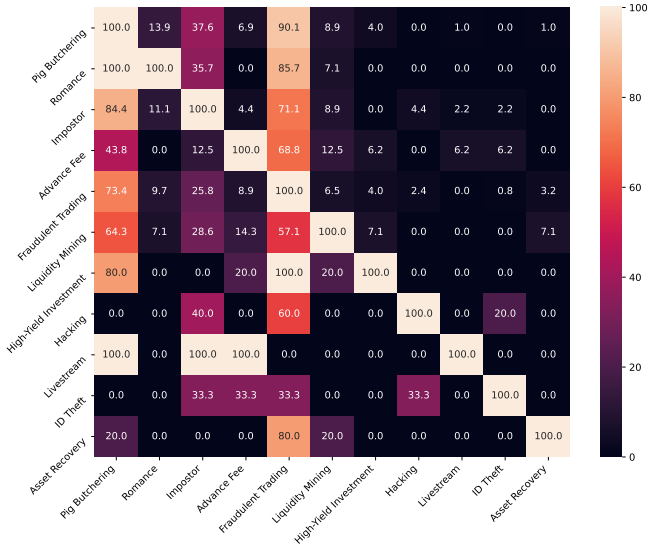

Fig. 1: Asymmetric heatmap of the percentage of different Scam Type co-occurrences. The figure is asymmetric since scam types co-occur with each other variably (best read horizontally).

accounting for 13.9% of Pig Butchering Scams, indicated in the second cell, first row of the heatmap.

Overall, we notice high levels of co-occurrence of Pig Butchering Scams with Romance Scams (100%), Impostor Scams (84.4%), Fraudulent Trading Scams (73.4%), High-Yield Investment Scams (80%), and Livestream Scams (100%). Romance Scams are associated with Pig Butchering Scams (100%) and Fraudulent Trading Scams (85.7%). The Advance Fee Scam appears to co-occur often with Fraudulent Trading Scams (68.8%), which is expected as many scammers convince their victims to pay 'fees' to release their supposed winnings made via trading. Unsurprisingly High Yield Investments always co-occur with Fraudulent Trading Platforms which facilitate the scheme.

Composing multiple scam types can make sense within the context of the lifetime of a scam. Other work focuses on the main type of scam rather than the scamming process. Most of these scams would be considered fraudulent trading scams by others, since that is the cash out method. However, we consider the context around the scam – how the scammers attract the victim to the scam (like pig butchering) and other scams needed to gain trust otherwise (like imposter scams). This helps us understand the changing nature of scams – rather than waiting for victims to find your website while they are looking for a cryptocurrency wallet over Tor or a free source of cryptocurrency via a search engine, most of the scammers here proactively reach out to victims as their initial planned contact vector. The preparation of these details will be discussed more in later sections, as we analyze the specific ways in which the scammer executes their plan.

2) Lure Methods: Scammers use social engineering methods to lure potential victims. Though these methods can be

diverse, many occur concurrently. Stajano and Wilson [35] developed seven principles portraying behavioral patterns that scammers use. Identifying these patterns is crucial to understanding attacker behavior and, thus, is the first step in stopping them. Prior work has adapted these principles to decipher techniques employed in different types of scams such as rugpulls [30]. Table IV briefly outlines these principles; we expound on them as follows:

Distraction Principle. Many scammers use backstories (as outlined in §IV-A), or intentions of friendships, professional relationships, or romance to lure and distract their victims from their main intention. Prior work demonstrates how useful and successful scammers are when harnessing the power of relationships [2], [39]–[41]. We found one incident where a scammer made the victim believe they were in a serious relationship – discussing marriage, children, and a home together. These tactics help gain the victim's trust and hope for the future so that when the scam is brought up after periods of conversation, the victim does not doubt it. We note that scammers invest a significant amount of time, sometimes months, in nurturing fake social relationships with their victims before victimizing them.

Social Compliance Principle. Scammers use this technique to establish social authority over the target, making the victim believe they are experts in trading/investing and therefore should be trusted for their judgment. Other scammers claim to be rich and successful and can therefore teach the victim how to make money.

Herd Principle. Scammers fabricate evidence to support their schemes by sending screenshots of fake positive reviews of the fraudulent platform and screenshots of their own large personal winnings. This helps validate their claims about making profits and the legitimacy of the used platform. Some also tell victims that they will invest money alongside them. One scammer told the victim they had placed $\$80k$ of their own money to encourage the victim to join them in trading.

Dishonesty Principle. This approach is used when the victim has already invested significant amounts and supposedly made large returns, only to be denied withdrawal. Unfortunately, this is the point many victims realize they have been deceived. In some cases, platforms falsely accuse victims of engaging in illegal activities like tax evasion or money laundering. This tactic serves as a means of extortion and aims to dissuade victims from seeking help from law enforcement due to their own involvement in illicit activities.

Kindness Principle. Scammers exploit the victim's willingness to help or naivety via their fake backstory and scenario (§IV-A). For example, a scammer pretended to be starting a non-profit to aid autistic kids and persuaded the victim to engage in joint trading activities to raise funds for the purported cause.

Need and Greed Principle. Scammers exploit the victim's financial need by offering false promises of monetary gains. In one scenario, the victim initially invests a some money ($\$650k$) and the platform quickly offers a ludicrous rate of return showing the victim an inflated sum ($\$10m$), prompting the victim to invest more money. We also find scammers making promises of high returns in short periods in other ways, e.g. by presenting fabricated evidence of their own substantial earning to encourage victims to invest (see herd principle). Other scammers manipulate victims in need of money. In one incident, a scammer befriended a widowed mother of four kids claiming to be a senior expert in trading, and offered investment lessons in cryptocurrencies.

Time Principle. Scammers use time pressure to push victims into making quick decisions to invest money. This can happen at the beginning of the scheme, where scammers may claim there's a limited-time deal with high returns, creating urgency for the victims to not miss out. Alternatively, they might tell victims that consistent trading or interactions within a specified timeframe (e.g. 5-7 days) is necessary to make profits. Time urgency also occurs in the final stage of the scam when victims are unable to withdraw their money and are pressured by scammers (or the platforms' customer support) to comply with certain requests to not lose their funds; for example, subscribing to a VIP account, paying taxes or fees, etc.

We have a wide variety of scams, so that lends a variety of different lures, much more so than other cryptocurrency scams (e.g. [30], [42]). This could also be due to the personalized nature of these scams, since most of them were a victim interacting with the scammer over a period of time. Perhaps the personalized nature of the scams is reflected in the variability of lure, where the scammer is (potentially) trying all the ways to lure the victim, perhaps only telling us about a few.

B. Pre-Activity

After the scammer creates their persona and constructs their scam, the next step in the process is the initial contact with the victim (aka the Pre-Activity). Scammers employ diverse approaches to target potential victims. Directly contacting potential victims stands out as the predominant method used here, with 110 incidents reported. In this approach, human scammers reach out directly to communicate with potential victims. As for the relationship between the scammer(s) and potential victims, the overwhelming majority of cases involve scammers who are strangers to their targets; a minority of instances ($n = 3$) involve old friends and family acting as accomplices in these schemes.

In contrast, indirect contact involves scammers not reaching out directly to a victim; rather, they establish platforms like fraudulent cryptocurrency trading services. Victims discover these platforms independently without any direct interaction or influence from a human scammer. Some come across them through social media advertisements or posts directed at the general public, or via communications on public channels in apps like Telegram. While there is no direct communication between the scammer and the victim during the initial stages of victimization, in some cases, human scammers interact with victims in later stages, predominantly as "customer support".

Lure Principles	Description
Distraction	Distract and confuse victims with overwhelming or unrelated information.
Social Compliance	Impose authority over victims by showcasing their financial knowledge and establishing credibility.
Herd	Encourage victims not to miss out on rewards by providing fabricated evidence of how others are making major profits in the scheme.
Dishonesty	Invite victims to the scheme and then turn against the victim and accuse them of illegal activity.
Kindness	Take advantage of naive victims and their willingness to help.
Need and Greed	Take advantage of victims' financial greed and offer false hopes of major financial rewards in return for an investment from the victim.
Time	Pressure victims to make decisions as the investment opportunity might not last.

TABLE IV: Description of adapted scam lure principles per Stajano and Wilson [35].

C. Activity

The next step is carrying out the scam. Here, we characterize the methods of communication beyond the initial contact (§IV-C1) and estimate the money lost and various factors that affect this (§IV-C2).

1) Communicating with Victims: When scammers directly initiate contact with potential victims, they use a variety of methods to communicate with them. A small number ($N = 4$) contacted victims by telephone, while others sent text messages or emails. However, the predominant method was through social media apps like Telegram, Instagram, and Facebook. It is worth noting that in these cases, scammers spent weeks and even months building trust with the victims.

During these extended periods of communication, most scammers switch between different communication channels or apps while interacting with the victims. The scammer initially uses a specific app for introduction and contact purposes and then directs the victim to use a different one after establishing some level of trust. Up to three different apps are used throughout the scam. Most of these apps are global, popular apps; in a minority of cases, victims were asked to download and use regional or unpopular apps.

Table III lists all the different social networks, applications, and platforms scammers use to approach or contact potential victims. We categorize applications based on the primary objective/function of these platforms. For example, TikTok supports direct messages between users, but it is marked as 'Video Streaming' as its primary task is not 'Messaging App.' Our frequency count is greater than the total entries of our dataset as many scammers used various platforms to communicate with single victims, hopping between different apps. More specifically, if a single entry involved WhatsApp, Line, and SMS, then this will count as three occurrences of 'Messaging App' for a single scam.

Preferred Communication Applications. Figure 2 shows the different apps that are used by our varied scams. Messaging Apps turn out to be the most popular applications that scammers use for many scams, including Pig Butchering, Impostor, Advance Fee, Fraudulent Trading, and Hacking scams. This is to be expected to some extent as many of those frauds require the scammer to convince the victim, hence using a messaging app provides easy communication. Regarding Romance Scams, as to be expected, dating apps are the most popular followed by messaging apps. As to be expected, all the

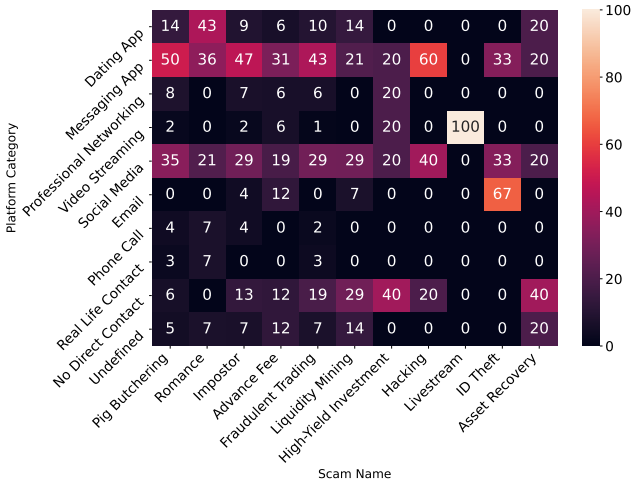

Fig. 2: Heatmap of the percentage of platform categories used per scam type. The total of each column will not amount to 100% as a scam might involve many platform categories.

cases of Livestream Scams took place via a Video Streaming platform or application.

Overall, the most used methods of communication seem to be Messaging applications and Social Media. At the same time, a single scam tends to involve various communication methods, with 36 cases where scammers changed their initial application of communication to a different one.

Platform Hopping. To better understand the elaborate process in which scammers involve their victims in, and how different applications are used for communication, we dive deeper into the application hopping methods of scammers. We employ Markov Chain analysis which shows the probability of a Platform Category having a shift (Figure 3). We involve all cases in our dataset, even the ones where the scammers did not hop through various applications in a single scam.

Overall we notice a distinct pattern: the majority of the scams in our dataset have various ways of initializing contact, but they will, with high probability, move to a messaging app eventually. The exceptions being scams that had no direct contact, used an unknown platform, or communicated via email – these scams never hopped platforms. This finding is in line with previous work which demonstrated how various social media profiles could give the illusion to a victim that

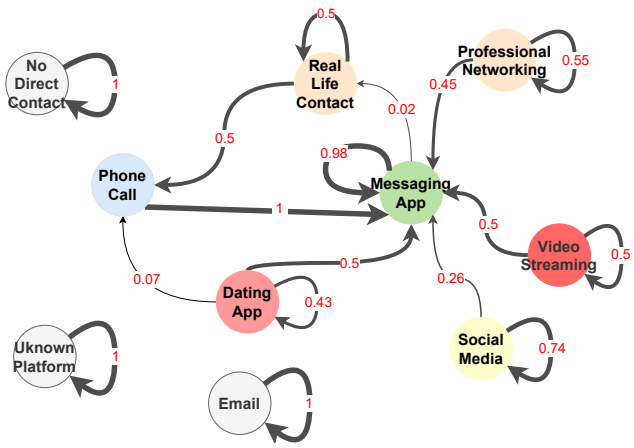

Fig. 3: Markov chain of Platform/App Category shift.

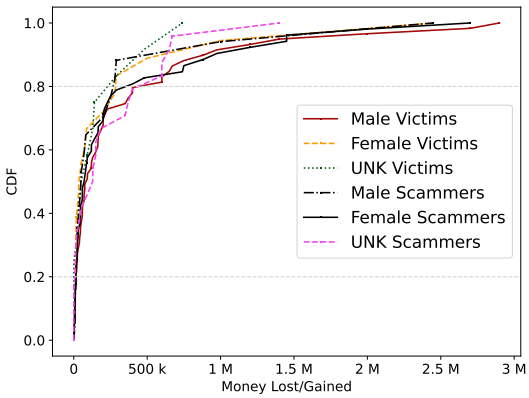

Fig. 4: Cumulative Distribution Function of the amount of money lost per victim gender, and the amount of money gained per scammer gender ($n = 90$).

the person they speak with is legitimate [31]. This pattern highlights that apps need to coordinate data sharing on scams in order to take them down.

2) Monetary Losses and Gains by Gender: Gender appears to be driving victimization. More specifically, we find that scammers who pretend to be male approach female victims, and scammers who pretend to be female approach male victims (Table II).

Actual Monetary Damages. First, we calculate the amount of money lost per victim and the money gained per scammer based on their gender, respectively, using a CDF shown in Figure 4. We perform this analysis to provide a distribution of the monetary losses per victim gender in an attempt to detect whether there is any significant difference between victims. If the gender of the victim or scammer was not defined in the complaint narrative, then we list the monetary losses/gains of that victim/scammer as an unknown ('UNK' in the figure) victim/scammer. For this analysis, we only consider the entries where the complaint narrative listed a concrete amount lost by the victim ($n = 90$).

While 50% of the male victims lost at least $\$92k$, 50% of female victims lost approximately a third of that - $\$35k$ (Figure 4). At the same time, scammers portrayed to be males seem to be less successful, with 50% of them earning at least $\$51k$ and 50% of scammers portraying to be female managed to elude their victims to least $\$70k$. This analysis shows that males tend to fall victim to higher amounts of money more often, while at the same time, female scammers tend to be more successful. This finding fits into our established pattern of victimization since we previously showed that scammers portraying to be female tend to target male victims (Table II).

We run a two-sample KS test on these distributions to test the null hypothesis that these sets of data have any significant differences between them. This test yields $p - values$ higher than 0.01 for all distributions; hence, we cannot reject the null hypothesis that the distributions are significantly different. Notably, the KS test on the distributions between 'Male Victims' and 'Female Scammers' resulted in $p = 0.998$, which means that these 2 distributions are almost exact copies of each other. This finding strongly suggests that almost all of the "Male Victims" in our dataset were scammed by "Female Scammers." Similarly, the KS test on distributions between "Female Victims" and "Male Scammers" resulted in $p = 0.995$, which strongly suggests that these two distributions are identical; hence most "Female Victims" were scammed by "Male Scammers."

Overall, we demonstrate that scammers likely portraying one gender to target the opposite gender. At the same time, male victims tend to fall victim to higher amounts of money and scammers that portray to be female tend to be more successful in eluding victims for more money, which most of the time tend to be males. This is aligned with previous work that found that men are more likely to be victims of an investment scam compared to women [43]. Considering how most of the scams in our dataset are investment-related scams, it creates a "fruitful" environment for scammers to target victims. Similarly, we find that victims are influenced by the large offered values in a scam, as suggested by the complaint narratives themselves. Very often, victims were promised large profits and showed a high level of trust towards their scammers [44].

Estimated Monetary Damages. The previous subsection considered the money lost for the complaint narratives with hard numbers. However, as detailed in §III-B, 34 narratives contained rough numbers, which we estimate using orders of magnitude. This subsection considers both the hard and the estimated numbers (90 records with concrete monetary losses, and 34 instances of estimated monetary losses).

The actual monetary damages of male victims are almost $\$20m$. Considering that this amount comes from 86 males, this is a substantial amount lost per victim on average (approximately $\$233k$). Using the ceiling of the calculated estimate of money, that amount rises to as much as an additional $\$17.4m$ (similar amount lost per male with 34 additional datapoints). Female victims lost over $\$5m$, but that amount does not rise

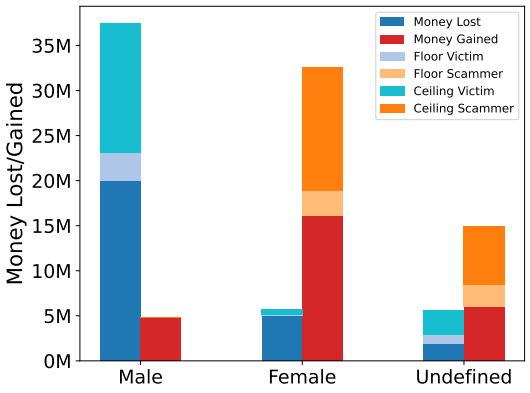

Fig. 5: Stack bar plot of total, floor, and ceiling money lost and gained per victims and scammers, respectively. ($n = 124$)

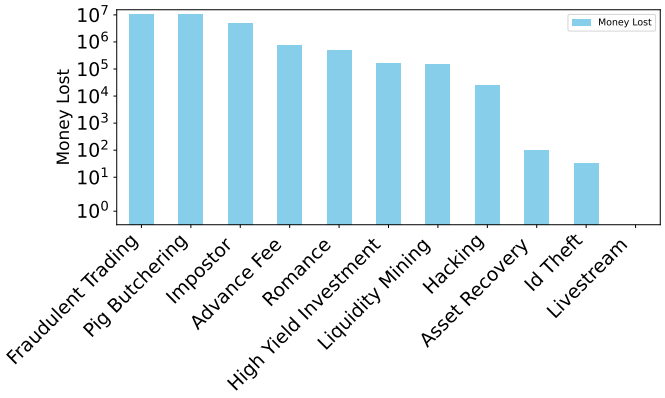

Fig. 6: Money lost per scam type ($n = 90$). (`symlog` scale on the y-axis combines logarithmic and linear scaling. This preserves the log scale for large values with a linear scale for smaller values).

much with the estimated values as our dataset for female victims had clear monetary losses.

From the scammer perspective, scammers pretending to be male gained $\$4.85m$. We have estimated values for male scammers as all the cases in our dataset listed specific amounts lost from victims to male scammers. Female scammers gained $\$16.1m$ with that amount possibly reaching as high as $\$32.4m$.

This analysis shows the devastating monetary damages towards victims, especially males, to these investment scams. Considering the amounts possibly lost from these scams, the average monetary loss per victim is significant.

Monetary Losses per Scam Type. We analyze the amount of money lost per scam based on the subset of the data with concrete loss numbers (Fig. 6). Many instances have multiple scam types. We divide the total amount lost for a single instance between each of the types; for instance, if a victim lost $\$99k$ to a scam which was pig butchering, romance, and fraudulent trading, then each scam will be assigned $\$33k$.

Overall, Fraudulent Trading Platforms (80 occurrences) amount to more than $\$10m$ lost, followed by Pig Butchering scams (71 occurrences) for approximately the same amount. Conversely, Romance Scams and High-Yield Investment Scams have lower occurrence rates in our dataset (6 and 2 respectively) but still result in substantial monetary losses, emphasizing the need for targeted awareness campaigns and investment by third parties that help facilitate this fraud to mitigate the risks associated with these deceptive practices.

D. Post-Activity

The final step is what happens after the original scam ends. We show what happens in illicit trading platforms (§IV-D1) and discuss successful vs. unsuccessful attempts (§IV-D2), noting that our data is skewed towards successful attempts.

1) Post Scam Victimization – Illicit Platforms: Cryptocurrency scams that involve a scammer controlled platform (website, app, etc.) often conclude with the victim being unable to withdraw their expected returns. While some scams end at this point, in many cases, perpetrators continue exploiting their initial victims' vulnerability and desperation.

After denying a withdrawal request, the platform not only provides a reason for this denial, but also offers a way out of that situation. This post scam victimization involves requests for additional money or personal information from individuals who are still hopeful of recovering their losses.

We observed some common patterns: VIP subscription opportunities for victims to be able to "withdraw faster", tax withholding requests, anti-money laundering penalties, and fees ranging from service charges to address or account verification to "bad credit score" fees. In one incident, a victim who had transferred over $\$1m$ was asked to pay $\$300k$ upfront to the IRS within 7 days. These mechanisms exist to either extract all of the money out of a victim or to even extract the most amount of an otherwise unsuspecting victim. Online Ponzi schemes often have "withdraw faster" fees to target the desperate and extract their last bit of money. Advanced fee fraud (aka Nigerian prince scams) often involves an upfront fee with additional fees that add up to the total scammed amount We even see this with victims trying to avoid buying an Android App from the official store; they then move to a third party store, download a free app packaged with malware (the "activity") and end up paying fees via an app request afterward (the post-scam victimization). Regulators and potential victims need to be aware that this multiple-dipping victimization happens with frequency in cybercrime. We need to act to prevent the second step which can sometimes be more harmful than previous steps.

2) Scheme Outcome: Crimes, including scams, have different outcome possibilities. The outcomes we find are: 1. Successful completion, or 2. Failed attempts. The primary goal of cryptocurrency scammers is financial gains. A successful scam results in significant harm, including monetary losses (detailed in Fig. 5). Successful scam schemes may perpetuate a cycle of repeat offenses and promote further criminal activity.

In contrast, there are cases of unsuccessful attempts in which the scammers' dishonesty and deceptive actions fail for various reasons. The majority of incidents (136) were

successful, leaving 7 scams unsuccessful. We find that initial contact or exposure to the scam by a potential victim does not guarantee success. In these instances, individuals who engaged with the scam through a platform or a human perpetrator were not deceived by deceptive tactics and did not transfer funds to the scammers despite interacting with them.

Surprisingly, the success rate for full fund recoveries was zero. Furthermore, very few victims managed to reclaim a small portion of their funds. In the latter case, some victims could only withdraw small amounts as part of the scheme. The platform allowed these withdrawals to appear legitimate and persuade victims to invest larger amounts (similar to the scam wallet ruse found by Vasek and Moore [9]).

Our dataset, by its nature, is skewed towards scam successes. We encourage similar datasets to consider adding failed attempts to aid this analysis further, allowing researchers to understand the wider array of scams better.

V. Recommendations for Countering Scams

Combating cryptocurrency scams requires a multi-faceted approach that involves the active participation of multiple stakeholders, including governments, online platforms, and the cryptocurrency community. Through concerted efforts and enhanced cooperation among these entities, it is possible to establish a more resilient defense against cryptocurrency scams. Each stakeholder holds an essential position in thwarting these scams and safeguarding consumers from potential financial harm and other adverse consequences. Based on our thorough analysis of the California DFPI Crypto Scam Tracker, we identify areas of intervention and propose measures and strategies that could effectively mitigate these scams:

A. Regulatory Clarity and Enforcement

Regulation is key in combating cryptocurrency scams. Government intervention is necessary in two main areas. First, there is a need to regulate and monitor cryptocurrency service providers including trading platforms and exchanges (§V-A1). Second, there is a need to clarify regulation concerning existing legal compliance procedures, as scammers exploit the ambiguity and consumers' lack of knowledge about the law, using compliance (e.g. tax compliance) as a scam tactic (§V-A2).

1) Regulating Cryptocurrency Service Providers: Cryptocurrency scams that we tackle in our work direct victims toward cryptocurrency service providers, such as exchanges and investment/trading platforms. Due to the ease of creating fraudulent websites that appear authentic, victims struggle to differentiate between legitimate and fraudulent platforms. A crucial step here would be for governments to oversee and regulate cryptocurrency service providers, ensuring compliance while also enabling consumers to easily authenticate the legitimacy of visited websites.

The lawmakers in California per se, have recently passed a new legislation called "Digital Financial Assets Law" (DFAL) which will come into force in 2025 [45]. This law will mandate cryptocurrency service providers to obtain a license to operate. The aim of this requirements is to assist consumers and potential targets by enabling them to differentiate genuine cryptocurrency platforms from fraudulent websites. Through increased awareness, it is expected that this measure will contribute towards reducing incidents of victims falling for illegitimate platforms.

In a similar vein, the European Union adopted the world's first comprehensive regulatory framework in 2023 with the introduction of the Markets in Crypto-Assets regulation (MiCA) [46]. Starting at the end of 2024, this regulation will enforce requirements for cryptocurrency service providers (such as exchanges/trading platforms, and custodial exchanges) to obtain a license to be allowed to offer their services within the EU. Additionally, competent authorities will play a monitoring role to identify non-compliant services and prohibit them from operating. This aims to hinder the prevalence of fraudulent platforms and provide users with appropriate consumer protection and a reliable environment.

While several regulators are implementing measures to oversee cryptocurrency service providers, two main challenges persist: enforcement and universality. The effective enforcement of regulations is tricky as a law's mere existence is insufficient without proper enforcement. Similarly, when only specific regions or countries enforce rules, fraudulent parties can easily relocate and seek out alternative jurisdictions (aka regulatory shopping [47]). Therefore, we must adopt global regulatory frameworks and allocate resources for law enforcement to investigate those engaging in fraudulent activities including cryptocurrency pig butchering scams.

2) Regulatory Clarity: We have detailed how scammers exploit government regulations and regulatory compliance to re-victimize their victims (§IV-D1). This is a common practice among many scammers who exploit the lack of knowledge among the population. Some even impersonate US government agencies such as the IRS [48] or more recently, the Federal Trade Commission (FTC). The FTC issued a warning against such scams after reporting losses exceeding $\$1.1b$ [49] [50].

As a solution, it is crucial to raise awareness about government procedures related to tax duties/evasion and anti-money laundering. Additionally, governments should establish clear processes and publicize them so that individuals can easily verify any suspicious email or request without having to incur significant costs by hiring a lawyer for assistance.

3) Trafficked Scammers as Victims: The involvement of law enforcement agencies in tackling these scams is essential. These scams are mostly carried out by organized groups rather than individuals acting alone [6] [4]. The exact nature and extent of these criminal networks remain uncertain. Though, there is evidence suggesting that human trafficking victims, under horrible circumstances, are enslaved and forced to contact potential victims and victimize them [6] [4].

To this end, we have two groups of victims: the victims of the scams and the trafficked scammers as victims. Consequently, fighting pig butchering and any other interactive scam begins with addressing the root cause: human trafficking. Without the enslaved trafficked "scammers", organized criminal groups would not be able to efficiently recruit members.

This is a massive issue globally considering that many of these groups are located in diverse jurisdictions, hence, international cooperation with law enforcement is a must.

B. Abused Third Parties

1) Cryptocurrency Platforms: Scammers often exploit well-known and major legitimate businesses such as Coinbase (13 scams) and Crypto.com (20 scams). By associating with reputable exchanges, scammers aim to gain the trust of their victims and present their schemes as legitimate. Despite the efforts of these platforms to prohibit fraudulent activities according to their terms and conditions, there appears to be oversight in effectively monitoring and enforcing these policies. For instance, the terms of service of Coinbase U.S. state the following: "*You may not use your Coinbase Account to engage in the following categories of activity: Fraud: Activity which operates to defraud Coinbase, Coinbase users, or any other person [...].*"

Despite exchanges stating a ban on these activities, some hold their users responsible for scams and fraud in certain situations such as when committed by third parties. In particular, the terms of service for crypto.com states:

"*1.3.2.4. You acknowledge that you and your digital assets may be subject to scams and other types of fraud perpetrated by third parties outside of our control. It is your responsibility to beware and protect yourself against such fraud.*"

It is imperative for exchanges to take on a more proactive role in preventing and detecting such scams, and overall, policing their platforms. Shifting the responsibility towards users while not countering third-party fraud is not a solution.

In addition to proactive measures, exchanges can play an active role in fighting crime with reactive measures. This includes freezing transactions and accounts belonging to criminal groups. In 2023, for example, the exchange OKX, following a collaboration with Tether and the U.S. Department of Justice, froze $\$225m$ in stolen USDT linked to an international organized crime group [51]. Exchanges constituting the largest intermediaries in the space play a vital role in promoting a safer environment. This can be done: 1. proactively by actively policing their platforms against possible exploiters, and 2. reactively by both enforcing platform rules on violators and collaborating with law enforcement.

2) Social Media Applications: Scammers are taking advantage of online social media applications to fabricate fake personas and contact potential targets. We find 39 of our 143 scams involve the use of social media apps for initiating contact and carrying out the scam (Table III). Many victims discovered the fraudulent trading/investment platforms only after encountering ads or posts on these apps. This raises the issue of apps allowing the advertisement of illegal or fraudulent content, creating an environment that is not secure for its users. Another issue that these apps must enhance is the user verification process during sign-ups to prevent identity theft and ensure that their users are genuine.

These platforms seem to act by managing the scams through policies that move the weight of responsibilities toward the end user. In fact, our analysis suggests that the ineffective countermeasures the platforms put in place allow scammers to abuse the trust victims can have in well-known platforms. The absence of an effective proactive approach allows these scams to proliferate and abuse the reliability of the platforms themselves. The combination of policy-based approaches and the effective detection of malicious content and users is, instead, an important deterrent.

C. Cryptocurrency Community

It is often hard for lay people to tell the difference between legitimate businesses and scams [52]. Cryptocurrency projects often promote themselves using language that is vague and focuses on returns rather than adding beneficial information for investors. More community work is needed to promote better marketing for new projects and encourage discourse above the hype. Education can help people grasp how the cryptocurrency market functions and stress the significance of authenticating sellers and platforms before placing trust in them.

VI. Conclusion

In this work, we analyze the narratives of cryptocurrency scams that have been collected by the California DFPI. Our work is the first to conduct a larger scale analysis of cryptocurrency pig butchering scam narratives. Some of our insights align with previous findings – our money lost estimates are in line with the IRS findings and our insight on victimization that continues after the scam "ends" is in line with common cybercriminal methods. We also demonstrate elements of novelty in how the scam was conducted like our diverse messaging methods and lure methods. We recommend that governments clarify existing regulations, third parties proactively manage their platforms, and the cryptocurrency community promote discourse above hype for legitimate projects.

Future work. The fraud we measure is largely off-chain (as is quite a lot of cryptocurrency fraud). In fact, much of it uses cryptocurrency as a ruse and accepts victim investments in fiat; thus it is harder to measure. We need a better community mechanism to receive and act on complaint narratives. The DFPI has started an interesting idea by publishing and updating this dataset. We strongly encourage other organizations (governmental or otherwise) around the world to contribute by publishing their own case narratives. We would particularly encourage the standardization of the reporting method which would aid in identifying relevant patterns and elements. Deepening our knowledge of the narratives may actually help researchers evaluate the taxonomy aspects as well as understand the modus operandi of scammers. This future focus could lead to effective identification methods.

In §II-B, we discuss work that collects data directly from criminals via victim advertisements. This is a great method for straightforward scams, but is less effective for understanding more complex scams which use a diversity of messaging platforms. We generally encourage more research into scam narratives to uncover large-scale patterns in the data.

ACKNOWLEDGMENTS

MO is supported by the UK Engineering and Physical Sciences Research Council [grant number EP/S022503/1]. AP is supported by the Dawes Trust.

REFERENCES

[1] US Federal Bureau of Investigation, "Internet crime report," 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

[2] C. Cross, "Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud," *Current Issues in Criminal Justice*, pp. 1–13, 2023.

[3] US Internal Revenue Service, "CI issues red flags, tips to avoid falling victim to pig butchering schemes during international fraud awareness week," 2023, https://www.irs.gov/compliance/criminal-investigation/ci-issues-red-flags-tips-to-avoid-falling-victim-to-pig-butchering- schemes-during-international-fraud-awareness-week.

[4] Chainalysis, "The chainalysis 2024 crypto crime report," 2024, https://go.chainalysis.com/crypto-crime-2024.html.

[5] M.-H. Maras and E. R. Ives, "Deconstructing a form of hybrid investment fraud: Examining 'pig butchering'in the united states," *Journal of Economic Criminology*, vol. 5, p. 100066, 2024.

[6] F. Wang, "Victim-offender overlap: the identity transformations experienced by trafficked chinese workers escaping from pig-butchering scam syndicate," *Trends in Organized Crime*, 2024.

[7] J. M. Griffin and K. Mei, "How do crypto flows finance slavery? the economics of pig butchering," 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235.

[8] J. M. Whittaker, S. Lazarus, and T. Corcoran, "Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (sha zhu pan)," *Journal of Economic Criminology*, vol. 3, p. 100052, 2024.

[9] M. Vasek and T. Moore, "There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams," in *Financial Cryptography and Data Security*. Springer, 2015, pp. 44–61.

[10] 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.

[11] P. Xia, H. Wang, B. Zhang, R. Ji, B. Gao, L. Wu, X. Luo, and G. Xu, "Characterizing cryptocurrency exchange scams," *Computers & Security*, vol. 98, p. 101993, 2020.

[12] X. Li, A. Yepuri, and N. Nikiforakis, "Double and nothing: Understanding and detecting cryptocurrency giveaway scams," in *Network and Distributed System Security Symposium (NDSS)*, 2023.

[13] E. Badawi, G.-V. Jourdan, and I.-V. Onut, "The "bitcoin generator" scam," *Blockchain: Research and Applications*, vol. 3, no. 3, p. 100084, 2022.

[14] J. Xu and B. Livshits, "The anatomy of a cryptocurrency pump-and-dump scheme," in *28th USENIX Security Symposium*, 2019, pp. 1609–1625.

[15] J. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek, "An examination of the cryptocurrency pump-and-dump ecosystem," *Information Processing & Management*, vol. 58, no. 4, p. 102506, 2021.

[16] M. La Morgia, A. Mei, F. Sassi, and J. Stefa, "The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations," *ACM Transactions on Internet Technology*, vol. 23, no. 1, pp. 1–28, 2023.

[17] M. Vasek and T. Moore, "Analyzing the Bitcoin ponzi scheme ecosystem," in *Bitcoin Workshop*. Springer, 2019, pp. 101–112.

[18] L. Nizzoli, S. Tardelli, M. Avvenuti, S. Cresci, M. Tesconi, and E. Ferrara, "Charting the landscape of online cryptocurrency manipulation," *IEEE Access*, vol. 8, pp. 113 230–113 245, 2020.

[19] K. Li, D. Lee, and S. Guan, "Understanding the cryptocurrency free giveaway scam disseminated on twitter lists," in *2023 IEEE International Conference on Blockchain*. IEEE, 2023, pp. 9–16.

[20] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on Ethereum: Towards healthier blockchain technology," in *2018 World Wide Web Conference*, 2018, pp. 1409–1418.

[21] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting ponzi schemes on Ethereum: identification, analysis, and impact," *Future Generation Computer Systems*, vol. 102, pp. 259–277, 2020.

[22] Z. Zheng, W. Chen, Z. Zhong, Z. Chen, and Y. Lu, "Securing the Ethereum from smart ponzi schemes: Identification using static features," *ACM Transactions on Software Engineering Methodology*, vol. 32, no. 5, jul 2023.

[23] C. F. Torres, M. Steichen, and R. State, "The art of the scam: Demystifying honeypots in Ethereum smart contracts," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1591–1607.

[24] T. Igarashi and K. Matsuura, "Scam token detection based on static analysis before contract deployment," *Workshop on Trusted Smart Contracts*, 2024.

[25] M. Fröwis, A. Fuchs, and R. Böhme, "Detecting token systems on Ethereum," in *Financial Cryptography and Data Security*. Springer, 2019, pp. 93–112.

[26] B. Mazorra, V. Adan, and V. Daza, "Do not rug on me: Leveraging machine learning techniques for automated scam detection," *Mathematics*, vol. 10, no. 6, 2022.

[27] F. Cernera, M. La Morgia, A. Mei, and F. Sassi, "Token spammers, rug pulls, and sniperbots: An analysis of the ecosystem of tokens in Ethereum and the Binance Smart Chain (BNB)," *USENIX Security Symposium*, 2023.

[28] P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, "Trade or trick? Detecting and characterizing scam tokens on Uniswap decentralized exchange," *ACM Conference on Measurement and Analysis of Computing Systems*, vol. 5, no. 3, pp. 1–26, 2021.

[29] A. Childs, "'I guess that's the price of decentralisation…': Understanding scam victimisation experiences in an online cryptocurrency community," *International Review of Victimology*, p. 02697580231215840, 2024.

[30] S. Agarwal, G. Atondo-Siu, M. Ordekian, A. Hutchings, E. Mariconti, and M. Vasek, "Short paper: DeFi deception – uncovering the prevalence of rugpulls in cryptocurrency projects," in *Financial Cryptography and Data Security*. Springer, 2023, pp. 363–372.

[31] M. Anderson, E. March, L. Land, and C. Boshuijzen-van Burken, "Exploring the roles played by trust and technology in the online investment fraud victimisation process," *Journal of Criminology*, p. 26338076241248176, 2024.

[32] California Department of Financial Protection and Innovation, "Crypto scam tracker," https://dfpi.ca.gov/crypto-scams/.

[33] A. Trozze, J. Kamps, E. A. Akartuna, F. J. Hetzel, B. Kleinberg, T. Davies, and S. D. Johnson, "Cryptocurrencies and future financial crime," *Crime Science*, vol. 11, pp. 1–35, 2022.

[34] G. Gibbs, *Analyzing qualitative data*, ser. The SAGE qualitative research kit. London: SAGE, 2007.

[35] F. Stajano and P. Wilson, "Understanding scam victims: seven principles for systems security," *Communications of the ACM*, vol. 54, no. 3, pp. 70–75, 2011.

[36] J. R. Norris, *Markov chains*, ser. Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, 1997.

[37] Z. Lwin Tun and D. Birks, "Supporting crime script analyses of scams with natural language processing," *Crime Science*, vol. 12, no. 1, p. 1, 2023.

[38] United Nations, "Online scam operations and trafficking: Into forced criminality in southeast asia: Recommendations for a human rights response," https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf, 2023.

[39] C. Cross and R. Layt, ""I suspect that the pictures are stolen": romance fraud, identity crime, and responding to suspicions of inauthentic identities," *Social Science Computer Review*, vol. 40, no. 4, pp. 955–973, 2022.

[40] C. Cross, ""I knew it was a scam": Understanding the triggers for recognizing romance fraud," *Criminology & Public Policy*, vol. 22, no. 4, pp. 613–637, 2023.

[41] C. Cross and T. J. Holt, "More than money: examining the potential exposure of romance fraud victims to identity crime," *Global Crime*, vol. 24, no. 2, pp. 107–121, 2023.

[42] G. A. Siu and A. Hutchings, ""Get a higher return on your savings!": Comparing adverts for cryptocurrency investment scams across platforms," in *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2023, pp. 158–169.

[43] M. T. Whitty, "Is there a scam for everyone? Psychologically profiling cyberscam victims," *European Journal on Criminal Policy and Research*, vol. 26, no. 3, pp. 399–409, 2020.

[44] P. Fischer, S. E. Lea, and K. M. Evans, "Why do individuals respond to fraudulent scam communications and lose money? the psychological de-

terminants of scam compliance," *Journal of Applied Social Psychology*, vol. 43, no. 10, pp. 2060–2072, 2013.
[45] State of California, "Digital financial assets law," 2023, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB39.
[46] European Parliament, Council of the European Union, "Regulation (EU) 2023/1114 of the european parliament and of the council of 31 may 2023 on markets in crypto-assets, and amending regulations (eu) no 1093/2010 and (eu) no 1095/2010 and directives 2013/36/eu and (eu) 2019/1937," 2023.
[47] M. Ordekian, I. Becker, and M. Vasek, "Shaping cryptocurrency gatekeepers with a regulatory "trial and error"," *Workshop on the Coordination of Decentralized Finance*, 2023.
[48] M. Bidgoli and J. Grossklags, ""Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing," in *2017 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2017, pp. 57–69.
[49] US Federal Trade Commission, https://www.ftc.gov/news-events/news/press-releases/2024/03/federal-trade-commission-warns-scammers-pretending-be-agency-staff.
[50] ——, https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today.
[51] OKX, "Following investigations by tether, the u.s. department of justice and us, tether voluntarily freezes 225m in stolen usdt linked to international crime syndicate," 2023, https://www.okx.com/learn/tether-okx-investigation.
[52] J. J. Si, T. Sharma, and K. Y. Wang, "Understanding user-perceived security risks and mitigation strategies in the web3 ecosystem," in *Conference on Human Factors in Computing Systems*, 2024.