The Dark Side of Crypto and Web3:

Crypto-Related Scams*

Lin William Cong† Kim Grauer‡ Daniel Rabetti§ Henry Updegrave¶

First Draft: August 2022; This Draft: February 2023

Abstract

We provide an overview of crypto-related scams, including investment scams, Ponzi schemes, and more recently, rug pulls that are commonly seen in Decentralized Finance (DeFi) projects. We then discuss data sources for studying Initial Coin Offering (ICO) scams, before examining the case of PlusToken, the largest crypto scam, AnubisDAO, the prototypical rug pull, and Luno's anti-scam initiative, a good prototype for other cryptocurrency exchanges and service entities to follow. User protection and education are crucial in preventing scams, despite the fact that they may require efforts from centralized entities and regulators.

JEL classification: G15, G18, G29, K29, K42, M41, O16..
Keywords: Cryptocurrencies, Cybercrime, Initial Coin Offerings, Rug Pull, User Protection.

*We are especially grateful to conference and seminar participants at the Interdisciplinary Challenges in Financial Data Science Conference, Pan-Asian Digital-Economy Meeting, Federal Reserve Cyber Monitoring Community of Interest Conference, The Economic Club of Memphis, European Securities and Markets Authority, 5th UWA Blockchain and Cryptocurrency Conference, Israel Money Laundering Authority Conference, University of Central Florida, University of Zurich (UZH) Blockchain Center, USAO-N.D. Cal. / U.S. DOJ Fraud Section / National Cryptocurrency Enforcement Team Cryptocurrency Fraud Seminar, and the US Treasury's Symposium on the Implications of Financial Technology for Banking for the insightful comments.Valerie Charlotte Hanke, Sanya Kohli, and Mahitha Penmetsa provided excellent research assistance. The authors acknowledge FinTech@Cornell, DEFT Lab, and Ripple's University Blockchain Research Initiative for research support.

†Cornell University and NBER. Email: will.cong@cornell.edu.
‡Chainalysis. Email: grauer@chainalysis.com.
§Tel Aviv University and FinTech at Cornell Initiative. Email: rabetti@mail.tau.ac.il.
¶Chainalysis. Email: henry.updegrave@chainalysis.com.

1 Overview

Scams represent the most significant form of cryptocurrency-based crime in terms of economic activity. In 2021, scams raked in nearly $10 billion worth of crypto from victims; as of August 2022, scams raked in nearly $7 billion in crypto.[1]

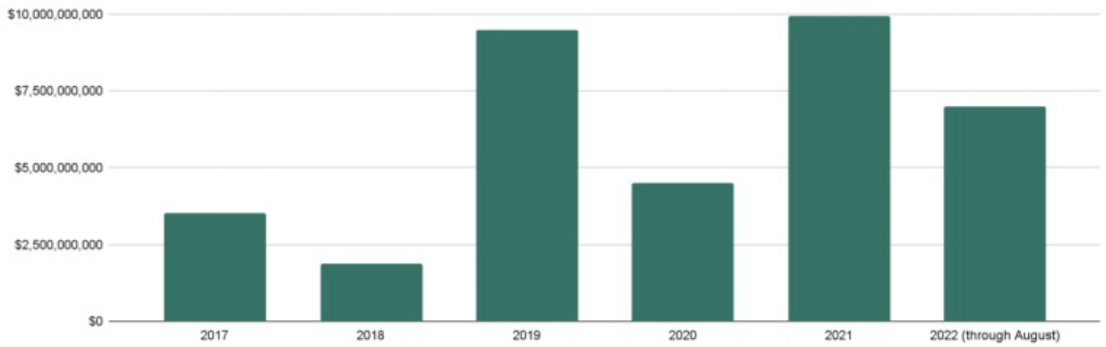

Figure 1. Total annual cryptocurrency value (in USD) received by scammers, 2107-2022.

Scams can take many forms, but most fall into one of the following categories:

- **Investment scams** are the most common category. In this type of scam, a scammer typically approaches users with a cryptocurrency investment opportunity promising extremely high returns and prompts them to invest by sending cryptocurrency from their wallets. Over time, the scammer may claim that the user's investment has grown in value, but users are typically unable to cash out. Often, these types of scammers posing as cloud mining companies users can "invest in" to receive a portion of mining proceeds;

- **Ponzi schemes** are similar to investment scams, but, rather than never paying out, they pay out fake returns from subsequent investors' deposits. Ponzi schemes bring in more revenue than any other type of cryptocurrency scam. The appearance of legitimate returns encourages users to invest more and recruit new investors, allowing the scheme to grow and gain hype. Users are often promised rewards for bringing in additional investors, which perpetuates this type of scam;

[1] Direct monetary losses from all fraud and financial scams around the globe are estimated to exceed $5 trillion annually (as of 2019), not to mention that victims often suffer depression, shame, and unemployment (Button, Lewis, and Tapley, 2009; Gee and Button, 2019; Phua, Sang, Wei, and Yu, 2022).

- **ICO scams** collect money by offering users to purchase a native token released by the company through an Initial Coin Offering (ICO). Users invest thinking their new coins will grow in value, but the scammers disappear with the investors' funds, leaving them with worthless crypto tokens. Though no longer very common, ICOs were once a popular way for nascent cryptocurrency projects to attract investment. As the ICO market grew quickly, many were willing to invest without performing much due diligence, creating a ripe environment for fraudulent ICOs;

- **Rug pulls** refer to scammers that portray themselves as legitimate cryptocurrency services or projects but shut down without returning users' funds. Like ICO scams, rug pulls often involve fraudulent, company-issued tokens purchased by interested users. Rug pulls are especially common in DeFi, given the relative ease of launching new DeFi tokens and the willingness of many to invest without performing due diligence. While anonymous developers launch many DeFi projects, many investors fail to audit a project's smart contract code or research the team;

- **Phishing scams** are widespread beyond the world of cryptocurrency and typically involve scammers spamming potential victims with emails that attempt to trick them into sending money or giving up information that can be used to access their financial accounts. In the world of cryptocurrency, scammers often send potential victims communications impersonating a cryptocurrency platform in an attempt to steal their password or wallet seed phrase or to get the victimes to connect their wallet to a malicious contract so that funds can be stolen. Scammers can usually get access to sensitive user information, such as email addresses after it has been lost in a larger data breach;

- **Sextortion or other blackmail scams** differ from the above-listed categories in that they do not require the victim to already be a cryptocurrency user. Blackmail scammers email potential victims claiming to have compromising information on them (often information of a sexual nature, hence "sextortion") and threaten to release this information unless they send the scammer a cryptocurrency payment. These threats are nearly always false. Like phishing scammers, blackmail scammers often either buy email addresses or obtain them via data breaches and spam many potential victims with threatening emails at once;

- **Giveaway or trust trading scams** typically claim to be conducting a cryptocurrency "giveaway" in which users are invited to send cryptocurrency in exchange for a larger amount later on — commonly double the initial amount. Once the user sends cryptocurrency, the scammer never returns any of it. Trust trading scammers usually promote their scams on social media, often by hacking into the account of a famous person and using their profile as a platform to increase their credibility.

Scammers generally take advantage of the hype and FOMO surrounding the cryptocurrency space, combined with the relative lack of knowledge the general populace has about how cryptocurrency works, both on a technical level and in terms of feasible financial returns. However, some cryptocurrency scams, such as sextortion, rely on other forms of emotional manipulation, including fear-mongering.

In addition to the billions of dollars in financial losses each year, cryptocurrency scams undermine faith in this emerging industry, which could scare off potential participants or result in restrictive regulations. Against this backdrop, the private sector should play a major role in stopping scams: Exchanges could proactively identify scams and prevent users from sending funds to scam addresses. While this would contradict the ethos of cryptocurrency in many ways, we argue that centralized services should take this action to protect their users and establish credibility in the system. We further argue that user and investor education remains urgent in the fast-evolving cryptocurrency and DeFi sectors.

2 Investment scams and rug pulls

Revenue from scams is typically dominated by investment scams, Ponzi schemes, and more recently, rug pulls.

Large-scale Ponzi schemes are especially interesting. They are rare but, if successful, can grow so large that they can single-handedly alter the scam landscape when and where they are active. For instance, of the $9.5 billion in total crypto scam revenue for 2019, over $2 billion came from the notorious PlusToken Ponzi scheme.[2] Likewise, $1.1 billion of 2021's $10 billion in scam revenue was collected by the Ponzi scheme Finiko, which largely targeted Russian-speaking countries.[3] In 2020 there was not a similarly dominant Ponzi scheme, and, as a result, the overall

[2]https://www.coindesk.com/markets/2020/11/27/chinese-authorities-have-seized-a-massive-4b-in-crypto-from-plustoken-scam/

[3]https://news.bitcoin.com/investors-lost-10000-on-average-to-russian-crypto-pyramid-finiko-poll-reveals/

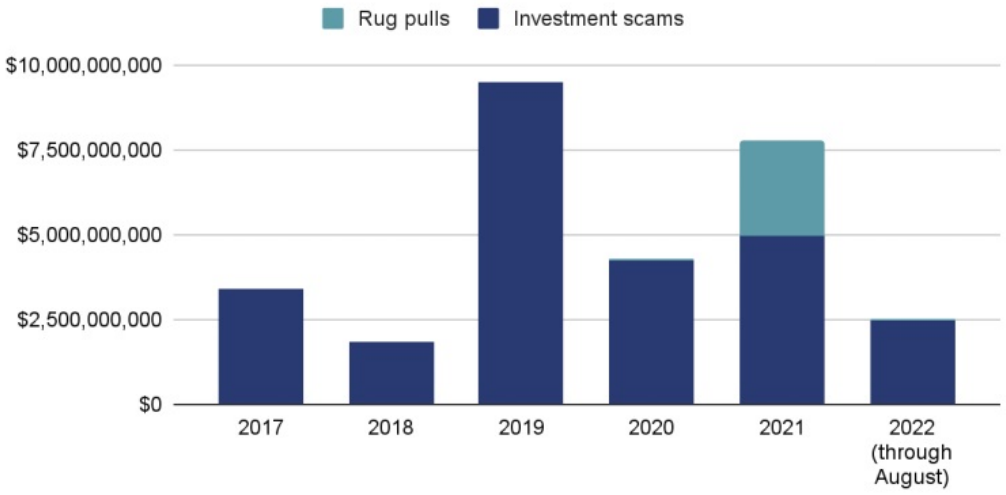

Figure 2. Total yearly cryptocurrency value received by investment scams and rug pulls, 2017-2022.

scam revenue was much lower. The same appears true until August 2022. While Ponzi schemes function very similarly to the more-common investment scams, we believe they tend to grow bigger because they pay out "returns" – money invested by new users – to early investors, allowing the schemes to spread through positive word of mouth. Investment scams, on the other hand, typically do not pay out false returns to new users.

Beyond investment scams and Ponzi schemes, a new type of scam has shown rapid growth recently: The rug pull. Rug pull revenue shot up from just $52 million in 2020 to $2.84 billion in 2021.

Rug pulls are most commonly seen in DeFi. More specifically, most rug pulls entail developers creating new tokens and promoting them to investors, who trade for the new token in the hopes that it will rise in value, in turn providing liquidity to the project. While this is generally how most DeFi projects start, in rug pulls, however, the developers eventually drain the funds from the liquidity pool, sending the token value to zero, and disappear.

Rug pulls are prevalent in DeFi because, given the right technical know-how, it is cheap and easy to create new tokens and get them listed on decentralized exchanges (DEXes) without a code audit. This is a crucial insight: No code audit means no checks and balances. This stands against the norm, which holds that decentralized tokens should be designed so that investors holding governance tokens can vote on how assets in the liquidity pool are used, making it impossible for the developers to drain funds out of the pool.[4] While code audits that would catch such vulnerabilities are the norm, they are not required in order to list on most DEXes, which contributes to an increase in rug pulls.

[4]https://coinmarketcap.com/alexandria/glossary/governance-token.

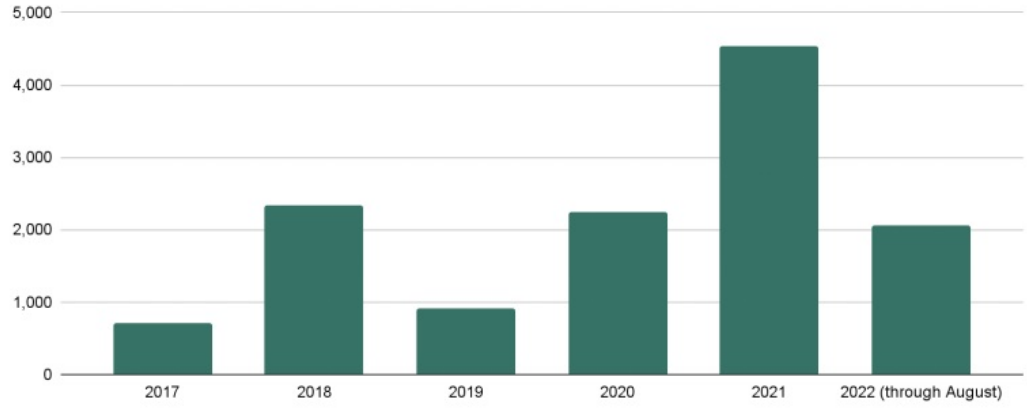

Figure 3. Total number of unique active scams, 2017-2021.

The number of unique active scams has risen in each of the previous three years. However, scam revenue has not grown but has fluctuated each year. This goes hand in hand with another trend we have observed over the last few years: The average lifespan of a financial scam is getting shorter and shorter.

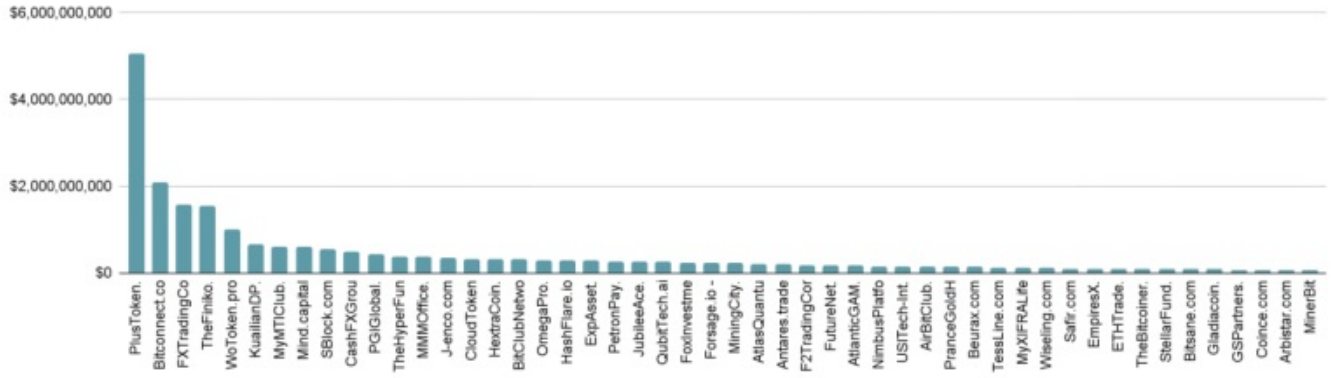

Figure 4. Top 50 scams by total value received since 2017.

The average financial scam was active for just 70 days in 2021, down from 192 in 2020. Looking back further to 2013, the average cryptocurrency scam was active for 2,369 days. Since then, the figure has trended steadily downwards.

One reason for this could be that investigators are getting better at investigating and prosecuting scams. For instance, in September 2021, the CFTC filed charges against 14 investment scams claiming to provide compliant cryptocurrency derivative trading services while, in reality, they had failed to register with the CFTC as futures commission

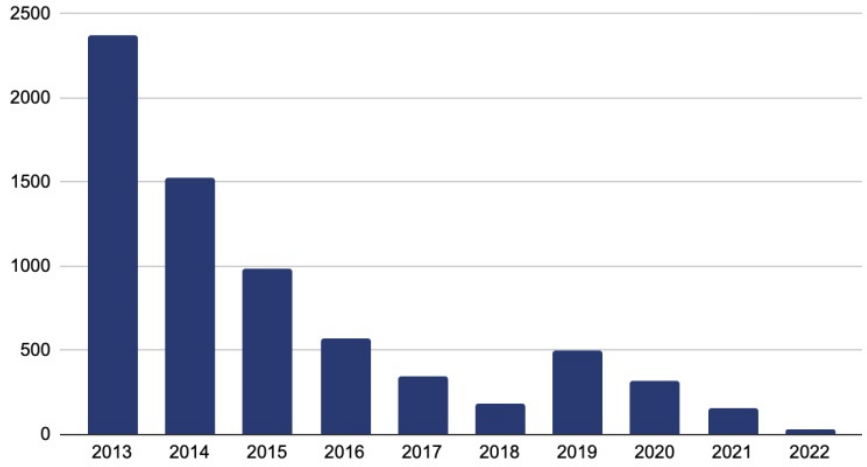

Figure 5. Average crypto scam lifespan, 2013-2022.

merchants.[https://www.cftc.gov/PressRoom/PressReleases/8434-21] Previously, these scams may have been able to operate undetected for a longer period of time. As scammers become aware of regulatory actions, they may feel more pressure to close up shop before drawing the attention of regulators and law enforcement.

3 Initial Coin Offerings (ICOs)

The ICO market boomed between 2017 and 2020, when more than 7,400 blockchain-based projects raised over 35 billion dollars across the world. The determinants of ICO success have been examined in several empirical studies (e.g., Adhami, Giudici, and Martinazzi (2018), Amsden and Schweizer (2018), Benedetti and Kostovetsky (2021), Davydiuk, Gupta, and Rosen (2020), Deng, Lee, and Zhong (2018), Howell, Neissner, and Yermack (2021), and Hu, Parlour, and Rajan (2018)), and include factors such as team size, white paper informativeness, and open coded GitHub account. Lyandres, Palazzo, and Rabetti (2021) find that social media and code activities are crucial determinants of ICO success and post-ICO performance in ways consistent with costly signaling. More importantly, the authors survey the challenges researchers face with ICO data quality.

3.1 Data quality

ICO information is scattered across a multitude of online sources, which aggregate various pieces of information regarding ICO characteristics, mostly by retrieving this information from ICO white papers. Consequently, various data sources cover subsets of attempted ICOs, and the degree of pairwise overlap in coverage varies widely, resulting in large differences in data composition and quality. More importantly, even if two data sources cover the same ICO, they often disagree on the values of ICO characteristics. Discrepancies among data sources are often on such a scale that using data from different sources may lead to dramatically different inferences by market participants.

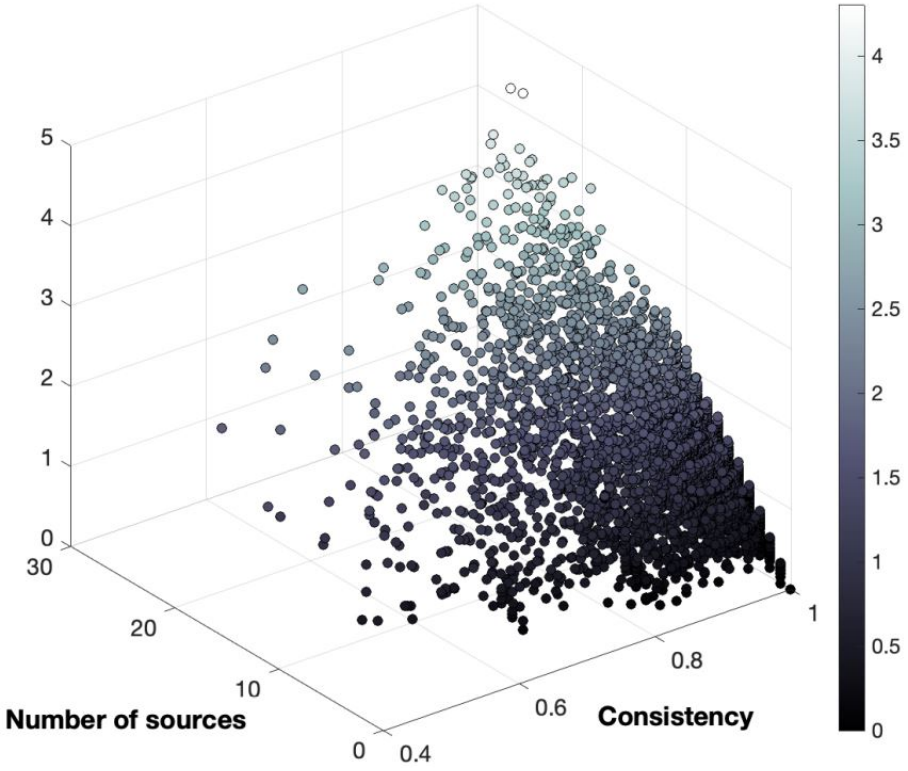

Figure 6. ICO Data Quality. Data source: Courtesy.

Figure 6 reports the overall ICO data quality as a function of the total number of sources and average consistency across sources for each ICO.[5] Darker points refer to low ICO data quality, while lighter points refer to high ICO data quality. The plot is based on more than 7,400 ICOs worldwide whose information was extracted from 11 ICO website

[5]Source: Courtesy (Lyandres et al. (2021)).

aggregators and suggests that information quality is increasing in data coverage. Concentrating on the portion of high-quality data, Lyandres et al. (2021) overturn several findings in the literature. For instance, they find that measure of ICO transparency—an indicator equaling one for ICOs that include a know-your-customer (KYC) provision — is significantly positively related to ICO success.

Understanding the determinants of ICO success and post-ICO performance is also important to understanding ICO failure. Especially given the high asymmetric information and excluding extreme cases, separating failed projects from scams is not trivial.

3.2 ICO scams

ICO token buyers typically have little financial knowledge and rely solely on scattered and imprecise ICO project information gathered by various data aggregators. Due to these shortcomings in the ICO market, it is generally deemed fraudulent. To make matters worse, very few ICOs are registered with the SEC, although most are likely to qualify as securities, meaning they exist outside of regulatory frameworks that protect investors.[6]

Assessing thousands of ICO-based token issuers, Phua et al. (2022) find that a large portion of ICO (about 40%) is fraudulent and estimates a total of 12 billion USD in ICO scams across the globe. ICO scammers target naive investors by mischaracterizing products, disseminating disinformation, and promoting false token rewarding campaigns, such as bonuses for early buyers and bounty campaigns. These misrepresentations are key ingredients for scammers to harvest naive investors. The findings of Phua et al. (2022) suggest that ICOs with misrepresentations are significantly more likely to be scams.

3.2.1 The role of ICO advisors

ICO advisors also play a fundamental role in ICO scams. ICO advisors, who are hired by issuers to launch token offerings, often work in multiple ICOs. If misrepresentation behavior is learned or passed through common advisors, the network position of an ICO should be related to its misrepresentation behavior. Consistent with this assumption,

[6]See https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

Phua et al. (2022) find that ICOs with higher Katz centrality in the network have more misrepresentations.[7] Surprisingly, advisors of misrepresented ICOs are not penalized. Instead, they often obtain additional advisory opportunities.

The assessments of freelancing ICO analysts also vary in quality and exhibit biases due to the reciprocal interactions of analysts with ICO team members (Barth, Laturnus, Mansouri, and Wagner (2021). The reciprocation rating happens as follows: An analyst sitting on the advisory board of ICO "A" gives a high rating to ICO "B," while an analyst sitting on the advisory board of ICO "B" reciprocates a high rating to ICO "A." Consequently, ratings predict ICO success, but imperfectly. Even favorably rated ICOs tend to fail when a greater portion of their ratings reciprocate prior ratings, and the market capitalization 90 days after listing on an exchange is smaller for tokens with more reciprocal ratings. These findings suggest that the failure of ICOs is not uniform but is related to measures of conflicts of interest.

3.2.2 Celebrities endorsement of fraudulent ICOs

Another common factor among fraudulent ICOs is the presence of celebrities in the marketing campaign. The marketing strategy often results in attracting naive investors to the ICO. For instance, a known ICO scammer, Moshe Hogeg, used a famous football player to promote Hogeg's Sirin Labs blockchain-based mobile phone.[8] The project eventually never took off, leaving investors with significant losses in just weeks from Sirin Lab's token issuance. Conversely, Hogeg amassed millions from investors and later invested the proceeds in financing other businesses, purchasing real estate, and acquiring the full rights of a popular football team in his home country.[9]

Overall, the evidence suggests that misrepresentation behavior is systemic within the initial coin offerings ecosystem.[10] Although holding promise as an alternative and relatively easy platform to raise capital for young start-ups worldwide, the proliferation of fraud spelled investors, decreasing valuations and eventually killing the market.

[7]Katz centrality computes the relative influence of a node within a network by measuring the number of the immediate neighbors (first-degree nodes) and also all other nodes in the network that connect to the node under consideration through these immediate neighbors (see https://networkx.org/documentation/stable/reference/algorithms/generated/networkx.algorithms.centrality.katz$_c$*entrality*.*html*).

[8]The extensive list of allegations against Hogeg includes misleading investors, theft, money laundering, and sexual assault (see https://www.coindesk.com/policy/2021/11/18/crypto-heavyweight-moshe-hogeg-reportedly-arrested-in-israel/).

[9]The SEC has warned that celebrity endorsements are often associated with ICO scams (see `https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos`).

[10]Evidence of information manipulation, in form of wash trades and tax-loss harvesting, has also been documented in other crypto markets (e.g., Amiram, Jørgensen, and Rabetti (2022), Amiram, Lyandres, and Rabetti (2021), Aloosh and Li (2021), Cong, Li, Tang, and Yang (2021), and Cong, Landsman, Maydew, and Rabetti (2022)).

4 Case Study: PlusToken, the $2 billion Ponzi scheme

PlusToken is one of the biggest cryptocurrency scams of all time, and also one of the biggest Ponzi schemes ever perpetrated in terms of dollars stolen — swindling 3 million investors out of nearly $5 billion. Nearly all of PlusToken's victims were ordinary retail investors, lured in by promises of double-digit monthly returns.[11]

Based in China, PlusToken presented itself as a cryptocurrency wallet that paid out monthly rewards of 10% or more of users' initial investment, claiming that rewards were generated from "exchange profit, mining income, and referral benefits." In reality, any rewards that were paid out came from new users' deposits. PlusToken also issued its own PLUS coin, which brought in investments from millions of users. PLUS coin would go on to be listed on several Chinese exchanges and hit a peak price of $350.

PlusToken's downfall came in June 2019, when six of the company's executives were reportedly arrested by Chinese authorities in Vanuatu. Soon after, the scam was exposed when users found themselves unable to withdraw cryptocurrency from their PlusToken wallets.[12] Some users who had invested their entire life savings were left with nothing. However, while their funds were frozen, cryptocurrency in wallets under PlusToken administrators' control continued to move in the coming weeks. Much was cashed out through independent over-the-counter brokers, with so much cryptocurrency hitting the market at once that the scammers may have temporarily driven down the price of Bitcoin.[13]

In total, Chinese media reports that over $3 billion worth of cryptocurrency were invested into PlusToken.[14] We tracked a total of 180,000 BTC, 6,400,000 ETH, 111,000 USDT, and 53 OMG (omisego) that went from scam victims to PlusToken wallets, equating to roughly $2 billion. Either figure would make PlusToken one of the largest Ponzi schemes to date.

[11] https://www.wsj.com/articles/cryptocurrency-scams-took-in-more-than-4-billion-in-2019-11581184800

[12] https://www.scmp.com/news/asia/australasia/article/3016604/six-chinese-nationals-wanted-beijing-internetscam-arrested.

[13] https://blog.chainalysis.com/reports/plustoken-scam-bitcoin-price/.

[14] https://bitcoinmagazine.com/articles/how-the-plustoken-scam-absconded-with-over-1-percent-of-the-bitcoinsupply.

4.1 Relentless self-promotion: How PlusToken reached millions of victims

One of the most remarkable things about PlusToken was its aggressive marketing strategy. The PlusToken scammers convinced millions of people to invest — mostly in China, Korea, and Japan — but even some as far away as Germany and Canada.

Dovey Wan, a noted expert in the Chinese cryptocurrency industry, provided a great deal of insight into PlusToken's promotional strategies in a 2019 interview with Bitcoin Magazine.[15] She described how PlusToken reached these people primarily through public groups on China's most popular messaging app (WeChat), where they heavily promoted their promise of 10-30% returns. She further emphasized that PlusToken targeted ordinary people without a considerable background in cryptocurrency, which helped fuel the scam. By promoting not only its product but also beginner-level educational materials on how to purchase Bitcoin, PlusToken targeted and exploited investors with low levels of cryptocurrency sophistication.

Figure 7. Plus Token Campaign. Credit: AZCoinNews

To further drive legitimacy, PlusToken hosted several in-person meet-ups and conferences to educate attendees on the company and on cryptocurrency as a whole. They also took out ads in supermarkets and other physical spaces.

[15] https://bitcoinmagazine.com/articles/how-the-plustoken-scam-absconded-with-over-1-percent-of-the-bitcoinsupply.

The PlusToken app itself was another marketing channel. In addition to a slick interface that let users easily convert Chinese yen into Bitcoin, Ethereum, and PLUS, the app also featured a gamified referral program in which users were rewarded for convincing others to sign up. In 2019, one of PlusToken's founders attended a charity event organized by the then Prince Charles of England, which further bolstered PlusToken's image and underscored just how significant the scope of the scam had become.

Overall, PlusToken's marketing strategy sought to achieve this massive scope via three tactics:

- Present cryptocurrency novices with a too-good-to-be-true high-yield investment opportunity;
- Spread their message far and wide through several online marketing channels, including customer referrals;
- Project the image of a legitimate, promising cryptocurrency startup by allowing users to see the "employees" behind the company — this tactic appears to have been particularly effective in maintaining the company's air of legitimacy even as rumors of a scam surfaced prior to users being locked out of the PlusToken app.

Law enforcement agencies and regulators should be on the lookout from now on, as other scammers may try to imitate PlusToken's brazen strategy.

4.2 How the PlusToken administrators utilized mixers, OTC brokers, and more to launder and cash out funds

Of the $2 billion that victims sent to PlusToken, some were paid out to early investors, presumably to maintain the illusion of high returns while PlusToken presented itself as a legitimate company. In many cases, it is difficult to tell whether transfers made by PlusToken were going to those early investors or to wallets under their own control. Nonetheless, we have tracked roughly 800,000 ETH and 45,000 BTC that we can definitively say the scammers transferred to their own wallets to launder. They have cashed out at least 10,000 of that initial 800,000 ETH, while the other 790,000 ETH has been sitting untouched in a single Ethereum wallet for months.

The flow of the 45,000 stolen Bitcoin is more complicated. So far, roughly 25,000 of it has been cashed out, while the other 20,000 is currently spread out across more than 8,700 cryptocurrency wallets, which speaks to the high level of effort the scammers put into obfuscating the movement of funds. The scammers have transferred Bitcoin more than

24,000 times, using more than 71,000 different wallets, and that is not even counting cash outs or transfers to off-ramps such as exchanges.

Many such transactions were conducted through mixers like Wasabi Wallet, which utilizes the CoinJoin protocol to make it more difficult to trace the path of funds. An example is in the Chainalysis Reactor in Figure 8.[16] Here, the funds are split off into large groups of new unique wallets and re-consolidated later, an activity typical of a mixer.

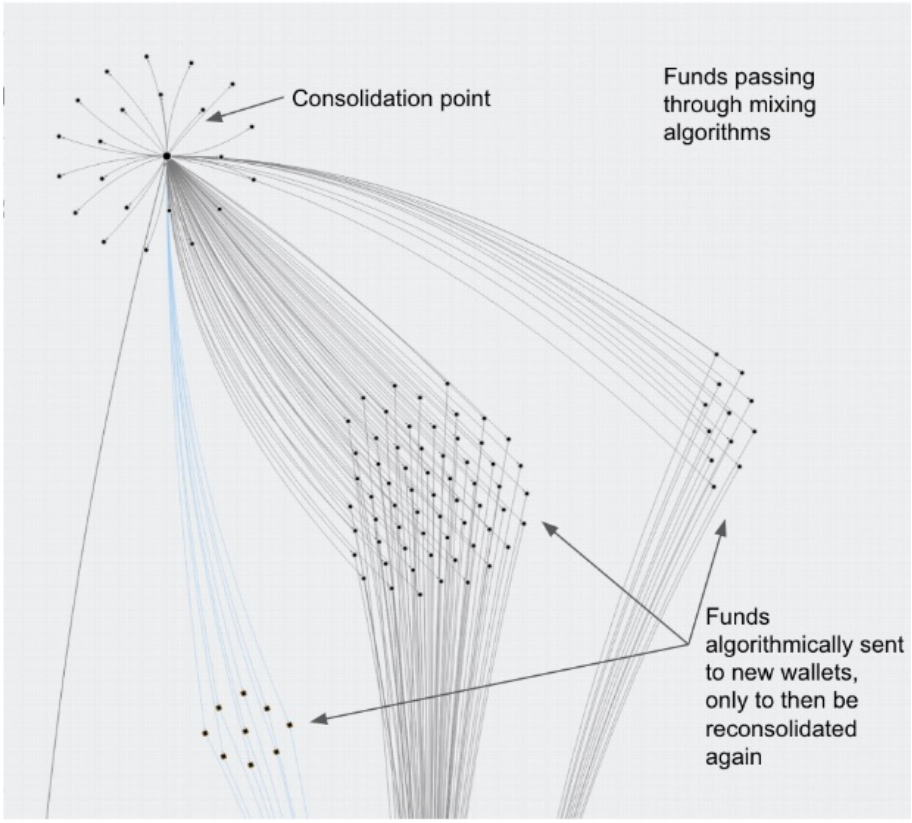

Figure 8. Funds Split

The graph below is a great example of the PlusToken scammers' obfuscation attempts. The funds start in the wallet in the upper left-hand corner and move to the right. Diagonal movements represent a change in the type of service used, while vertical movements represent the use of a mixer.

In the end, the funds moved to the wallet of an OTC broker operating on Huobi to be liquidated – that is how nearly all of the funds so far have been cashed out. For reference, over-the-counter (OTC) brokers facilitate trades between individual buyers and sellers who cannot or do not want to transact on an open exchange. OTC brokers

[16]https://www.chainalysis.com/chainalysis-reactor

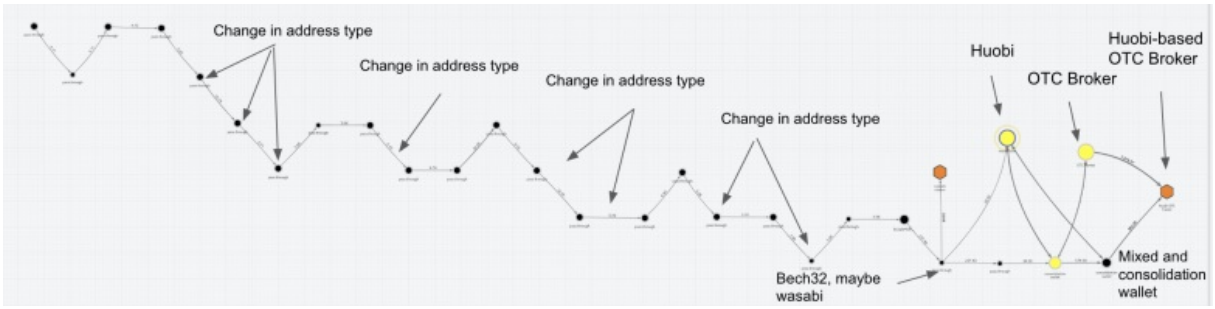

Figure 9. Obfuscation Attempts

are typically associated with an exchange but operate independently. Traders often use OTC brokers if they want to liquidate a large amount of cryptocurrency for a set, negotiated price.

Some OTC brokers have significantly lower KYC requirements than most exchanges, which can make them attractive to criminals like the PlusToken scammers. Compliant exchanges monitor transactions and keep customer information on file so that they can report suspicious activity and comply with subpoenas from law enforcement. But OTC brokers play by different rules. While many are legitimate, others take advantage of lower KYC requirements to offer services to users with illicit funds. Some even specialize in the movement and laundering of criminal money, as we explore in more detail in our discussion on money laundering.

Figure 10. Plus Token CEO meets the royal family

The continuing movements of PlusToken funds following the arrests suggest that some of the scam's administrators remain free. Many are especially curious as to the location of Leo, the enigmatic man who presented himself as PlusToken's CEO and made many videos promoting the company. Leo also appeared at several PlusToken events and even managed to snap a photo with Princes Charles of the British royal family at a charity event, which PlusToken soon used in promotional materials.

As of late 2020, while 27 PlusToken administrators and executives are reported to have been arrested, Leo's whereabouts and full name remain unknown.[17] The South China Morning Post reports that Chen Bo, one of the scam's founders, was sentenced to 11 years in prison and ordered to pay a large fine.[18]

5 Case Study: AnubisDAO, the prototypical rug pull

AnubisDAO, a scam that duped investors out of $58 million, provides an excellent example of how rug pulls in the DeFi ecosystem work.

Figure 11. AnubisDAO's Twitter banner. Credit CryptoHubK.

AnubisDAO launched on Thursday, October 28, 2021, claiming it planned to provide a decentralized, free-floating currency backed by a basket of assets. With little more than a DOGE-inspired logo – the project had no website or white paper, and all of its developers went by pseudonyms – AnubisDAO raised nearly $60 million from investors practically overnight, all of whom received the project's ANKH token in exchange for funding the project's liquidity

[17] https://cointelegraph.com/news/27-key-execs-at-plustoken-scam-are-reportedly-arrested

[18] https://www.scmp.com/economy/china-economy/article/3112115/chinese-cryptocurrency-scam-ringleaders-jailed-us225-billion

pool.[19] But a mere 20 hours later, all the funds raised, primarily held in wrapped Ethereum (wETH), disappeared from AnubisDAO's liquidity pool, moving to a series of new addresses.

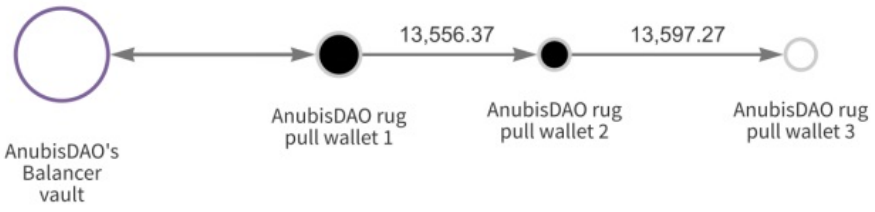

Figure 12. How AnubisDAO scammers removed investor funds from the protocol's liquidity pool.

We can see these transactions on the graph above. AnubisDAO used contracts created through Balancer's Liquidity Bootstrapping Protocol to receive and hold the wETH investors sent to their liquidity pool in exchange for ANKH tokens. However, the address that deployed the liquidity pool contract was already in possession of the vast majority of the liquidity provider (LP) tokens for that pool.[20] 20 hours after the sale began, the address that created the pool cashed out its massive holdings of LP tokens, allowing them to make off with nearly all the wETH and ANKH tokens in the pool. That transaction is shown in the Chainalysis Reactor screenshot (Figure 1.13).

The thief then moved that wETH through a series of intermediary wallets. Soon after this, the Twitter account that had acted as the public face of AnubisDAO went offline, and ANKH's value plummeted to zero.

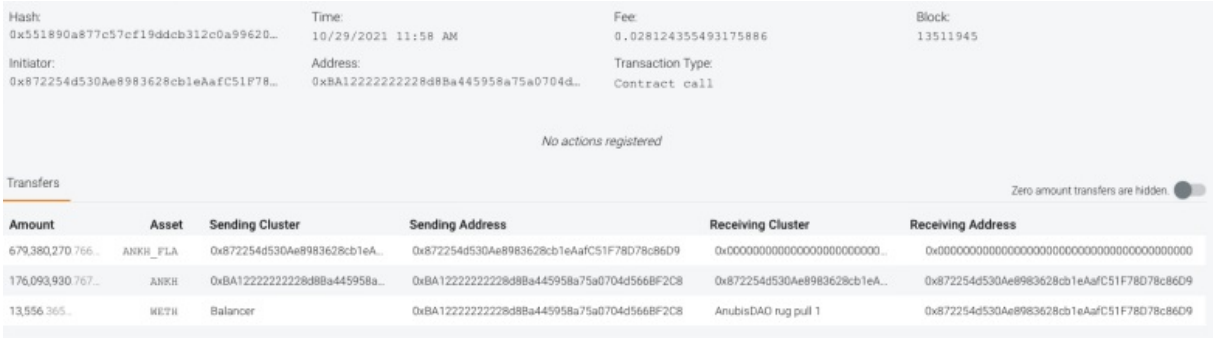

Figure 13. Intermediary wallets.

[19] https://decrypt.co/84924/anubisdao-investors-lose-60-million-in-alleged-rug-pull

[20] https://www.gemini.com/cryptopedia/liquidity-provider-amm-tokens#section-lp-tokens-and-crypto-liquidity-providers

Since the theft, there has been a great deal of finger-pointing and conflicting explanations.[21] One of the project's pseudonymous founding developers claimed that another founder, who had access to AnubisDAO's liquidity pool, is solely responsible for the rug pull, while that founder claims to have fallen victim to a phishing attack that compromised the pool's private keys. However, the evidence that the founder supplied does not support that theory. At this time, all signs point to a standard rug pull, but it is unclear whether or not all of the developers were in on it.

AnubisDAO should serve as a cautionary tale to investors evaluating similar opportunities. The most important takeaway is to avoid new tokens that have not undergone a code audit—a process by which a third-party firm analyzes the code of the smart contract behind a new token or other DeFi project and publicly confirms that the contract's governance rules are ironclad and contain no mechanisms that would allow for the developers to make off with investors' funds. They also check for security vulnerabilities that could be exploited by hackers. Solidity Finance is one example of a firm that provides code audits, but there are several others that are also considered trustworthy.[22] Investors may also want to be wary of tokens that lack the public-facing materials one would expect from a legitimate project, such as a website, white paper, or tokens created by individuals not using their real names.

6 Case Study: Luno's anti-scam initiative provides a model for other cryptocurrency exchanges

Mainstream cryptocurrency platforms like exchanges are in the perfect position to fight back against scams and instill more trust in cryptocurrency by warning users or even preventing them from executing those transactions. In fact, one popular platform did just that in 2021, and the results were extremely promising.

Luno is a leading cryptocurrency platform operating in over 40 countries, with an especially heavy presence in South Africa. In 2020, a major scam was targeting South African cryptocurrency users, promising outlandishly large investment returns. Knowing its users were at risk, Luno decided to take action in partnership with blockchain analysis firm Chainalysis.

[21] https://cointelegraph.com/news/investors-rug-pulled-after-pouring-57m-into-dog-themed-olympusdao-fork
[22] https://solidity.finance/

The first step was a warning and education campaign. Using in-app messages, help center articles, emails, webinars, social media posts, YouTube videos, and even one-on-one conversations, Luno showed users how to spot the red flags that indicate an investment opportunity is likely a scam, teaching them to avoid pitches that appear too good to be true.

Luno then went a step further and began preventing users from sending funds to addresses it knew belonged to scammers. In partnership with Chainalysis, Luno was able to proactively identify addresses with the scam in question and halt users' transfers to those addresses before they were processed. It was a drastic strategy in many ways — cryptocurrency has historically been built on an ethos of financial freedom, and some users were likely to chafe at a perceived limitation on their ability to transact. Still, through education, Luno established the trust necessary to sell customers on the strategy.

Luno first began blocking scam payments for South African users only in November 2020 and then rolled the feature out worldwide in January 2021. The plan worked, and transfers from Luno wallets to scams fell drastically throughout 2021.

Figure 14. Daily value received by scams from Luno, 30-day moving average.

The 30-day moving average daily transaction volume of transfers to scams fell 88% from $730,000 at its peak in September 2020 to just $90,000 by November.

Scams represent a huge barrier to successful cryptocurrency adoption, and fighting them cannot be left only to law enforcement and regulators. Cryptocurrency businesses, financial institutions, and blockchain analysis providers

have an important role to play as well. With this strategy, Luno took a courageous step towards establishing greater trust and safety in cryptocurrency, something we hope to continue seeing in the industry.

References

Adhami, S., G. Giudici, and S. Martinazzi (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business 100*, 64–75.

Aloosh, A. and J. Li (2021). Direct evidence of bitcoin wash trading. Working paper. Available at https://dx.doi.org/10.2139/ssrn.3362153.

Amiram, D., B. N. Jørgensen, and D. Rabetti (2022). Coins for bombs: The predictability of on-chain transfers for terrorist attacks. *Journal of Accounting Research 60*(2), 427–466.

Amiram, D., E. Lyandres, and D. Rabetti (2021). Cooking the order books: Information manipulation and competition among crypto exchanges. Avaliable at http://dx.doi.org/10.2139/ssrn.3745617.

Amsden, R. and D. Schweizer (2018). Are blockchain crowdsales the new "Gold rush"? Success determinants of initial coin offerings. *McGill University Working Paper*.

Barth, A., V. Laturnus, S. Mansouri, and A. F. Wagner (2021). The role of analysts in unregulated financial markets: Evidence from initial coin offerings Available at https://www.aeaweb.org/conference/2022/preliminary/paper/rddgyy8k.

Benedetti, H. and L. Kostovetsky (2021). Digital tulips? Returns to investors in initial coin offerings. *Journal of Corporate Finance 66*, 1–20.

Button, M., C. Lewis, and J. Tapley (2009). A better deal for fraud victims: Research into victimsÄô needs and experiences.

Cong, L. W., W. R. Landsman, E. L. Maydew, and D. Rabetti (2022). Tax-loss harvesting with cryptocurrencies. Working paper. Available at https://dx.doi.org/10.2139/ssrn.4033617.

Cong, L. W., X. Li, K. Tang, and Y. Yang (2021). Crypto wash trading. Working paper. Available at https://dx.doi.org/10.2139/ssrn.3530220.

Davydiuk, T., D. Gupta, and S. Rosen (2020). De-crypto-ing signals in initial coin offerings: Evidence of rational token retention. *Carnegie Mellon University Working Paper*.

Deng, X., Y. T. Lee, and Z. Zhong (2018). Decrypting coin winners: Disclosure quality, governance mechanism and team networks. *Shanghai Univesity of Finance and Economics Working Paper*.

Gee, J. and M. Button (2019). The financial cost of fraud 2019: The latest data from around the world.

Howell, S. T., M. Neissner, and D. Yermack (2021). Initial coin offerings: Financing growth with cryptocurrency token sales. *Review of Financial Studies 33(9)*, 3925–3974.

Hu, A., C. Parlour, and U. Rajan (2018). Cryptocurrencies: Stylized facts on a new investible instrument. *Financial Management 48(4)*, 1049–1068.

Lyandres, E., B. Palazzo, and D. Rabetti (2021). ICO success and post-ICO performance. *Management Science 68*(12), 8515–9218.

Phua, J. W. K., B. Sang, C. Wei, and G. Y. Yu (2022). Trust, but verify: The economics of scams in initial coin offerings. Available at http://dx.doi.org/10.2139/ssrn.4064453.