

Clemson University

TigerPrints

Media Forensics Hub Creative Inquiry Reports Watt Family Innovation Center Media Forensics
Hub

2023

Crypto Bestiary: A monstrous manual to the many fraudulent accounts involved in cryptocurrency scams and fraud.

Patrick Warren

Darren Linvill

Steven Sheffield

Jayson Warren

Leland Fecher

See next page for additional authors

Follow this and additional works at: https://tigerprints.clemson.edu/mfh_ci_reports

Authors

Patrick Warren, Darren Linvill, Steven Sheffield, Jayson Warren, Leland Fecher, Kate Tesh, Jack Taylor, Malia Fairbanks, Alexa Gubanich, Janna Gubanich, Sarah Meadows, Josephine Rohrer, Adrian Colaianni, Conor Pridnia, Ella Kea, Garret Kent, Kaitlyn Sammons, Phebe Webb, Justin Shay Easler, Josiah Lamont, Katie Batten, Parker Hundley, and Molly Sutton



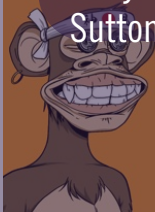
CLEMSON® UNIVERSITY

MEDIA FORENSICS HUB

Crypto Bestiary

A monstrous manual to the many fraudulent accounts involved in cryptocurrency scams and fraud.

Patrick Warren, Darren Linvill, Steven Sheffield, Jayson Warren, Leland Fecher, Kate Tesh, Jack Taylor, Malia Fairbanks, Alexa Gubanich, Janna Gubanich, Sarah Meadows, Josephine Rohrer, Adrian Colaianni, Conor Pridnia, Ella Kea, Garret Kent, Kaitlyn Sammons, Phebe Webb, Justin Shay Easler, Josiah Lamont, Katie Batten, Parker Hundley, Molly Sutton





Crypto Bestiary

Cryptocurrencies have fueled the growth of online fraud in various forms. They are poorly understood by many users, have value that shifts quickly and unexpectedly, and are easy to move in a digital world without borders. Cryptocurrency is seemingly purpose built as a tool for hucksters and scammers. The Federal Trade Commission claims that 46,000 people reported losing over a billion dollars in cryptocurrency to scammers in the first six months of 2021,¹ a figure only including those potentially few people have been brave enough to share that they have been victims. The world of cryptocurrency can be scary for the uninitiated.

One common way in which crypto-fraud is accomplished is through social media and the use of fake accounts. Some accounts purport to be crypto-fans, others make you believe they are experts in crypto-investment and are happy to help you uncover hidden riches. All of them, however, are seeking to take your money and leave you with nothing but fear and regret.

This crypto-bestiary will present you, the neophyte, six of the most terrifying of crypto-creatures seeking to steal your treasure. Heed what we tell you as a lesson, be wary of where you venture and watch for the signs.

¹ Fletcher, E. (2022, June 3). Reports show scammers cashing in on crypto craze. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>

Crypto Zombie

Terrain: All platforms, especially X (Twitter)

Purpose: Artificially inflate the perceived prominence of another social media account, giving the account greater credibility

Strengths: Low cost

Weaknesses: Easy to identify, only affective in large numbers

Number appearing: 100 - 100,000

Detection Difficulty: Easy

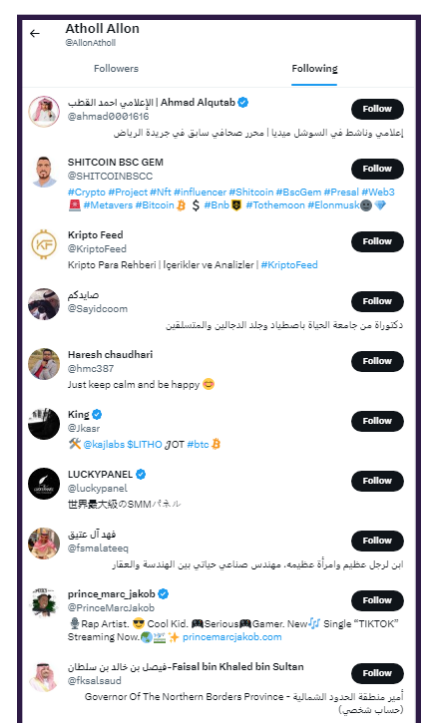
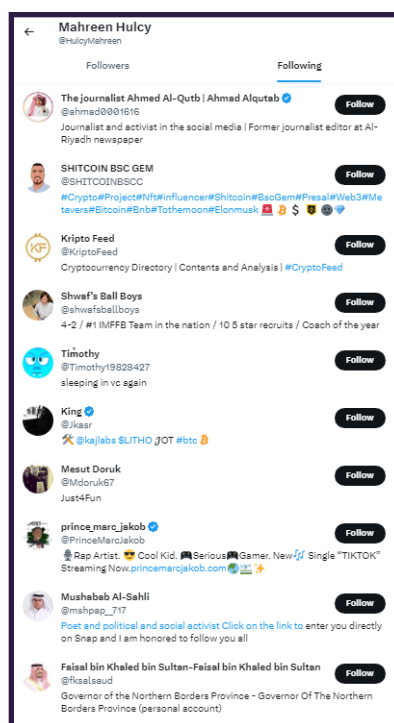
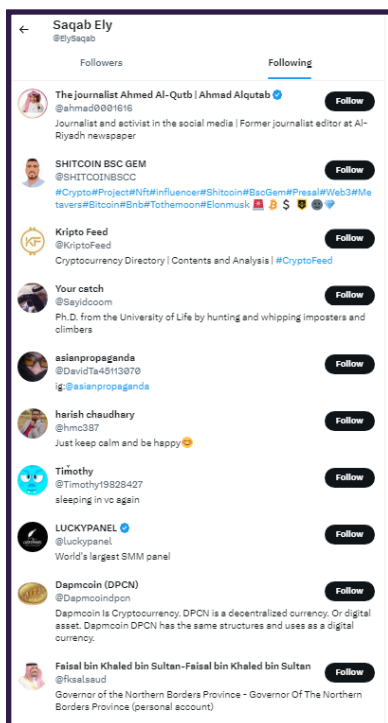
The crypto zombie is a mindless automaton, living its life in thrall to its many masters. Created as part of a global market, they exist to follow other accounts and their services are sold in online marketplaces to users hoping to make their account appear to be more popular. Powerless alone, zombies normally appear in packs of no less than 100, but often ranging in the many thousands. Their services can be purchased for mere pennies. They may follow a range of types of accounts (entertainers, influencers, start-ups, etc.), but given the importance of perception in the

crypto-marketplace, crypto related accounts make up a majority of the zombie's diet.

The crypto zombie's only power lies in its ability to raise the follower count of its masters. They often take no actions apart from following, leaving a shell of an account with no posts and no followers of their own. As a result, individual zombies are little threat. In large numbers, however, they can make other crypto scam accounts appear very powerful.

Examples

Crypto zombies are common and examples are easy to find. They often come in pods. If we examine, for instance, accounts following @KriptoFeed, the Twitter account for a Turkish language, crypto news site, we find at least one pod of zombies. These accounts were all created recently, have not posted or liked any content, and together follow an eerily similar set of other accounts. These include additional crypto related accounts (e.g. @SHITCOINBSCC) but also accounts belonging to self-described social media influencers, online games, adult accounts, CEOs, and at least one Saudi prince.



Passive Income Siren

Terrain: All platforms, especially Instagram

Purpose: Direct scam of individual users

Strengths: Often appear genuine

Weaknesses: Direct exposure to the truth

Number appearing: Solitary

Detection Difficulty: Challenging

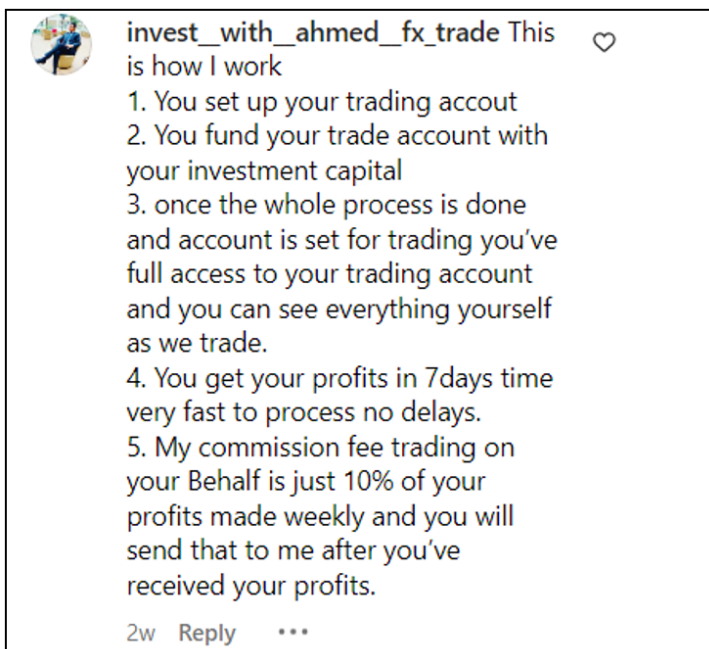
The siren prey on naïve and reckless explorers of the internet, relieving them of their wealth and leaving them no reward and no recourse. These accounts take on the appearance of professional and often attractive men or women who are offering their services as financial mentors and investment strategists. They promise to share secret knowledge regarding how to build wealth through crypto currency investment and require only a small initial

investment. Sirens share pictures of happy clients, often with new cars or wads of cash, supposedly obtained thanks to the wise council of the siren. Many posts give quotes from clients, showering the siren with praise regarding how their help has improved the investor's life and fortune. Sirens also intermittently post inspirational images with messages such as "Success is a decision" and "It's time to transform your life."

The siren's call, however, is a dangerous lie.

Sirens offer no proof their clients or success is real beyond that which is easily falsified. Identical stories of satisfied "investors" are often, in fact, shared by multiple sirens as they not only steal from their prey, but also from each other. Images of the sirens themselves are similarly false, normally taken from genuine attractive internet denizens or stock photo models.





Reach out in any way to a crypto siren and they will make what seems a straightforward and honest business proposal. Send them a small stake of money and they will invest it on your behalf. Weekly withdrawals are often "guaranteed" from that point forward and you will be on your way to financial security. It is, in fact, a crypto version of a very old scam. Just like past frauds, however, once the crypto siren has your money you will never hear from them again.



Examples

Sirens are easy to identify once you understand what you are looking for. Search “professional crypto trader” on Instagram and you will quickly find a long list of accounts with open DMs and far more emojis in their bio than what you would expect from a typical financial advisor. Careful image searching of their profile images unmasking the siren beneath.

The siren Lisa Donald, for instance, is actually Anna Maria Göbel, a very real attorney in Germany who practices family law. Siren Rebecca Donald, however, is in reality Amanda Silva Vieira, a software engineer living in Brazil. Crypto sirens not only steal money, they also steal identity.

 <p>trade_with_lisa_donald_099 Follow</p> <p>175 posts 653 followers 5,976 following</p> <p>BINARY TRADE EXPERT Investment Management Company EXCELLENT TRADING SIGNAL 📈 ACCOUNT MANAGER 📊 GOD FIRST ✨ PROFESSIONAL CRYPTO TRADER 📈 WEEKLY WITHDRAWAL GUARANTEED 📈 100%PAYOUT ✨ 24/7 AVAILABILITY</p>	 <p>Anna Maria Göbel · 3rd Fachanwältin für Familienrecht Talks about #ehe, #recht, #familie, #finanzen, and #trennung North Rhine-Westphalia, Germany · Contact info 832 followers · 500+ connections</p>
 <p>mrs.rebecca.donaldfx Follow Message</p> <p>206 posts 2,326 followers 7,495 following</p> <p>professional crypto trader 📈 Investment Management Company Forex Expert / Binary Trader 📈 ENTREPRENUR EXPERTTRADER BITCOIN MINER FOREX TRADER TRADER 9 YEARS OF EXPERIENCE DM LETS EARN HUGE PROFIT www.cash.app</p>	 <p>Amanda Silva Vieira (She/Her) · 3rd Software Engineer at Clutch & Co-Founder at AfroPython Porto Alegre, Rio Grande do Sul, Brazil · Contact info 500+ connections</p>

Satoshi's Hydra

Terrain: All platforms

Purpose: Various scams

Strengths: Appearance of legitimacy

Weaknesses: None

Number appearing: N/A

Detection Difficulty: Challenging

The Hydra is a rare but powerful beast. Unlike other crypto beasts, the hydra is not made up of a single account, but many accounts working as one. Destroying a single account, or even many, will not kill the hydra as they will simply create more to replace those that are removed.

Hydras exist for many reasons. Often, they are created to publicize a new coin or NFT product. Others engage in investment scams similar to the Passive Income Siren. Hydras are composed of many accounts, one central account which is backed by a cast of supporting accounts. The central account is the main player in the scam being perpetrated and the backing accounts purport to be real users who boost the central account and lend it credibility through positive posts and reposts. Creation of a hydra is a major undertaking, but they can be highly convincing and lucrative for their architects.

Example


By any standard, Klava Petina is an ancient Hydra, spreading her influence on Facebook since at least 2017. Originally from Moscow but now living in London, Klava purports to be an expert in online trading, a senior account manager at a firm called SwipeFxTrade. Klava's timeline is full of posts from thrilled investors, all sharing photos of happy families with new cars and new homes purchased thanks to Klava's investment help. These posts are themselves filled with dozens of likes, hearts, and comments from others who have had similar experiences. The posts are all thoughtful and professional and the accounts, themselves, from a cursory analysis, all appear genuine. Their own timelines share photos and moments from what appear to be lives well lived.

Klava herself, however, is a fraud, as are nearly all of the accounts engaging with her. Klava's profile image is stolen from Nadin Strelets, a successful Russian publisher and not an expert in crypto investment strategies. Her grateful admirers are all carefully managed fabrications. But look below the surface of these accounts and the reality falls apart and their persona are also stolen. Even wedding photos for these accounts fail to receive any engagement from real people. The only thing real about Klava Petina is the money she takes.



Klava Petina

 Add Friend

 Message



Klava Petina is 🥳 feeling positive.

April 12 · 🌐

Congratulations to Mr Davila on your new house 🏡. If you are positive, you'll see opportunities instead of obstacles. I'm glad to see smile on my clients faces. Well done i really appreciate this feedback from you. it keep me moving 🙌. Keep a smile on your face. Keep a spring in your step. Congratulations once again on your platinum level 🥳🥳🥳🥳



🥳🥳 53

76 comments

👍 Like

➦ Share



Ricky Cardona
Congratulations 🥳🥳🥳

Like 4w



Sherry Miles is 🥳 feeling blessed with Klava Petina.

June 3 at 8:59 AM · 🌐

Yesterday was a very great day in my life that i won't forget i was happy and grateful for everything that has happened i always had a dream of having my own car but yesterday i got one for my self

Congratulations to me on my first car 🚗

I was refered by a friend who's also a member of this platform we where having a conversation one day and she told me about Bitcoin and how she has been earning alot of money in this company i feel it was an amazing idea so i took a step t... See more



🥳🥳 49

90 comments

Shriekers of Szabo

Terrain: All platforms, primarily X (Twitter)

Purpose: Artificially inflate the perceived prominence of a social media post, giving that post greater reach and greater credibility

Strengths: Low cost

Weaknesses: Easy to identify, only affective in large numbers

Number appearing: 25 - 25,000

Detection Difficulty: Easy

Related to crypto zombie, shriekers are often created in large batches and their services sold in a global market. Like the zombie, their purpose is to make another account appear more popular and credible than reality dictates, a valuable service in many arenas but especially in the world of crypto. Shriekers' exist solely to repost and like individual messages, a normally accomplished in large numbers.

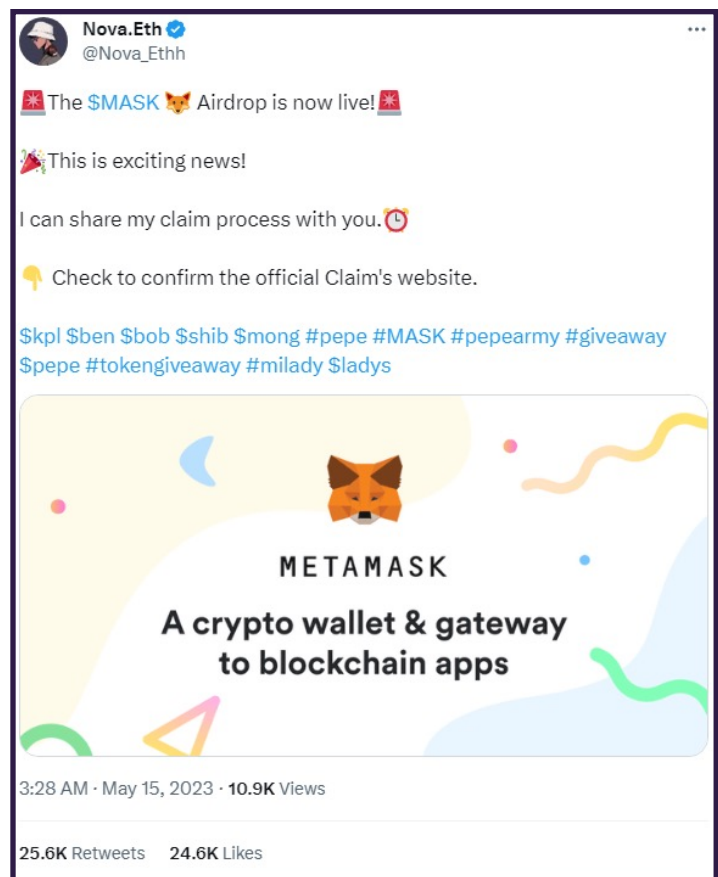
Shriekers are among the most common of crypto beasts. They are cheap to create and cheap to employ. Little effort goes into building shriekers. They are not artisanal, but constructed algorithmically and rarely are they given unique persona. Their lot in life does not require charisma, however, as they exist solely to increase engagement numbers and not to engage in their own frivolity.

Social media companies monitor their platforms for shriekers and they are sometimes culled in large numbers. Their loss means little to their human puppet-masters, however, as they can be quickly replaced.

Example

The blue-check mark Twitter account @Nova_Ethh has relatively few followers. It normally tweets once a day about crypto currency or finance and most of its tweets receive little engagement, perhaps one or two likes. Periodically, however, it will have a tweet with tens of thousands of retweets and likes. These tweets often have equal numbers of likes and retweets, a clear sign Shriekers have been active. Organic Twitter activity normally results in more likes than retweets on any given tweet.

One of these tweets occurred on May 15, 2023 when @Nova_Ethh tweeted an announcement regarding a \$MASK Airdrop. Nearly all of the 25,627 accounts which retweeted this message are shriekers. Only a few dozen have more than ten followers, and 25,015 had one or fewer. Nearly all of the messages from these shriekers are related to very similar airdrops.



Token Toady

Terrain: X (Twitter)

Purpose: Mass contest entry

Strengths: Symbiosis

Weaknesses: Fake contests

Number appearing: 10 - 100

Detection Difficulty: Easy

The toady is a special form of crypto beast, preying not on the unwary, but feeding symbiotically from the crypto currency industry itself. Often created to do the bidding of real Twitter users, in reality the Toady serves many masters.

In the cryptic and ancient tomes of Twitter known as “Terms of Service” lie a little read but often followed code known as the “[Guidelines for Promotions on Twitter](#).” This code allows users to hold contests on Twitter in which they may offer prizes in exchange for “Tweeting a particular update, for following a particular account, or for posting updates with a specific hashtag.” While the code explicitly discourages users from creating multiple accounts to enter such contests, in practice it emboldens just such behavior. Use of multiple accounts for contest entry purposes is, in fact, a win-win-win. The contest receives more engagement, the entry accounts improve their creators’ chances of winning, and Twitter itself has more daily active “users.” Those that follow Twitter’s rule and enter contests only once, however, are more likely to lose.

It is for this reason that toadies proliferate on Twitter. These accounts are created by real users and then follow a simple script to enter engagement contests. Obviously, engagement contests are not exclusive to crypto Twitter, it’s possible to find contests on the platform

helping to promote everything from fast food to K-pop. They are especially common on crypto Twitter, however, as they help create buzz for new tokens, and in crypto, perception is everything. The fractions of coin offered for winning these contests are highly sought after.

Examples

Denizens of [Github](#) offer free tools to create toadies capable of entering “more than 1000 giveaways per day.” They aren’t hard to uncover on Twitter, just look for crypto #giveaway contests and find the accounts that have followed the contest entry rules by retweeting the post. The threads are full of burner accounts and bots.

\$Doge Demon

Terrain: All platforms, primarily X (Twitter)

Purpose: Repurpose followers

Strengths: Operated by real humans and appears genuine

Weaknesses: Angry followers

Number appearing: Solitary

Detection Difficulty: Challenging

The demon is a powerful beast, often wielding great powers of persuasion and engagement. Like other beasts, demons may have a variety of motivations, but many involve cryptocurrencies given the opportunities there to toy with the minds of humans and take financial advantage of them. Demons are particularly dangerous because they are in many ways genuine. The demon may be, in some ways, what it says it is. Demons, however, are born from a lie.

A demon's power is to corrupt an existing social media account, bending it to the demon's will and possessing it with the demon's own form. This process of possession starts when a human user obtains an existing account, either one the user already maintains or, more likely, a hacked account purchased on the mysterious "dark web." The account is then stripped of its previous identity, everything from the profile description to previous posts are removed until only the followers remain. The more followers left, the more powerful the demon may become. The human user then replaces the previous identity with a persona of their choosing, one which then has access to all of the unwitting followers of the account's previous form. Those followers then become subject to all forms of fraud and influence available to the diabolical demon.

Example

The Twitter account @krisspax is a Demon crypto influencer. His Twitter account, with tens of thousands of followers, posts a mix of viral videos and thoughts on crypto investment. It also links to Kriss's YouTube channel, where he dispenses crypto currencies related news and advice, building a following as a crypto influencer.

Prior to November, 2022, however, @krisspax was called @conspiraboomers, a Twitter account which shared "Crazy boomer conspiracies." It is doubtful Kriss controlled the account in this period, and there is some evidence the previous owner sold the account. We don't know for certain how Kriss obtained the account, but we do know @conspiraboomer's followers did not choose to receive Kriss's crypto advice in their daily feed.

