Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies

Vilma Luoma-aho[1], Johnny Botha[2] and Miriam Hautala[1]
[1]School of Business and Economics, University of Jyvaskyla, Finland
[2]Council for Scientific and Industrial Research, Pretoria, South Africa

Vilma.luoma-aho@jyu.fi
jbotha1@csir.co.za
miriam.a.hautala@jyu.fi

Abstract: As deepfakes and scams online become more common, many individuals, organizations and nation-states struggle to maintain trust and remain credible sources for their stakeholders. Increasingly algorithms shape the digital information landscape, choosing what content is displayed and deepening the individual silos of information seeking. Recently it has been suggested that the best efforts to combat misinformation are not to try to stop its spread but through understanding the vulnerabilities on which it lands in the individual receiving the false information. There is an urgent need to investigate the mechanisms and extent of deception in online environments, as little is known about these specific vulnerabilities that then cause individuals to become victims for online scams. In the digital environment, different vulnerabilities exist yet they result from siloed studies in specific contexts. This paper starts by categorizing the different levels on which digital communication may be vulnerable. Further, this research asks how these vulnerabilities are utilized and what persuasion tactics are at use when crypto scams are concerned. Building on the persuasion principles, this paper analyzes three recent highly successful online scams. The findings conclude that social proof and scarcity were most used influence mechanisms, suggesting that scam prevention needs to understanding the vulnerabilities on which these influence mechanisms build.

Keywords: Digital vulnerabilities, Misinformation, Persuasion tactics, Crypto currency, Scams

1. Introduction

New AI technologies of the post-truth era (Lewandowsky, Ecker, & Cook, 2017) enable the creation of increasingly convincing fake and false content. As nations and institutions are "unable to control the spread of either true or false information" online (Canel & Luoma-aho, 2019), vulnerability to digital scams and propaganda is increasing online. Furthermore, such lack of control causes fragility, reduces collaboration, and deepens information vacuums of lacking or missing information (Rhodes, 2022; Pamment, Nothhaft, Agardh-Twetman, & Fjällhed, 2018; Alaraatikka, Koistinen, Kaarkoski, Huhtinen, & Sederholm, 2022). Recent research suggests that central for the success of scams are the individual level vulnerabilities: how do the individuals evaluate the credibility of influence attempts and what are the digital vulnerabilities enabling these (Ariely, 2023)?

Scams build on the ability to persuade individuals that something is real. Persuasion, understood as a process of deliberately attempting to alter another individual's or group's beliefs, views, and behaviour (Gunden et al., 2020; Petty & Cacioppo, 1986), builds on providing its target with just enough cues to appear authentic. These mechanisms of deception and believing something that is not authentic or real have remained understudied (Chadwick & Stanyer, 2021), despite the major financial losses caused by such hoaxes. In fact, little is known about the vulnerabilities on which the influence attempts build deception on in online environments. This research asks what individual vulnerabilities are utilized and what persuasion tactics influence individuals to fall for crypto-currency scams online?

Recent measures suggest the amount of global financial losses due to scams and frauds has been suggested to be up to $485.6 billion (Nasdaq & Verafin, 2024). Further, it is worth noting that the majority of corporate hoax cases remain unreported due to their sensitive nature, public backlash if discovered and high potential negative impact on the brand or corporate reputation. Many of these cases could have been avoided had corporations and organizations been better prepared and understood the different individual level vulnerabilities. In this paper, the focus is on persuasion principles (Cialdini, 2014) and analyzing their role in three recent online crypto scams that fooled great numbers of people to join. The focus of this paper is to consequently propose a process on how an investigator would go about investigating crypto crimes and scams on the blockchain. As the adoption of blockchain technologies continues to increase at unprecedented rates, it is imperative to produce investigative toolkits and use cases to help reduce time spent trying to catch bad actors within the generally anonymous realm of cryptocurrencies.

The paper is organized as follows. First, the paper looks at vulnerabilities enabling corporate and individual hoaxes on three levels of individual, social and situational. Second, the vulnerabilities that deepfakes and hoaxes build on are explained by introducing persuasion principles of (Cialdini, 2014). Third, three recent illustrative examples of different ways to scam individuals are analyzed, and to conclude, lessons learned from these examples for how digital vulnerabilities could be better prepared for by organizations and individuals are discussed.

2. New Vulnerabilities

(Lewandowsky, Ecker, & Cook, 2017) suggests that an environment where facts and fiction combine and the real truth is difficult to distinguish from scams results from four societal trends. First, the societal mega-trend of a decline in the social capital of authentic collaboration outside the internet has left people vulnerable as decisions are made individually and isolated without dialogue and deliberation with others. Second, there is growing economic inequality and financial challenges for many societies, which causes stress and makes individuals also take irrational risks. Third, there is an increase in opinion strength and polarization in society, making strong claims seem more natural than previously. Fourth, a slow decline in trust in scientific evidence and experts has led to a lack of understanding of the realities behind complex systems (such as crypto). Finally, there is an increasingly fractioned media landscape without a common "public opinion" forming where facts can be checked and myths debunked, and individuals can fall deep inside their biased thinking of their niche online communities without having to be interrupted by the truth (Ariely, 2023).

Vulnerability refers to some form of reduced capacity, actual or potential inability to fend off harm (Lee & Scanlon, 2007). Such vulnerabilities can take place in the physical, psychological, socioeconomic, or even social realms, and they may or may not be known by the organization or individual. Summarizing vulnerabilities has listed three different levels where they occur (Pamment, Nothhaft, Agardh-Twetman, & Fjällhed, 2018; Hansson, et al., 2020).

- Individual, cognitive vulnerabilities (such as cognitive biases)
- Social, public opinion vulnerabilities (manipulativity of narratives)
- Situational, system-level stress (situations of stress).

Individuals prepare for, critically analyze and become aware of only those messages they realize to be attempts to influence them. According to the persuasion knowledge model (Friestad & Wright, 1994), an influence attempt loses its power the moment an individual becomes aware of its persuasion mechanism and creates a certain reactance to it. Hoaxes are planned to avoid such realizations and to keep people from developing negative reactance (Viererbl & Koch, 2022).

What makes people convinced is often a combination of providing what they want to hear and see. In practice, believability results from the content of the message, how much the individual is personally involved and the kind of attitude the individual takes towards a topic. Strongly important are also the individual's emotions as well as the perceived benefit to be gained (Kraemer & Mosler, 2010). There are 6 principles of persuasion that can be utilized by scams (Cialdini, 2014), working together in combination or activated individually. These principles build on the individual as well as social vulnerabilities, but also situational pressures can activate and strengthen their power.

1. Reciprocity: individuals feel obliged to repay favours of any sort and like to follow the advice or recommendations of people they feel they owe something to, for example, a friend who has invested in crypto (Alslaity & Tran, 2021).
2. Consistency and previous commitments: individuals have a need to remain aligned in their thinking and actions, (Tinc, Sorensen, Goodspeed, & Jenkins, 2022), and factors such as personal beliefs, societal expectations and persona-related. For example, if they want to be considered a tech-savvy individual, crypto investments are valuable.
3. Social proof: individuals want to do things others in society are doing and the more people appear to be involved, the more tempting it is (Tinc, Sorensen, Goodspeed, & Jenkins, 2022). For example, if your neighbours are investing in crypto, there is more pressure to join the group and also invest.
4. Liking: Individuals respond better to messages individuals like or look up to, or see similarities with. For example, as Elon Musk is originally from Pretoria, South Africa, individuals from that region tend to like him and take his advice (Goss, Rothschild, & Hutson, 2021).
5. Authority: Individuals tend to obey perceived authorities, even if it goes against their personal beliefs. Further, people trust advice or recommendations from perceived experts on specific topics (Zalake,

de Siqueira, Vaddiparti, & Lok, 2021). For example, as the world's richest man, Elon Musk is considered an expert for advice on money and investing.

6. Scarcity: Individuals view opportunities as more valuable "when they are less available" (Cialdini, 2014)For example, a limited-time-only – crypto exchange offer makes individuals act faster than those that would always remain open.

When it comes to crypto scams, the individual-level vulnerabilities are often built on cognitive biases such as the confirmation bias of seeing only information that confirms their beliefs (Chadwick & Stanyer, 2021). Further, on the social level of digital platforms and networks, an overconfidence effect and the biases caused by in-group thinking (such as the cheerleader effect) take place on many online discussion forums where crypto is discussed. Further, the situational level vulnerabilities are often brought about by financial struggles or stress that societies undergo making way for a negativity bias and enabling the easier belief of false information (Bouko, Naderer, Rieger, Van Ostaeyen, & & Voué, 2021).

3. Recent Crypto Scams Building on Digital Vulnerabilities

Many crypto scams have been circulating in recent years, causing major cryptocurrency financial losses and becoming significant issues for society. The blockchain is decentralized and relatively unregulated and scammers often exploit this very nature of cryptocurrencies to manipulate prices, steal funds or deceive investors. Fake news and misleading social media posts can create an urgency under investors and cause panic sells or buys, which would then lead to volatile price fluctuations, benefitting the fraudsters. In fact, contrary to the original purpose of web3 and its potential to strengthen societies and foster inclusion, many new blockchain technologies have turned into a mechanism for exploitation and inequality. These technologies are especially utilized in areas and conditions of poverty and corruption, and some have suggested a new form of colonialism, 'crypto-colonial' extra-activism, where vulnerable populations become victims of technological advancements disguised in hopes of financial independence (Howson, 2023).

Crypto scams utilize weaknesses in human cognition and emotions that are difficult to regulate and defend. To improve the resistance of societies to such scams, the focus should be on individual vulnerabilities. In each of the types of crypto scams, the attackers make use of unique methods and persuasion tactics to lure their victims. The anonymity in crypto transactions makes it very difficult to trace or recover lost funds, which amplifies the risk for people who fall victim to these deceptive practices. Participants in the crypto market must mitigate financial losses. Ponzi schemes, phishing attacks, fake Initial Coin Offerings (ICOs), impersonations, giveaway scams, rug pulls or exit scams and pump-and-dumps are some of the common scam types that have cost investors huge amounts of monetary losses (Botha, Botha, & Leenen, 2023a).

3.1 Case Selection

To study these vulnerabilities in practice, the paper examines three different types of global crypto scams. The selection criteria for the case examples were that the selected cases focused on cryptocurrencies, included severe financial losses for victims and were publicly discussed in the media. Further, the impact of the selected cases had been verified by previous studies scale (Botha, Botha, & Leenen, 2023a), and the cases had to be of continued interest where similar scams were still current. These criteria limited the selection, and only one major case was picked when several different scams of the same kind occurred. It is important to note, that most scams go unreported as corporate and individual victims prefer privacy for fear of reputational damage caused by publicity of the case.

3.2 Theory-Driven Content Analysis

To understand these mechanisms better, 3 different types of scams were content analyzed by theory-driven content analysis built on Cialdini's 6 principles of persuasion (Cialdini, 2014) . As the cases called for a deductive approach and predefined categories, theory-driven content analysis was chosen as it enables a qualitative approach that best utilizes existing theories or frameworks to guide the analysis of data (Szabó, Soós, & Schiller, 2024). A coding scheme was developed based on the persuasion principles from literature and allowed the researchers to test the occurrence of the principles in practice. The three types of crypto scams selected for analysis represented the most popular scam types: The giveaway scam, pump-and-dump scam and Ponzi schemes. These are next examined in more detail, first focusing shortly on the scam and its events and after the case introductions, the summarized analysis of the persuasion types utilized.

3.3 Case 1: Giveaway Scam

The giveaway scam, for example, usually goes hand in hand with the impersonation scam type. A giveaway scam is a form of social engineering where the scammer attempts to deceive the potential investor into believing that some famous person is hosting a cryptocurrency giveaway. The investor is requested to send a specific amount of crypto to a given crypto address, with the promise that the platform would giveaway double the amount sent by the investor. The logic and arguments the scammers would use to get the victim to send bitcoins is so that the platform can verify the wallet address and the legitimacy of the investor's account (Botha & Leenen, 2024). It should be noted that exchanges do host legitimate giveaways from time to time as part of marketing campaigns. However, an exchange would never ask participants to send them crypto coins to receive a giveaway (Hauer, 2020).

Social media sites are often used to market or announce giveaway scams. Scammers will impersonate a company, a celebrity or a famous influencer. Advantage is taken of the famous person's trustworthy reputation on social media platforms such as Facebook, Twitter (X), YouTube, Telegram, Instagram, TikTok, etc. Elon Musk has often been impersonated in recent years in crypto giveaway scams. Figure 1 shows an image of a tweet (x), supposedly posted by Musk, promoting a giveaway being hosted by Tesla. It should be noted that this tweet is not a real text tweet, but an image that was manipulated and did not originate from Musk. The tweet has a link incorporated and when clicked on it redirects the user to the scammer's landing page which appears to be from Tesla or Musk offering "free" Bitcoin and Ethereum, Figure 2 (Botha, Botha, & Leenen, 2023a; Hauer, 2020).

Another technique scammers use is to send a direct message (DM) on social media platforms pretending to be a celebrity or an ambassador of that celebrity, advising a potential victim to participate in the giveaway. Upon engagement, the conversation will be directed to WhatsApp, which makes it seem to be a more personal platform to engage, building on the trust of the victim.

YouTube Livestreams is another popular technique used to advertise a giveaway. The scammer would create a YouTube video, combining an older stream of an interview with a famous person with his live stream, manipulating the content to make it look like the interview is currently live. The video will be overlayed with details of the giveaway. The user would then click on a link or a QR code that would redirect them to the landing page, see Figure 2, with the details of the giveaway. In addition to the live stream video, the scammer would make use of chatbots and display chats of multiple users next to the video. This gives the sense that many people are currently watching the live interview, creating more urgency to act and also tapping into the principle of social proof that everyone is online and actively participating in the giveaway.

Lastly, scammers also still make use of email to lure their victims. Phishing emails are sent attempting to convince the user that a crypto giveaway is being hosted. When the user clicks on the link, they will be redirected to the landing page of the scam details

Figure 1: Tweet from Scammer Impersonating Elon Musk (Hauer, 2020)

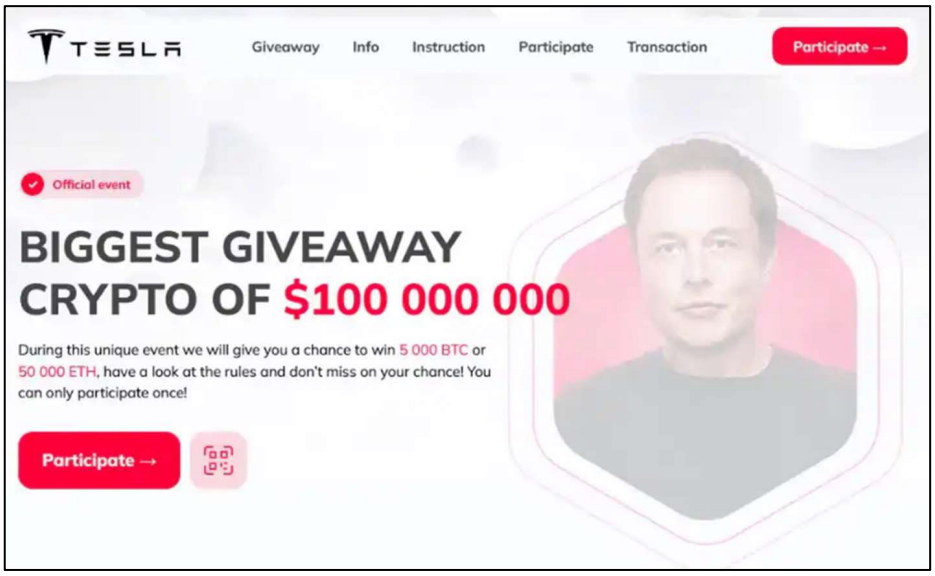

Figure 2: Landing Page of the Giveaway from TeslaGuez, 2023)

3.4 Case 2: Pump-and-Dump Scam

A pump-and-dump scheme or scam is when insiders "pump" a coin or token. Pumping a coin means to increase its value significantly so that it creates a lot of attention and interest the market. The moment others jump in, the initial investors will "dump" (sell all their coins), causing a massive decrease in price and leave late investors at a loss. Figure 3 shows a candlestick chart of a coin that has been pumped and dumped in a timespan of three hours. Typically how this would work is a telegram group will be created where a hype will be created around a pump that would happen at a specific time. For a number of days, 2 weeks or so, marketing campaigns will run and a telegram group will get more excited and more participants will join in. The announcement will say, for example, a pump will occur on a Sunday at 17:00 (refer to Figure 3). They won't tell which coin, usually some low market capital value coin. The coin to be pumped gets revealed at the time of the announcement. They will tell all members of the telegram group that they expect a pump of 1000% growth and everyone will get rich. Looking at Figure 3, it is shown that the pump started at 16:00 already (Kamps, 2018).

At 17:00, the coin to be pumped gets announced on the telegram group. All participants will jump onto an exchange of their choice (that has the coin to be pumped listed) and place a market buy order. Figure 3 shows that most of the pump already occurred by 17:00 by the time investors jump in. The graph will go up slightly more and then the initial investors dump all their coins, causing the coin to decrease rapidly, as shown on the chart in Figure 3. Investors waited for their big pump but, instead the value is now decreasing. Some investors would have made some profits if they sold in time, but not nearly close to the 1000% promised. Other investors would already be at a loss (Kamps, 2018).

On the telegram group, the organizers will announce that investors should get ready for the second wave of the pump. Now, the investors who made some profits, are all hyped and getting ready for the second pump, placing another buy order. But the second wave never comes, leaving all investors dry. The initial organisers are not known, only a telegram name and the group they were linked to. To catch these scammers is almost impossible. Some investors would realize they have been scammed and never participate in a pump-and-dump again. Other investors would think, they were not lucky this time, maybe in a next pump they would make all their losses back. They would stay on the telegram group, waiting for the next coin to be pumped, which would take place, for example, in another two weeks' time. They would participate again, and would lose again. It should be noted that pump-and-dumps are illegal and one should never participate in these events (Kamps, 2018).

Figure 3: Pump-and-dump Candlestick Chart (Kamps, 2018)

3.5 Case 3: Ponzi Scheme

Ponzi schemes are fraudulent investments or scams. A platform would be created where members would sign up and see their portfolios. Each member is required to invite new members to the scheme that would be placed under them, following a multi-level marketing (MLM) approach. High rates of returns are promised, which do occur in the initial phases. It is similar to a pyramid scheme where only the early investors would benefit the most. Returns are only sustainable by bringing in new and more investors (Chen, 2021). The scheme would make investors believe that a cloud mining package or a very successful trading bot or some lending scheme is generating profits, monthly, weekly or some even promise daily.

A good example of a recent crypto Ponzi scheme, is Mirror Trading International (MTI). MTI was a network or MLM scheme that claimed to offer automated crypto trading services via bots, on behalf of its members. The scheme promised a consistent monthly return of 10% to members. In some cases 1% was promised daily, depending on the level a member was on the platform. The platform started operating in 2017 and made good returns for all members. Until December 2020, when the website suddenly went down. False news was spread that the CEO, Mr Johann Steynberg, vanished and fled the country for he received death threats and his life was in danger. This caused a major panic under investors. On the one end, investors were not sure if they lost all of their investments. On the other end, members of the scheme felt sorry for the CEO whose life was supposedly in danger (Botha, Botha, & Leenen, 2023b).

Steynberg was arrested on 29 December 2021 for allegedly presenting fake identification to law enforcement officers, one year after he fled the country. Up to this time, law cases were filed, and people had realised they have been scammed. Some investors were hopeful that they would receive their money back when the news came out that the CEO was arrested (Botha, Botha, & Leenen, 2023b). However, he was under house arrest in Brazil. Or so it was believed. A trusted source with knowledge of the case reported to MyBroadband, an African news company, that over 46,000 Bitcoins passed through the platform (Vermeulen, 2022). The latest news on this matter was that Steynberg died on 22 April 2024 from a severe heart attack. A number of conspiracy theories are swirling and, at the time of writing, the matter is being investigated by the Directorate for Priority Crime Investigations (DPCI), also known as the Hawks, from South Africa (Cronje, 2024).

4. Analysis of the Scams According to the Persuasion Principles

As for the vulnerabilities of the individuals caught in the scams, there were vulnerabilities on all three different levels of individual, social and situational. In addition to these vulnerabilities, there were several persuasion principles at use for the scams. Those principles are explained next in Tables 1, 2 and 3 focusing on the specific

types of scams. Though all persuasion principles could be detected in the cases on some level, clear distinctions were found between what was the most important for each scam and their credibility.

As can be seen from Table 1, the giveaway scam is built strongest on the principles of scarcity, authority, liking and social proof. For this, the vulnerabilities were hence mostly on the individual and societal level, and the most valuable mechanism remains utilizing the apparent social connections and trust on which the individual victims learn to rely. Consistency and reciprocity as persuasion mechanisms serve merely a supporting role and remained less valuable for these types of giveaway scams.

Table 1: (Cialdini, 2014) Persuasion Principles Utilized in the Crypto Giveaway Scam: Hosted by Tesla and/or Elon Musk

Reciprocity	**Somewhat utilized**: In some cases with small-value coins or tokens giveaways, the scammer would give the victim double back the amount of coins invested straightaway. But, this is only to gain more trust so that the victim can get greedy and deposit a larger amount of coins. Once the larger amount was sent by the victim, the scammer would disappear.
Consistency	**Somewhat utilized**: The scammer can use the fact that crypto is a new technology and if the victim is somewhat tech-savvy or wants to be seen as so they would feel that the crypto investments are valuable and are aligned with their beliefs.
Social proof	**Strongly utilized**: By using chatbots on the YouTube live stream technique, the scammer is leveraging on social proof. Making it look like others are participating in the giveaway. This would cause the victim to be more likely to follow and participate.
Liking	**Strongly utilized**: Many people like and follow Elon Musk. By building rapport, establishing mutual trust, showing genuine interest and finding common ground the scammer increases the likelihood of successful persuasion.
Authority	**Strongly utilized**: The scammer impersonates a celebrity or powerful influencer, using their expertise, credibility and trustworthy reputation as leverage. For example, Elon Musk is well known to be very knowledgeable in technology and he has a big interest in crypto. Impersonating him will win the trust of many victims.
Scarcity	**Strongly utilized**: By creating an urgency for the victim to act now or he/she will lose out on a one-time opportunity or offer. The scammer taps into people's fear of missing out and drives them to take immediate action.

Table 2 illustrates the persuasion principles utilized in the crypto pump-and-dump scams. The Pump-and-dump scams operate differently to the degree that they rely most heavily on social proof and scarcity. On the other hand, the role of authority is not utilized at all, and reciprocity, consistency and liking are only somewhat utilized. The vulnerability levels were particularly evident on social and situational levels, as social proof and scarcity arise in certain social and situational contexts. Additionally, individual vulnerabilities are exploited, as personal attributes influence an individual's ability to comprehend or respond to information.

Table 2: (Cialdini, 2014) Persuasion Principles Utilized in a Crypto Pump-and-Dump Scam

Reciprocity	**Somewhat utilized**: A false promise is made for very high returns. Some investors would make some good returns in a pump-and-dump scheme. In this sense, something was given as promised. And these would probably enter such a scheme again, if they know their timing to jump in and out of the trade in time, before the dump, or before they would be at a loss in their trade.
Consistency	**Somewhat utilized**: The scammers will continue with this type of scam for months, making investors believe that if they get in and out at the right time they would get rich quickly. The same technique is used over and over. Even the members who lost big amounts of money, would believe that the next time it will be their time, and they would participate again.
Social proof	**Strongly utilized**: By using chatbots on the Telegram group, the scammer is leveraging on social proof. Making it look like others are participating in the pump. This would cause the victim to be more likely to follow and participate.
Liking	**Somewhat utilized**: The only liking in this scam is the crypto community. A strong crypto community and believers will take part in this scam.
Authority	**Not utilized**: In this scam normally no impersonation of a celebrity or powerful influencer is used. However, it is possible to impersonate a company making investors believe that a trust worthy company is hosting a pump. However, this is not how these scams usually operate.
Scarcity	**Strongly utilized**: By creating an urgency for the victim to act now or he/she will lose out on a one-time opportunity or offer. The scammer taps into people's fear of missing out and drives them to take immediate action.

Table 3 shows the persuasion principles utilized in the MTI Ponzi scheme. Unlike the previous types of scams, this format builds strongly on reciprocity and consistency, together with scarcity and social proof. In terms of vulnerabilities, this means building on individual and cognitive vulnerabilities, as well as social vulnerabilities, by exploiting manipulative narratives and relationships between the participants.

Table 3: (Cialdini, 2014) Persuasion Principles Utilized in the MTI Crypto Ponzi Scheme

Reciprocity	**Strongly utilized**: The platform generated good returns as promised from 2017. Members invested to the platform, and returns could be withdrawn for three years, until December 2020.
Consistency	**Strongly utilized**: The scammers used the fact that crypto is a new technology and trading bots are the latest technology and they claimed to have developed these bots to be very successful in trading. Users who did not know anything about crypto, but wanted to be seen as tech-savvy and that they are investing in crypto, could do so by using the MTI platform. However, the users never owned any crypto, it was all false information provided on the platform's dashboard.
Social proof	**Strongly utilized**: Many marketing videos were done live whereby it looked as if hundreds of members are all joining in the audience. The platform would also take certain members as examples to show case their riches all gained from the platform. These members were all early investors. Late investors would not make those kind of returns.
Liking	**Somewhat utilized**: No famous person were used. However, the marketing people made Steynberg sounded like a super clever person who has been able to beat the system with his trading bots that was supposedly developed by Steynberg himself. Members liked Steynberg and believed in him.
Authority	**Somewhat utilized**: Steynberg was announced as an overnight successor. The marketing team used him as the authoritative figure in the scheme. If Steynberg believed the market is good for investments, the members believed that too.
Scarcity	**Strongly utilized**: The scammer taps into people's fear of missing out and drives them to take immediate action. By creating an urgency for the victim to act now or he/she will lose out on a one-time opportunity or offer. The earlier a member invests, the better the chances of becoming financially free. The trading bot was said to be very successful and no other company has figured out what MTI has, they were the only ones who could predict the market with the trading bot.

What all three examples have in common is utilizing a combination of the different persuasion strategies, refer to Table 4.

Table 4: (Cialdini, 2014) Persuasion Principles summarized in all crypto currency scams analyzed

Persuasion Principle	Crypto Giveaway Scam	Pump-and-dump Scam	Crypto Ponzi Scheme
Reciprocity	Somewhat utilized	Somewhat utilized	Strongly utilized
Consistency	Somewhat utilized	Somewhat utilized	Strongly utilized
Social proof	**Strongly utilized**	**Strongly utilized**	**Strongly utilized**
Liking	Strongly utilized	Somewhat utilized	Somewhat utilized
Authority	Strongly utilized	Not utilize	Somewhat utilized
Scarcity	**Strongly utilized**	**Strongly utilized**	**Strongly utilized**

Interestingly, all cases relied heavily on social proof and scarcity, making understanding their underlying logic important when attempting to understand the scams. Each type of scam, however, relies on different strategies.

5. Conclusion

Recent studies have suggested that individual and societal vulnerabilities play an increasingly larger role in the spread of misinformation and the successful execution of online scams. Understanding these vulnerabilities becomes especially important as AI improves the impact of deepfakes and new technologies enable the easier spread of manipulated information. The paper detected different influence strategies at use on which the specific crypto scams analyzed relied, ranging from authority figures of crypto giveaways to the role of consistency and social proof of Ponzi schemes and the scarcity principle behind pump-and-dump scams.

As all scams analyzed utilized two persuasion principles over others, social proof and scarcity. This means the vulnerabilities enabling these different types of scams vary, and so the remedies must address several different factors. A common suggestion is improving individual resilience to scams through increased media literacy or persuasion knowledge (Friestad, 1994) and becoming more aware of the different cognitive biases and vulnerabilities. Another suggestion has been to address the societal inequalities and siloes through different

depolarization strategies (Kubin & von Sikorski, 2021), to make less ground for scams to build on. These alone, however, are not enough, there will always be situational vulnerabilities that make individuals under stress react in harmful ways (Ariely, 2023).

The practical implications of this paper are several. First, this paper hopes to serve as a starting point for understanding all three levels of digital vulnerabilities by shedding light on the influence mechanisms on which the crypto scams build on and with these serve as strengthening societies and organizations in their resilience to scams. As social proof and scarcity appear to work the best in crypto scams, potential efforts to improve victims' resilience should focus on strengthening these areas. How to verify if others have actually participated in the way it seems? How to make scarcity less appealing? There are several limitations for this paper, Including its limitation of only three examples, and one influence strategy framework. Future studies could focus on broadening the understanding of the different influence mechanisms beneath other types of scams. Future studies should look into also the unsuccessful attempts of scamming, and look at how the resistance of individuals could be improved, as well as collect and analyse more examples across cultures.

References

Alaraatikka, M., Koistinen, P., Kaarkoski, M., Huhtinen, A., & Sederholm, T. (2022). If you are late, you are beyond help: Disinformation and authorities in social media. *Proceedings of the 9th European Conference on Social Media* (pp. 7-13). Helsinki: In I. Lupa-Wojcik & M. Czyzewska (Eds.). doi:10.34190/ecsm.9.1.168

Alslaity, A., & Tran, T. (2021). Users' Responsiveness to Persuasive Techniques in Recommender Systems. *Frontiers in artificial intelligence*, *4.* doi:https://doi.org/10.3389/frai.2021.679459

Ariely, D. (2023). *Misbelief: What Makes Rational People Believe Irrational Things.* New York: HarperCollins.

Botha, J., & Leenen, L. (2024). An Analysis of a Cryptocurrency Giveaway Scam: Use Case. Jyväskylä, Finland: Academic Conferences International Limited.

Botha, J., Botha, D., & Leenen, L. (2023a). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. Baltimore, USA: Academic Conferences International Limited.

Botha, J., Botha, D., & Leenen, L. (2023b). An Analysis of the MTI Crypto Investment Scam: Use Case. Athens, Greece: Academic Conferences International Limited.

Bouko, C., Naderer, B., Rieger, D., Van Ostaeyen, P., & & Voué, P. (2021). *Discourse patterns used by extremist Salafists on Facebook: identifying potential triggers to cognitive biases in radicalized content* (Vol. 19(3)). Online: Taylor and Francis. doi:10.1080/17405904.2021.1879185

Canel, M., & Luoma-aho, V. (2019). Public Sector Communication: Closing Gaps Between Citizens and Public Organizations. John Wiley & Sons. doi:https://doi.org/10.1002/9781119135630

Chadwick, A., & Stanyer, J. (2021). Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework. *32*(1), 1–24.

Chen, J. (2021). *Ponzi Scheme: Definition, Examples, and Origins*. Retrieved Oct 23, 2024, from https://www.investopedia.com/terms/p/ponzischeme.asp

Cialdini, R. (2014). *Influence: Science and practice (Vol. 4, pp. 51-96).* Boston: Pearson education.

Cronje, J. (2024). *Hawks investigating whether crypto Ponzi kingpin Johann Steynberg has died*. (News24) Retrieved Oct 23, 2024, from www.news24.com: https://www.moonstone.co.za/hawks-investigating-reported-death-of-mti-founder-johann-steynberg/

Friestad, M. &. (1994). The Persuasion Knowledge Model: How people cope with persuasion attempts. *Journal of Consumer Research, 21*(1), 1-31. Retrieved from https://doi.org/10.1086/209380

Goss, B. D., Rothschild, P. C., & Hutson, M. M. (2021). Applying Persuasion Theory to Sport Properties' Digital Media. *Journal of Managerial Issues: JMI, 33*(3), 237–258.

Guez, S. (2023). *Chatbots, Celebrities, and Victim Retargeting: Why Crypto Giveaway Scams Are Still So Successful*. Retrieved Oct 22, 2024, from https://www.akamai.com/blog/security-research/cryptogiveaway-

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. *International Journal of Disaster Risk Reduction*, 51.

Hauer, T. (2020). *Crypto giveaway scams and how to spot them*. Retrieved Oct 22, 2024, from https://www.coinbase.com/blog/crypto-giveaway-scams-and-how-to-spot-them

Howson, P. (2023). The Blockchain Scam That's Ruining the World. In P. Howson, *Let Them Eat Crypto* (p. 289). Pluto Press.

Kamps, J. K. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. .: Crime Science Journal. doi:https://doi.org/10.1186/s40163-018-0093-5

Kraemer, S. M., & Mosler, H. (2010). Persuasion factors influencing the decision to use sustainable household water treatment. *International Journal of Environmental Health Research, 20*(1), 61–79. doi:https://doi.org/10.1080/09603120903398301

Kubin, E., & von Sikorski, C. (2021). The role of (social) media in political polarization: a systematic review. *Annals of the International Communication Association*, *45(7)*, pp. 188–206. doi:10.1080/23808985.2021.1976070

Lewandowsky, S., Ecker, U., & Cook, J. (2017). Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. *Journal of Applied Research in Memory and Cognition*. doi:10.1016/j.jarmac.2017.07.008

Nasdaq & Verafin. (2024). *Global Financial Crime Report.* USA: Nasdaq. Retrieved Oct 21, 2024, from https://elements.visualcapitalist.com/wp-content/uploads/2024/04/1711973384569.pdf

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). *"Countering information influence activities: The state of the art".* Swedish Civil Contingencies (MSB). Retrieved from https://lup.lub.lu.se/search/publication/825192b8-9274-4371-b33d-2b11baa5d5ae

Rhodes, S. (2022). Filter bubbles, echo chambers, and fake news: How social media conditions individuals to be less critical of political misinformation. *Political Communication, 39*(1), 1-22. Retrieved from https://doi.org/10.1080/10584609.2021.1910887

Szabó, Z. A., Soós, S., & Schiller, E. (2024). Deductive content analysis as a research method in the field of education sciences - A systematic literature review of journal articles in Web of Science (2019–2023). *Journal of Adult Learning, Knowledge and Innovation*.

Tinc, P., Sorensen, J., Goodspeed, M., & Jenkins, P. (2022). Do Cialdini's "Principles of Influence" Motivate Safe Practices on Farms? *Journal of Argomedicine, 27*(3), 272-283. doi:https://doi.org/10.1080/1059924X.2021.1950591

Vermeulen, J. (2022). *Good news for Mirror Trading International scam victims*. Retrieved Oct 23, 2024, from https://mybroadband.co.za/news/cryptocurrency/440928-good-news-for-mirror-trading-international-scam-victims.html

Viererbl, B., & Koch, T. (2022). The paradoxical effects of communicating CSR activities: Why CSR communication has both positive and negative effects on the perception of a company's social responsibility. *Public Relations Review, 48*(1). doi:https://doi.org/10.1016/j.pubrev.2021.102134

Zalake, M., de Siqueira, A., Vaddiparti, K., & Lok, B. (2021). The effects of virtual human's verbal persuasion strategies on user intention and behavior. *International Journal of Human-Computer Studies, 156*(1).