An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022

Johnny Botha[1], Danielle Petronella Botha[2] and Louise Leenen[3]
[1,2]Council for Scientific and Industrial Research, Pretoria, South Africa
[3]University of Western Cape and CAIR, Cape town, South Africa

jbotha1@csir.co.za
dbotha3@csir.co.za
lleenen@uwc.ac.za

Abstract: Blockchain and cryptocurrency adoption has increased significantly since the start of the Covid-19 pandemic. This adoption rate has overtaken the Internet adoption rate in the 90s and early 2000s, but as a result, the instances of crypto scams have also increased. The types of crypto scams reported are typically giveaway scams, rug pulls, phishing scams, impersonation scams, Ponzi schemes as well as pump and dumps. The US Federal Trade Commission (FTC) reported that in May 2021 the number of crypto scams were twelve times higher than in 2020, and the total loss increased by almost 1000%. The FTC also reported that Americans have lost more than $80 million due to cryptocurrency investment scams from October 2019 to October 2020, with victims between the ages of 20 and 39 represented 44% of the reported cases. Social Media has become the go-to place for scammers where attackers hack pre-existing profiles and ask targets' contacts for payments in cryptocurrency. In 2020, both Joe Biden and Bill Gates' Twitter accounts were hacked where the hacker posted tweets promising that for all payments sent to a specified address, double the amount will be returned, and this case of fraud was responsible for $100,000 in losses. A similar scheme using Elon Musk's Twitter account resulted in losses of nearly $2 million. This paper analyses the most significant blockchain and cryptocurrency scams since the start of the Covid-19 pandemic, with the aim of raising awareness and contributing to protection against attacks. Even though the blockchain is a revolutionary technology with numerous benefits, it also poses an international crisis that cannot be ignored.

Keywords: Blockchain, Covid-19, Crypto-crime, Cryptocurrency, Crypto-scams.

1. Introduction

Blockchain adoption has increased significantly in recent years, and so has crypto-crime. Some may argue that Bitcoin gives power back to the people. However, the popularity of cryptocurrencies in recent years has attracted the attention of many scammers and fraudsters. Undoubtedly, the rise of cryptocurrency has added to the immense increase in crime rates. Illicit transactions in cryptocurrency have reached a staggering $14-billion in 2021, an 80% increase from 2020 - which constitutes a new record. Chainalysis[1], a blockchain data platform, stated that the rise of decentralised finance (DeFi), is the leading factor behind the spread of crypto scams (Chainalysis, 2021). Out of all hacks and scams in 2021, 21% took advantage of a loophole in DeFi (Xia, et al., 2020).

Scammers have been around long before crypto, but some of the characteristics of crypto are very appealing to them. Crypto has no middleman as in the case with banks. Instead, direct transactions occur between two individuals. The Covid-19 pandemic brought difficult times with job losses and salary cuts. People became desperate to invest in alternative methods and crypto seemed like the perfect solution with the consequence that scammers took advantage of this opportunity. Crimes in the cryptocurrency space victimise innocent people - it places a big barrier in its further adoption and increases government restrictions. Investigating and exploring cryptocurrency transactions remain intractably hard due to its pseudonymous nature and with every cryptocurrency having its own protocol and blockchain (Social Links, 2022).

This study analyses the most significant crypto-scams since the start of the Covid-19 pandemic. It aims to raise awareness and contributes towards protection against these attacks. Blockchain is a revolutionary technology with immense benefits. However, the technology attracts crime and poses an international crisis.

2. Types of Crypto Crimes and How to Avoid Them

2.1 Giveaway

One of the most common scams is the giveaway scam. This is where the attacker lures the victim in by announcing to give away certain cryptocurrencies or assets. For example, one instance is where a contribution

[1] https://www.chainalysis.com

of one Ethereum coin (sent to a specified address) results in double the amount returned. Normally a target will receive a link to a landing page website, with fake transactions indicating that participants are indeed getting paid. In several cases the website has a timer that is activated with the intent of placing the target under the impression that there is a limited time for the offer to be taken up (Bureau, 2022).

Several social media sites are being used for these scams such as YouTube, Twitter and Instagram. In the case of YouTube, livestreams of interviews with celebrities are available. The stream links are surrounded by text details on how to participate in these schemes. Furthermore, it will also appear as if thousands of people are participating in the livestreams. However, these are generally bots and not real people. The YouTube account will often also appear to have been verified. In these cases, the accounts were hacked, all contents were deleted, and the attackers run their own livestreams. Other ways of launching this type of attack is when an attacker runs advertisements that appear around legitimate videos. Targets will then click on these advertisements and be transferred to a fake site.

2.2 Rug Pull

A new scam called a "rug pull" refers to the expression "someone pulls the rug from underneath you". They are also referred to as exit scams. This type of scam appears to be an investment company where people can invest funds with very attractive returns. The company will consequently disappear, and victims are robbed of their funds. Back in 2017, this was mostly driven by the Initial Coin Offering (ICO) schemes. Today they are more prevalent in the Non-Fungible Tokens (NFTs) and Decentralised-Finance (DeFi) spaces.

In the case of NFTs, the scammer creates a collection of images, issues them to be minted and promises an exciting roadmap with great returns. Once the mint process is completed and all people have procured their NFTs, the project creators delete the website and all social media linked to the project, thus pulling the rug, and leaving their victims upended. Another method is called the slow rug pull. In this case, the creators slowly extricate themselves from the project over several weeks or even months, causing targets to lose interest in the project. The slow rug pull is more common as this leaves no real traces of intent to defraud pointing to the attacker.

The DeFi space differs from NFTs and ICOs. Instead of sending money to a project or protocol, one needs to supply liquidity. The liquidity is used in a decentralised exchange and investors can get very lucrative returns. The creators will hype the project to increase its demand and to increase the liquidity pool size. After people have staked funds for some time on the DeFi platform, the creators will withdraw all the coins from the liquidity pool, removing all the value injected into the currency by investors, driving the price very low or even to down zero in some cases. This is called a DeFi rug pull and is the most common exit scam. Three types of rug pulls exist within DeFi:

- *Liquidity Stealing*: Token creators extract all coins from the liquidity pool driving the price to zero.
- *Limiting sell orders*: The developers are the only ones who can sell tokens. As soon as they received investments they sell the tokens for other currency pairs, leaving a worthless token to investors.
- *Dumping*: Developers immediately sell off enormous numbers of tokens, reducing the price and leaving investors with worthless tokens.

According to Moody (2022), the number of rug-pulls has been increasing annually since 2020. In 2021 the biggest financial losses of over $2.28 billion due to rug pulls have been recorded. Figure 1 presents the total amount of cryptocurrency (in USD) stolen in rug-pulls during 2020 to August 2022. Note that the graphs in Figures 1, 3 and 4 were compiled by the authors based on data from Moody (2022).

The data compiled in Figure 1 only captures rug pulls from 2020 until August 2022. During the remainder of 2022, it is important to note that further rug pulls may take place which could increase the total value lost. Many scams that took place in previous years, were only identified weeks or months after it took place. This may also be the case regarding the current data. Data capturing events taking place after the writing of this paper can be accessed via Moody (2022).

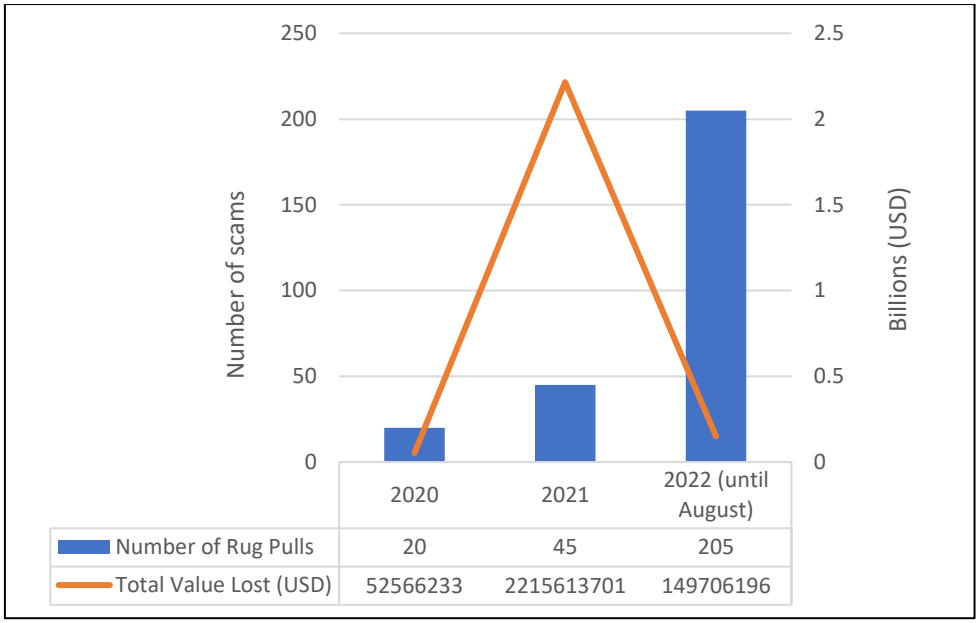

Figure 1: Total cryptocurrency value stolen in rug pulls vs the number of rug pulls

2.3 Phishing Scams

Phishing scams are pervasive within any system where human gullibility or inattention can be used against the user. As blockchain and Web 3.0 are evolving, so too are the techniques employed by phishers (Andryukhin, 2019). Scammers are fooling people to log into fake cryptocurrency exchange websites, getting access to their exchange account details and stealing their funds. Attackers have also started to directly target people's cryptocurrency wallets. The most damaging scam is when an attacker obtains the user's wallet private keys. This can happen by making users believe they need to reset their passwords and provide their secret recovery seed phrases. Another method is to ask the user to enter the seed phrase to access a certain website to allow a connect to their wallet. Once the attacker has this seed phrase, he has full access to your wallet (Bureau, 2022).

2.4 Impersonation

Impersonation is when the scammer tries to take advantage of some famous person's trustworthy reputation on social platforms such as Twitter, Telegram, Discord, Instagram, TikTok, etc. These scammers will send a direct message (DM) on the platform, pretending to be a celebrity and to offer advice to the victim on some crypto investment. They will provide a number asking the victim to WhatsApp them, where they will act as if they are providing more personal assistance. They will explain how the target can double their money by sharing a link on which the victim will click and send money to the platform or crypto address. This scam continues after the victim has sent the money; the attacker will send a fake proof of profits generated. The attacker will then request a withdrawal fee or pay them their cut of the profits first (Bureau, 2022).

2.5 Ponzi Scheme

Ponzi schemes are fraudulent investments or scams, promising high rates of returns, which do occur in the initial phases. It is similar to a pyramid scheme and normally mostly benefits early investors. Returns are only sustainable by bringing in more investors (Chen, 2021). The scheme makes people believe that a cloud mining package, lending scheme or very successful trading bot provide daily profits. These schemes also rely on current members referring their friends and family for additional rewards, which is called multi-level marketing (MLM) schemes (Bureau, 2022).

2.6 Pump-and-Dump

A pump-and-dump is when insiders "pump" or increase a token's price until a point where it creates attention and market interest. The moment others jump in, the initial investors will "dump" or sell their coins, causing a massive decrease in price, leaving late investors at a loss. A pump will be set to happen at a particular date and time. Figure 2 shows an example of such a pump-and-dump in a timespan of only three hours. Note that by the time the coin to pump is announced, the value has already been increased. These schemes are well coordinated in places such as Telegram groups. As soon as the public buys in, the organisers will do the dump causing losses for late investors.

Figure 2: Pump-and-Dump (Kamps, 2018)

3. The Worst Crypto-Crimes during the Pandemic

Using data consolidated by Moody (2022), it is clear that the number of Crypto scams has risen annually. Scams such as Ponzi Schemes, impersonations, Rug Pulls, Exit Scams, Phishing and Pump-and-Dumps were considered, whilst money laundering has been excluded. While the data available for 2022 is incomplete at the time of writing, the number of scams has already surpassed previous years, as seen in Figure 3.

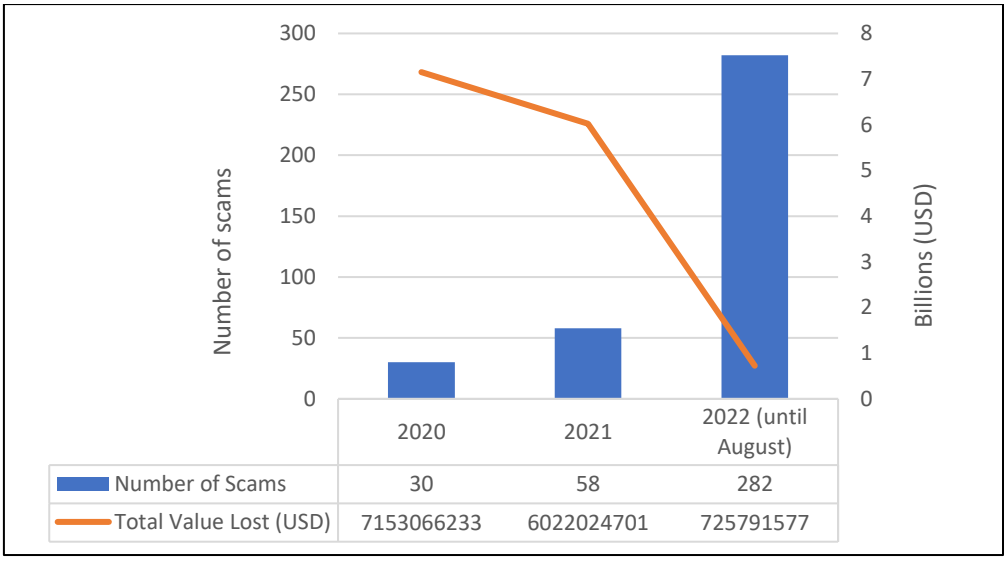

Figure 3: Number of scams per year with corresponding financial losses

Interestingly, the total value lost in 2022 is less than in previous years. However, more scams may still come to light during the remainder of the year; it is important to note that the total value lost to scams may still increase. Large-scale crashes within the crypto space, such as the Luna network (Forbes, 2022) and FTX exchange (Berwick, 2022) are both recent occurrences that, if confirmed to be scams after investigation, could push the total value lost in 2022 up by $60Bn and $2Bn respectively. This would make 2022 the year accruing the biggest financial losses.

A breakdown of the two major scam types based on monetary losses, Ponzi Schemes and Rug-Pulls, are presented in Figure 4, alongside all other losses in scams such as phishing, pump-and-dumps, impersonation,

etc. Note that some crypto scams of 2022 are suspected to be Ponzi schemes, but this has yet to be confirmed. It is possible that the amount lost to Ponzi schemes could be greater as more evidence is found.

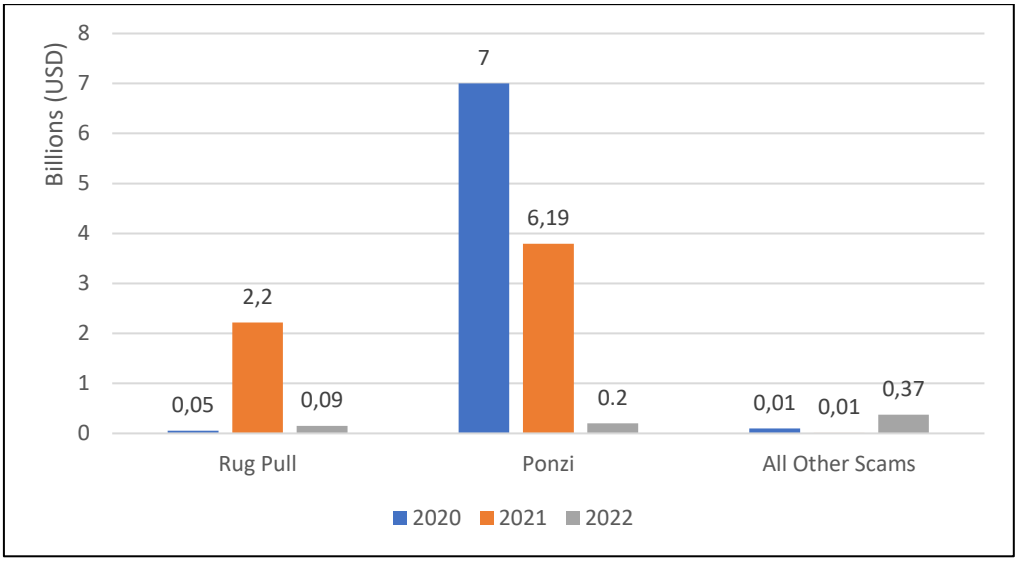

Figure 4: Financial Losses by Scam Type per Year

Table 1 lists the fifteen largest of these scams from 2020-2022, based on financial losses. The scams listed in the table are discussed below in more detail, grouped according to the year in which they occurred. In addition, the scams that affected the most users are investigated, as well as the global landscape of occurrences. Lastly, arrests made in relation to the scams are discussed.

In 2020, at the advent of the pandemic, approximately 40% of the largest scams recorded in Table 1 took place, consisted completely of Ponzi schemes. The largest of these schemes, PlusToken, was a multinational pyramid scheme whose operators have since been indicted. This scheme promised astronomical returns on investment and incentivised current investors to recruit new members, a trademark Ponzi scheme tactic (Leng, 2020). The racket owned roughly 1% of the Bitcoin supply at the height of the operation (Harper, 2020). Closely following PlusToken in losses in 2020 is MTI; The scheme accepted buy-ins in Bitcoin and is the largest fraudulent scheme that has been charged by the CFTC (Commodity Futures Trading Commision, 2022). Arbistar 2.0 SL (Nelson, 2020), BitClub (Crypto-Mining-Pool) (United States Department of Justice, 2022), and Forsage (Securities and Exchange Comission, 2022a) all offered similar returns on investments and were indicted as Ponzi or Pyramid Schemes.

At the start of 2021, the largest scams seemed to diversify, including several high-profile rug-pulls alongside more Ponzi Schemes. The Africrypt rug pull, considered one of the largest-ever crypto heists alongside PlusToken, is currently involved in an ongoing investigation and liquidation approved by South-African courts (Zimwara, 2021). Thodex, a cryptocurrency exchange, used aggressive campaigns such as luxury cars to lure investors. In April 2021, Thodex was shut down, having stolen approximately $2 billion (Baltrusaitis, 2022). Other Ponzi Schemes in this timeframe include Finiko (Tassev, 2021) and EmpiresX (Securities and Exchange Commission, 2022b), both affecting hundreds to thousands of users by offering too-good-to-be-true returns on investment. In addition, four noteworthy rug-pulls took place; Anubis Decentralised Autonomous Organisation (DAO) (Hakki, 2021), DeFi100 (Kolhatkar, 2021), Meerkat Finance (Sopov, 2021) and Snowdog DAO (Radmilac, 2021). All these rug-pulls were DeFi-based offerings that "rugged" investors after draining liquidity pools before delivering a real product. Some (such as Meerkat Finance and Africrypt) initially placed the blame on hacking events that never took place.

Table 1: The most significant crypto scams during the pandemic 2020-2022

Name	Type	Year	Losses (financial)	Country of origin	Affected users	Arrests made
PlusToken	Ponzi Scheme	2020	$4 billion	China & South-Korea	±3 million	Yes
Africrypt	Rug Pull	2021	$3.6 billion	South-Africa	±2 million	No
Thodex	Rug Pull	2021	$2 billion	Turkey	±390,000	Yes
MTI	Ponzi Scheme	2020	$1.7 billion	South-Africa	±280,000	Yes
Arbistar	Ponzi Scheme	2020	$1 billion	Spain	Up to 32,000	Yes

Name	Type	Year	Losses (financial)	Country of origin	Affected users	Arrests made
BitClub	Ponzi Scheme	2020	$722 million	Netherlands	Unspecified-thousands	Yes
Forsage	Ponzi Scheme	2020	$300 million	Russia & USA	Unspecified-millions	Yes
Morris Coin	Rug Pull	2022	$140 million	India	±1.1 million	Yes
Ormeus Coin	Ponzi Scheme	2022	$124 million	USA	±12,000	Yes
EmpiresX	Ponzi Scheme	2021	$100 million	USA	Unspecified-thousands	Yes
Finiko	Ponzi Scheme	2021	$95 million	Russia	Unspecified-hundreds	Yes
AnubisDAO	Rug Pull	2021	$60 million	Hong-Kong	Unknown	No
DeFi100	Rug Pull	2021	$32 million	Unspecified	Unknown	No
Meerkat Finance	Rug Pull	2021	$31 million	Unspecified	Unknown	No
SnowdogDAO	Rug Pull	2021	$30 million	Unspecified	Unknown	No

During 2022 (August at the time of writing), fewer noteworthy scams have been uncovered. So far, two large rug-pulls are Morris Coin and Ormeus Coin. The former was a fake Initial Coin Offering (ICO) (Jacob, 2022) and the latter a coin purportedly to be used as a mining currency (Pimentel, 2022). Both lured investors via social media.

Though some scams are difficult to trace due to anonymity extended via blockchain technologies (ByBit Learn, 2021), the location of origin could be determined for most of the top scams. The distribution of the scams is quite even spread globally, with South-Africa, Russia and the USA being the countries producing multiple of the most significant scams. Notably, South-Africa produced two of the top four crypto scams, as seen in Table 1.

PlusToken (Leng, 2020), Africrypt (Zimwara, 2021) and Morris coin (Jacob, 2022) affected the most users. Generally, Ponzi Schemes seem to affect more users. This could be due to the business model – investors are incentivised to recruit new members in the hope of increasing their profits. Though the Morris Coin scam did not cause financial losses as large as the Ponzi schemes, it amassed many participants (Jacob, 2022). Further, it can be difficult to quantify the number of people affected by rug-pulls. Sellers may obfuscate sales progress to hinder attempts to ascertain the legitimacy of the project (Investopedia, 2022).

Roughly 66% of the discussed cases resulted in arrests. Individuals were charged in various manners, including accounts of fraud, market manipulation, and more. The scams that have not yet resulted in arrests are mostly rug pulls. Creators often remain anonymous, making it much harder to track bad actors (ByBit Learn, 2021).

4. Protection Against Crypto Scams

4.1 Giveaway and Impersonation

The giveaway scam is normally linked to the impersonation scam where the scammer pretends to be a legitimate platform such as Coinbase[2] promoting a 5000 BTC giveaway when you send them, for example, 1 BTC. A legitimate investment platform or exchange will never ask for crypto in exchange for receiving more in return. Other type of impersonations are celebrities and YouTube live streams. These impersonator accounts will often have more followers than the real account to confuse the users, but these followers are all bots. To avoid these scams, awareness should be raised that no famous influencer on YouTube, Twitter, TikTok, etc. will send a DM to some unknown individual. Celebrities have thousands of followers and do not have the time to interact with followers one-on-one. Platforms such as Twitter and Telegram gives a blue tick for verified accounts. In addition, the public should not click on links sent by someone that offers crypto investment advice.

The only way to avoid these types of scams is to understand that no-one on the Internet is going to give something away for free, and no one will double an investment amount. If it sounds too good to be true, it normally is. One should think twice before sending crypto funds because all transactions are irreversible and participants will not be able get their money back (Hauer, 2020; Bureau, 2022).

4.2 Rug Pull

Rug pulls are more common in new cryptocurrency projects and investors should make sure they are choosing established projects. For example, Bitcoin has been used worldwide and its inner workings have been reviewed

[2] https://www.coinbase.com

thoroughly. Newer projects do not have such a track record and leave room for hiding certain aspects from investors. One indication, although it is not a guarantee, is to establish whether a new cryptocurrency is listed on well-known exchanges such as Binance[3] or Coinbase[2]. These exchanges do thorough reviews on assets before listing them. However, the trade-off is that the highest rewards may come from projects before they are listed on these exchanges. Scammers normally prey on the fear of missing out (FOMO) on massive gains, luring investors towards projects before being listed on well-known exchanges (Rosen, 2022).

To avoid a crypto project rug pull one would need to perform broad due diligence. Research needs to be done before investing and extremely high annual percentage yield (APY) promises should heighten caution (Bureau, 2022). Before investing, an investor should understand how a product works and not just blindly invest based on hype. Investors should also determine if the company has been registered and does indeed exist. In addition, establishing if a project has been audited (refer to LCX audits by CERTIK[4]) and doing research on the project team are advised. If no actual person can be identified behind a project and only pseudo-names are being used, it is a red flag (Rosen, 2022).

If there are any limits on sale orders, it is an indication of a scam project. If no liquidity is locked and the price explodes with a small number of token holders, it should raise some questions. It is recommended to perform transaction and on-chain data analysis. It is most likely a rug pull if there is little trading activity and it appears only in a few decentralised exchanges (DEXs). Potential investors should stay calm and avoid FOMO. Excessive advertising content indicates a rug pull as most new coins normally starts slow and small. Other common signs to look out for are if the project appeared overnight, developers are anonymous, there is a low liquidity, the total value locked (TVL) is low, the liquidity is unlocked, disproportionate token distribution, low effort website and a lack of social media presence (Vardai, 2022).

In the case of NFTs, one should be a lot more discerning when buying or minting. Only 5% of NFT projects will be very profitable and 95% would probably go to zero. This type of investment is a very high risk, and one should do a lot of research before participating (Bureau, 2022).

4.3 Phishing Scam

An investor should never enter his seed phrase anywhere on a website to access the website or to send any funds. Leaving a seed phrase on your personal computer or in the cloud is a very risky. It has been reported that hackers have stolen $655K from one MetaMask[5] user by picking the seed from an iCloud backup. To avoid a seed phrase from being included in a backup, one should exclude the MetaMask (hot wallet) app from iCloud backups via the iOS settings. In addition, enabling two-factor authentication for MetaMask is advised. It is also recommended to keep cryptocurrencies in a cold wallet if they are not actively being traded. Keeping investments out of social media would make an individual less of a target as hackers are keeping an eye out for high-value victims (Toulas, 2022).

Another attack method is when the attacker gives a victim their seed phrase on a fraudulent site. When the victim installs the wallet and enters the seed thinking it is their seed, when in fact it is under the scammer's control. Once the victim sends funds to the wallet, the scammer runs off with it. Sometimes scammers will buy advertisement space on Google for their links to be visible before the actual real website is available, enticing users to click on these links and follow their installation steps (Akhtar, 2021). To avoid these scams, never click on any advertisements for crypto wallets. The attacker can try to make the victim connect their wallet to a fraudulent decentralised application (DApp), signing a smart contract and allowing the attacker to spend on their behalf. This scam is popular under the NFT DApps. An example of this occurred in 2021 where a Bored Ape Yacht Club[6] collector lost 16 high value NFTs, valued around $2.2 million, when he approved a phishing contract (Chawla, 2021). To avoid this type of scam, a user must make sure they are on the official DApp website and that they know which DApps they have approved. Etherscan[7] provides the functionality to show all the smart contracts a user has given approval to and when it was given. It also allows a user to revoke certain smart contracts that the user does not recognize.

[3] https://www.binance.com/en
[4] https://www.certik.com/projects/lcx
[5] https://metamask.io
[6] https://opensea.io/collection/boredapeyachtclub
[7] https://etherscan.io

4.4 Ponzi Scheme

To avoid a Ponzi scheme, one needs to be very sceptical and compare the returns to the market average. If the scheme is consistently above that average, it should raise suspicion. In addition, one should be able to find out exactly how an investment platform is generating returns (Bureau, 2022). The US SEC (Securities and Exchange Commission, 2022c) released a report detailing "red-flags" to help identify possible crypto Ponzi schemes - presented in Table 2.

Table 2: SEC Ponzi Scheme Red-Flags

Red flag	Description
Low-risk, high-returns	If an investment guarantees exceedingly attractive, high returns on investment, one should be very sceptical.
Overly consistent returns	If an investment does not fluctuate with market conditions, it could be an indicator of a Ponzi scheme.
Investments that are unregistered with an authority	If an investment is not regulated by some authority, it can be exceedingly difficult to determine the legitimacy thereof.
Unlicenced Sellers	Many Ponzi schemes consist of unlicensed sellers. If a seller is registered, it could indicate involvement with Ponzi schemes.
Overly complex fee structures	If the fee structures are too complex or secretive, it can be obscuring true intentions. Structures that are too complex to understand or are incomplete, should be avoided.
Minimum investor qualifications not necessary	Legitimate investment opportunities afforded to individuals generally require the investor to be accredited. If an investment does not require your net worth or salary, one should be sceptical.
Paperwork issues	If an investment opportunity is slow to produce paperwork/makes excuses as to why paperwork is unavailable in writing, one should be sceptical.

4.5 Pump and Dump

Pump-and-dumps are illegal and should always be avoided. Firstly, they occur in low market cap coins because it is easier to move the prices of these coins. Secondly, the coins will mostly be on shady exchanges. Thirdly, if there is no news about a certain coin's price increase, it is more likely the works of scammers. One can also look at previous trading volumes; if a token has had low trading volumes for the past few months and suddenly a spike occurs, it could be a clear sign of early accumulation. The pump operators need to buy the coins upfront before they dump them, therefore the accumulation waves need to be assessed (Bureau, 2022).

Pump-and-dump schemes are normally more based on hype and speculation than on a business model. They tend to create a heightened sense of urgency to invest. If a company is not yet profitable, common sense should be used as in to why one would invest. Potential investors should look at a company's financial statements and earnings report (Beers, 2022).

5. Conclusion

Blockchain adoption continues to increase and so does crypto-crimes and scams, especially since the Covid-19 pandemic. With job losses and salary cuts, people became desperate for a new source of income. The crypto space provided this opportunity, but it also created the perfect playground for scammers. This study highlights the most significant crypto-scams from 2020 to 2022, based on monetary losses and the number of users affected. The scams have been grouped according to type, the year they occurred, financial losses, country of origin, number of affected users and whether any arrests have been made. In addition, the study aims to raise awareness on protection against these scams. Recommendations are provided on identifying a specific scam and how to avoid them. Since there is no official legislation in place for crypto-scams, it remains a very significant international threat that cannot be ignored.

References

Akhtar, T. (2021, 11 4). *MetaMask, Phantom Wallet Users Targeted in Crypto Phishing Scam: Report*. Retrieved from Coindesk.com: https://www.coindesk.com/business/2021/11/04/crypto-phishing-scam-targets-metamask-phantom-wallet-users-report/

Andryukhin, A. (2019). Phishing Attacks and Preventions in Blockchain Based Projects. *International Conference on Engineering Technologies and Computer Science (EnT)* (pp. 15-19). Moscow: IEEE.

Baltrusaitis, J. (2022, September). *Thodex crypto exchange's CEO arrested for allegedly defrauding investors of $2.7 billion.* Retrieved from Finbold: Cryptocurrency News: https://finbold.com/thodex-crypto-exchanges-ceo-arrested-for-allegedly-defrauding-investors-of-2-7-billion/

Beers, B. (2022, 09 22). *Pump-and-dump scheme: What it is and how to avoid one*. Retrieved from Bankrate.com: https://www.bankrate.com/investing/pump-and-dump-scheme/

Berwick, A. (2022, November 14). *At least $1 billion of client funds missing at failed crypto firm FTX*. Retrieved from Reuters: https://www.reuters.com/markets/currencies/exclusive-least-1-billion-client-funds-missing-failed-crypto-firm-ftx-sources-2022-11-12/

Bureau, C. (2022, 5 18). *WORST Crypto Scams in 2022!! DONT Fall For These!!* Retrieved from YouTube: https://www.youtube.com/watch?v=GKTa5ciCJl4

ByBit Learn. (2021, August 27). *Why Crypto Rug Pulls Happen in DeFi — and How to Avoid Them*. Retrieved from ByBit Learn: https://learn.bybit.com/investing/why-crypto-rug-pulls-happen-in-defi/

Chainalysis. (2021). *The 2021 Crypto Crime Report.* Chainalysis. Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

Chawla, V. (2021, 12 30). *Bored Ape NFT Collector Loses $2.2M in Phishing Scam*. Retrieved from Cryptobriefing.com: https://cryptobriefing.com/bored-ape-nft-collector-loses-2-2m-in-phishing-scam/

Chen, J. (2021, 10 21). *Ponzi Scheme*. Retrieved from Investopedia: https://www.investopedia.com/terms/p/ponzischeme.asp

Commodity Futures Trading Commision. (2022, June 30). *CFTC Charges South African Pool Operator and CEO with $1.7 Billion Fraud Involving Bitcoin*. Retrieved from CFTC.gov: https://www.cftc.gov/PressRoom/PressReleases/8549-22

Forbes. (2022, September 20). *What Really Happened To LUNA Crypto?* Retrieved from Forbes Digital Assets: https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=302d8e074ff1

Hakki, T. (2021, October 31). *AnubisDAO Investors Lose $60 Million in Alleged Rug Pull*. Retrieved from Decrypt: https://decrypt.co/84924/anubisdao-investors-lose-60-million-in-alleged-rug-pull

Harper, C. (2020, August 19). *How The PlusToken Scam Absconded With Over 1 Percent Of The Bitcoin Supply*. Retrieved from Bitcoin Magazine: https://bitcoinmagazine.com/business/how-the-plustoken-scam-absconded-with-over-1-percent-of-the-bitcoin-supply

Hauer, T. (2020, 4 6). *Crypto giveaway scams and how to spot them*. Retrieved from blog.Coinbase.com: https://blog.coinbase.com/crypto-giveaway-scams-and-how-to-spot-them-59e24d220616

Investopedia. (2022, March 28). *How to Identify Cryptocurrency and ICO Scams*. Retrieved from Investopedia: https://www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/

Jacob, S. (2022, January 8). *Morris Coin scam: At least 1.1 million investors may have been cheated*. Retrieved from Business Standard: https://www.business-standard.com/article/companies/morris-coin-scam-at-least-1-1-million-investors-may-have-been-cheated-122010800045_1.html

Kamps, J. K. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science 7* (p. Article 18). Crime Science Journal. doi:https://doi.org/10.1186/s40163-018-0093-5

Kolhatkar, S. (2021, May 24). *DeFi100 Coin Scam: DeFi100 Creators Rug Pull Investors, Disappear With $32 Million*. Retrieved from Republic World: https://www.republicworld.com/technology-news/other-tech-news/defi100-coin-scam-defi100-creators-rug-pull-investors-disappear-with-32-dollars-million.html

Leng, S. (2020, December 1). *Chinese cryptocurrency scam ringleaders jailed in US$2.25 billion Ponzi scheme involving PlusToken platform*. Retrieved from China Macro Economy: https://www.scmp.com/economy/china-economy/article/3112115/chinese-cryptocurrency-scam-ringleaders-jailed-us225-billion

Moody, R. (2022, September 20). *Worldwide crypto & NFT rug pulls and scams tracker*. Retrieved from Comparitech: https://www.comparitech.com/crypto/cryptocurrency-scams/

Nelson, D. (2020, October 22). *Spanish Police Arrest Head of Billion-Dollar Crypto Arbitrage Platform on Fraud Allegations*. Retrieved from CoinDesk: https://www.coindesk.com/markets/2020/10/22/spanish-police-arrest-head-of-billion-dollar-crypto-arbitrage-platform-on-fraud-allegations/

Pimentel, B. (2022, March 8). *Two siblings were charged in a global $124 million crypto fraud operation*. Retrieved from Protocol: https://www.protocol.com/bulletins/ormeus-crypto-fraud

Radmilac, A. (2021, November 27). *Avalanche's first memecoin SDOG ends in a $30M possible rugpull*. Retrieved from Cryptoslate: https://cryptoslate.com/avalanches-first-memecoin-sdog-ends-in-a-30m-rugpull/

Rosen, A. (2022, 6 30). *How to Avoid 'Rug Pulls,' the Latest Cryptocurrency Scam*. Retrieved from Nerdwallet.com: https://www.nerdwallet.com/article/investing/rug-pull

Securities and Exchange Comission. (2022a, August 1). *SEC Charges Eleven Individuals in $300 Million Crypto Pyramid Scheme.* Retrieved from U.S. SEC Press Release: https://www.sec.gov/news/press-release/2022-134

Securities and Exchange Commission. (2022b, June 30). *SEC Charges Empires Consulting Corp. with Fake Trading Scheme*. Retrieved from U.S. SEC: https://www.sec.gov/news/press-release/2022-119

Securities and Exchange Commission. (2022c). *Ponzi schemes Using virtual Currencies.* Office of Investor Education and Advocacy. SEC. Retrieved from https://www.sec.gov/files/ia_virtualcurrencies.pdf

Social Links. (2022, April 22). *Enhancing Cryptocurrency Investigations with OSINT*. Retrieved from https://blog.sociallinks.io/: https://blog.sociallinks.io/cryptocurrency-investigations/

Sopov, V. (2021, April 03). *Largest Binance Smart Chain Fraud: Meerkat Finance (MKAT) Rug Pulled with $32 Million Losses*. Retrieved from U.Today: https://u.today/largest-binance-smart-chain-fraud-meerkat-finance-mkat-rug-pulled-with-32-million-losses

Tassev, L. (2021, November 12). *Finiko Fugitives Suspected of Moving 750 BTC From Crypto Pyramid's Wallet*. Retrieved from Bitcoin.com: https://news.bitcoin.com/finiko-fugitives-suspected-of-moving-750-btc-from-crypto-pyramids-wallet/

Toulas, B. (2022, 4 18). *Hackers steal $655K after picking MetaMask seed from iCloud backup*. Retrieved from BleepingComputer.com: https://www.bleepingcomputer.com/news/security/hackers-steal-655k-after-picking-metamask-seed-from-icloud-backup/

United States Department of Justice. (2022, March 24). *Nevada Man Admits Money Laundering and Tax Offenses Related to BitClub Network Fraud Scheme*. Retrieved from U.S. Attorney's Office: District of New Jersey: https://www.justice.gov/usao-nj/pr/nevada-man-admits-money-laundering-and-tax-offenses-related-bitclub-network-fraud-scheme#:~:text=NEWARK%2C%20N.J.%20%E2%80%93%20A%20Nevada%20man,U.S.%20District%20Judge%20Claire%20C.

Vardai, Z. (2022, 09 22). *How to avoid getting rug-pulled in crypto and DeFi*. Retrieved from forkast.news: https://forkast.news/how-avoid-getting-rug-pull-scammed-crypto-defi/

Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., . . . Liu, X. (2020). Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. *2020 APWG Symposium on Electronic Crime Research (eCrime)*, (pp. 1-14). doi:10.1109/eCrime51433.2020.9493255

Zimwara, T. (2021, August 3). *South Africa Bitcoin Heist: Court Grants Liquidators Authority to Track Missing Africrypt Investor Funds*. Retrieved from Bitcoin.com: https://news.bitcoin.com/south-africa-bitcoin-heist-court-grants-liquidators-authority-to-track-missing-africrypt-investor-funds/