Citação: (BARTOLETTI et al., 2021)

Tema: Cryptocurrency Scams: Analysis and Perspectives

Referencia bibliográfica: BARTOLETTI, M. et al. Cryptocurrency Scams: Analysis and Perspectives. **IEEE Access**, v. 9, p. 148353–148373, 2021.

Fichamento

|  |  |  |
| --- | --- | --- |
| Pagina | Texto | Comentário |
| 1 | there is a major concern about cryptocurrency scams, where fraudsters try to deceive investors to gain an undue Advantage |  |
| 2 | We define scam as any unlawful behaviour of one or more persons who intentionally deceive people to obtain something illegal or unfair. More specifically, in a crypto scam, fraudsters exploit one the peculiar features of blockchain technologies, i.e. the availability of crypto-assets that can be anonymously (or pseudonymously) exchanged for fiat currencies.  we do not consider ‘‘pump and dump’’ schemes, where fraudsters intentionally create hype on some crypto-assets in order to pump their prices and sell their stocks right away  Anti-Phishing Working Group [13] features an online reporting system which categorizes scam data into: (i) phishing URLs; (ii) phishing emails; (iii) malicious IPs; (iv) malicious domains; (v) cryptocurrency (suspicious exchanges, wallet providers, trading platforms, and investment fund).  we propose a taxonomy of crypto scams which consists of seven main features, which capture different types of illegal activity, and can be mixed to characterize hybrid scams. |  |
| 3 | A) PONZI SCHEMES  Ponzi schemes are scams that advertise themselves as highyield investment programmes (HYIPs) [14], [15]. They typically lure users with the promise of high profits in return for their investments by paying high levels of interest (see e.g. Figure 1). In practice, Ponzi schemes only pay users with the funds invested by new users, and therefore implode as soon as new investors stop joining. As a result, most investors in Ponzi schemes just lose their money. |  |
| 4 | B) MALWARE  The alleged untraceability of cryptocurrencies has been extensively exploited by malware developers. There are two types of malware closely related to cryptocurrencies:   1. Ransomware: After infecting the victim’s device, this kind of malware encrypts the data on the device, and locks it until the user pays a ransom (usually in Bitcoin). Figure 2 shows a screenshot of a device infected by Wannacry, along with the instructions to pay the ransom. 2. Crypto loggers This kind of malware tries to steal information about the victim’s accounts on crypto services (like, e.g., wallets). In particular, crypto loggers try to obtain the private key needed to transfer crypto-assets from the victim’s account to the fraudster’s. They often work as a transparent interface while the user is surfing the web, or is searching for password files |  |
| 5 - 6 | C) FAKE CRYPTO SERVICES  In the cryptocurrency ecosystem, there are multiple services to simplify their use and management. They include exchange services, wallets and mixers. However, numerous criminals develop these types of services in the form of fraud, as described below.   1. **Fake exchange** Fake exchange frauds deceive users by offering incredibly competitive market prices for purchasing cryptocurrencies. Indeed, they trick users with quick and easy access to some cheap currency. Figure 3 shows a fake exchange service at paybillsbitcoin.com, mirrored from BtcToPal.com. 2. **Fake wallet** Wallet services allow users to manage, send and receive cryptocurrencies. In this scenario, users can run into wallet scams characterised by various types of fraudulent behaviour. For example, some wallets steal the entire amount indiscriminately, while others take a small percentage of the daily deposit. Finally, others withdraw when the deposit exceeds a certain threshold. 3. **Fake mixing** Transactions in blockchain systems (e.g. Bitcoin) are linked together, so it is possible to inspect cryptocurrency movements between addresses. However, mixing services make it possible to erase the links between initial and final addresses, randomise the number of transactions, add delays to transactions, and use other extraneous addresses. On the other hand, fake mixers receive the money and steal it without sending it to the client. Figure 1 was a website of a fake mixer called ’’BitcoinMixer’’, online up to December 30, 2020. Several users sent money to this fake mixer and never received it back, as reported on BitcoinTalk. Moreover, a BitcoinTalk topic shows a list of fake mixers 4. **Fake mining pool** Cryptocurrencies based on the Proof Of Work (POW) mechanism require a computational effort to create blocks. Therefore, users who create blocks, called miners, receive a reward. This type of scam asks users to participate by investing money to buy mining hardware. Despite what the scam promised, the money invested is not used to buy new hardware but rather to pay interest to previously registered users. 5. **Fake donation** Usually, donors make donations to projects or people for good. Fraudsters exploit people’s virtue, creating fake donation campaigns, and instead of giving the money as a donation, they steal the money and disappear |  |
| 7 | Andryukhin [43] reviewed and classified the prominent frauds that occurred in blockchains, how the fraudsters implemented them, and how to mitigate scams. While analysing social engineering attacks, the authors found ’’Clone’’, a clone website to create IOTA wallet keys, and estimated that USD 4 million worth of MIOTA tokens had been stolen.  Holub and O’Connor [7] tracked a Bitcoin phishing campaign called ’’Coinhoarder’’ for over six months. The campaign theft USD 10 million by launching typosquatting domains containing clones of crypto exchange websites. For example, they find ’’block-chain.info’’ and ’’blockchian.info/wallet’’.  D) ADVANCE-FEE SCAMS  According to the FBI [49], ‘‘An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return.’’ In an advance-fee scam, scammers typically contact the victim via e-mail or social media using a fake e-mail address or social media account. They promise the victim a significant amount of money in exchange for a small upfront payment that scammers claim will use to obtain a substantial sum as a reward. If the victim makes the payment, the scammer either disappears or adds several additional charges that the victim has to pay. Recently, several of these scams campaigns have taken place on Twitter, using well-known personalities such as Elon Musk, as shown in Figure 6 example |  |
| 8 – 9 | E. BLACKMAIL  In blackmail scams, fraudsters usually claim to have hacked the victim’s device, and installed a key logger, or recorded the victim with the webcam. The mail typically asks for a ransom in Bitcoin to delete the material, threatening that they will otherwise sell it, or publish on social networks. Figure 7 shows an actual example of blackmail that the scammer sent to a potential victim. More advanced fraudsters tailor personalised emails to victims, by exploiting databases of emails and hacked passwords  F. FAKE ICO  An Initial Coin Offering (ICO) is a way for blockchainrelated currencies to raise funds before their official launch similar in many ways to Initial Public Offerings for shares. Fake ICO scams apply the same strategy by luring users into buying fake coins. Typically, a cryptocurrency company releases a predetermined number of coins on the open market in the same way that shares are issued when a company goes public. Many ICOs are legitimate cryptocurrencies that have the potential to make an investor as much money as any other stock [53]. Fake cryptocurrencies advertise themselves with peculiar features that others do not have via brand new websites. To try to mitigate this problem, the SEC launched a parody website in 2018 that mocks ICO [54], along with a fake eight-page white paper, fake celebrity endorsements, and a fake team working on the ICO. According to a study realised by Satis Group in 2018, approximately 80% of ICOs conducted in 2017 were scams, with no actual product to offer [55]. Moreover, in 2017, ICO gained USD 1.6 billion, of which USD 150 million belongs to fake ones [43].  To cite some examples of Fake ICO scams [53], [55], Pincoin was launched in 2018 and raised USD 660 million. PlexCoin in 2017 raised USD 8.5 million, while Bitconnect in 2016, reached a market cap of over USD 2.6 billion. OneCoin is perhaps the most famous. It was launched in 2014 as a mined cryptocurrency even though it was a Ponzi scheme. The FBI discovered it raised to USD 4 billion in income. Savedroid was funded in 2015 and raised USD 50 million until 2018. At the time of writing, it is still listed on exchanges. Finally, AriseCoin was an ICO attempt by a fake bank named AriseBank. The SEC stopped it in January 2018. |  |
| 9 | G. MONEY LAUNDERING Money laundering consists of making large amounts of money obtained from illegal activities appear to come from legitimate sources. It consists of three stages: placement, layering and integration. In the first stage, dirty money is introduced into the legitimate financial system. Then, the money is moved several times to create confusion, moving through numerous accounts. Finally, it is integrated into the financial system through further transactions until the process is completed. The main problem associated with this criminal activity is to make the proceeds legal without arousing the suspicion of law enforcement. |  |
| 19 | Based on our experience, we provide the following recommendations for counteracting crypto scam  A. RECOMMENDATION #1.  IMPROVE SCAM REPORTING SYSTEMS As we have noted in Section III, the existing public data sources on crypto scams are heterogeneous, and not completely reliable. This hampers the development of effective scam detection and classification tools, for which it would be crucial to have a uniform and reliable dataset of scam. To overcome these issues, our recommendation is to construct a scam reporting system which is comprehensive (i.e., it allows users to report scams of any type, targeted to any blockchain), with a uniform taxonomy of scams (like, e.g., the one we have proposed in Section II) and moderated, so to reduce the amount of spurious or incorrect data. Further, this system should guide users towards the correct self-classification of scams, e.g. by providing an interactive questionnaire, and by showing scam templates of the various types.  B. RECOMMENDATION #2. DEVELOP A BROWSER EXTENSION TO WARN AGAINST SCAMS A success factor of cryptocurrency scams, besides users’ greediness, is that non-technical users often find it difficult to distinguish fraudulent websites from legit ones. Accordingly, we recommend the implementation of a browser extension which inspects websites, alerts users when it detects potential scams, and advises users what to do if they have already been scammed. Similarly, the browser extension could alert users when they try to send money to blockchain addresses related to scams, or when they read blackmails. Our toolchain can be the basis for developing such a browser extension. | Conclusão |