Hornuf, Lars; Kück, Theresa; Schwienbacher, Armin

Working Paper

Initial Coin Offerings, Information Disclosure, and Fraud

CESifo Working Paper, No. 7962

Provided in Cooperation with:
Ifo Institute – Leibniz Institute for Economic Research at the University of Munich

Suggested Citation: Hornuf, Lars; Kück, Theresa; Schwienbacher, Armin (2019) : Initial Coin Offerings, Information Disclosure, and Fraud, CESifo Working Paper, No. 7962, Center for Economic Studies and ifo Institute (CESifo), Munich

This Version is available at:
https://hdl.handle.net/10419/214964

CESifo WORKING PAPERS

7962
2019

November 2019

Initial Coin Offerings, Information Disclosure, and Fraud

Lars Hornuf, Theresa Kück, Armin Schwienbacher

CESifo

Impressum:

CESifo Working Papers
ISSN 2364-1428 (electronic version)
Publisher and distributor: Munich Society for the Promotion of Economic Research - CESifo GmbH
The international platform of Ludwigs-Maximilians University's Center for Economic Studies and the ifo Institute
Poschingerstr. 5, 81679 Munich, Germany
Telephone +49 (0)89 2180-2740, Telefax +49 (0)89 2180-17845, email office@cesifo.de
Editor: Clemens Fuest
www.cesifo-group.org/wp

An electronic version of the paper may be downloaded
· from the SSRN website: www.SSRN.com
· from the RePEc website: www.RePEc.org
· from the CESifo website: www.CESifo-group.org/wp

CESifo *Working Paper No. 7962*

Initial Coin Offerings, Information Disclosure, and Fraud

Abstract

We study the extent of fraud in initial coin offerings (ICOs), and whether information disclosure prior to the issuance predicts fraud. We document different types of fraud, and that fraudulent ICOs are on average much larger than the sample average. Issuers that disclose their code on GitHub are more likely to be targeted by phishing and hacker activities, which suggests that there are risks related to disclosing the code. Generally, we find it extremely difficult to predict fraud with the information available at the time of issuance. This calls for the need to install a third-party that certifies the quality of the issuers, such as specialized platforms, or the engagement of institutional investors and venture capital funds that can perform a due diligence and thus verify the quality of the project.

JEL-Codes: G180, G380, M130.

Keywords: initial coin offering, fraud, crypto-currencies, crowdsales.

Lars Hornuf
University of Bremen
Faculty of Business Studies and Economics
Max-von-Laue-Straße 1
Germany – 28359 Bremen
hornuf@uni-bremen.de

Theresa Kück
University of Bremen
Faculty of Business Studies and Economics
Max-von-Laue-Straße 1
Germany – 28359 Bremen
thkueck@uni-bremen.de

Armin Schwienbacher
SKEMA Business School
Université Côte d'Azur
Avenue Willy Brandt
France – 59777 Euralille
armin.schwienbacher@skema.edu

This Version: November 19, 2019
We thank the participants of the paper development workshop *Developments in Entrepreneurial Finance: Crowdfunding, Blockchain, and ICOs* at Lyon Business School and the *3th European Alternative Finance Research Conference* at Utrecht University for their valuable comments and suggestions.

1. INTRODUCTION

Since the advent of Bitcoin in 2008, which until today remains the most widely used digital currency worldwide, digital currencies have gained in popularity. More recently, tokens based on different blockchains have been created to raise funds from a large crowd of people for the development of a project or firm (Adhami et al., 2018; Fish, 2019). At the same time, concerns about fraud have arisen, claiming that many of these Initial Coin Offering (ICOs) are scams (Liebau and Schueffel, 2019). We investigate whether information provided prior to the ICO gives hints on the risk of fraud, and document the severity of the phenomenon.

Similar to an initial public offering of corporate securities where a prospectus is published before the securities issuance, firms planning an ICO draft a whitepaper, which in the past was not formally approved by financial markets authorities. In this study, we collect detailed information from the whitepapers for a sample of 1,393 ICOs that took place worldwide from September 2016 to July 2018. We have coded the whitepapers along various dimensions in terms of type and extent of information provided to investors. Regulators and professionals have been arguing that different indicators, so-called red flags, may hint to the fact that an ICO could be a fraud (Kaal, 2017). These include, for example, whether there is a soft cap during the ICO, whether sufficient information is available on the founders or how the funds will be spent. We construct measures for a large range of these red flags to study their predictive power. In a next step, we run a rigorous search of fraud cases that were reported in the media. A thorough search is done for every ICO in our sample.

We obtain the following results. First, we were able to classify fraudulent behavior into seven categories. Some fraud cases even fall into more than one category. Fraud can originate from corporate outsiders or the issuers itself. Most often, fraudsters deceive investors of ICOs through phishing attacks, in which case external fraudsters or the issuer itself unduly gets hold of the investments. Frequently, the issuer also simply disappears after receiving the funds, which has often been referred to as exit fraud. In total, we could identify 274 fraud cases within the 1,393 ICOs studied; 188 suspected and 175 confirmed fraud cases. Second, we find that whether specific information is disclosed hardly predicts whether an issuer is fraudulent or not. In other words, the information provided during the issuance is hardly useful to predict whether the venture behind the ICOs is a fraud. The information provided by the issuer may simply be wrong and unreliable in the first place, which indicates a need to externally verify the information that is voluntarily provided.

Two important factors relate to fraudulent cases. The first is the amount raised, as ICOs that eventually are found to be fraudulent raise on average almost four times more money. While the causal relation is unclear, one possible reason for this positive relation is that the incentives to fraud are greater the more money is raised (Becker, 1968). Corporate outsiders and insiders such as founders may be more tempted to fraud. In economic terms, a one-standard deviation increases in the amount raised is associated with an increase in the fraud probability of 38%. The second factor predicting fraud is whether the code of the venture was disclosed on GitHub, a platform where startups can post their code in order for others to verify the lack of errors. Disclosing the code on GitHub is generally viewed as a sign of trustworthiness and transparency and thus helpful to raise more money (Dabbish et al., 2012; Amsden and Schweizer, 2019; Howell

et al., 2019). However, we document that this increases the likelihood of phishing by corporate outsiders by 7%, thereby also generating risks for investors and the startup. This finding is new in the literature and of great importance for the tech community.

The remainder of the article is structured as follows. In a first step, we provide examples of business models that have used ICOs to raise capital and common types of fraud involved (Section 2). Thereafter, we present our data and results (Section 3 and 4). Finally, we discuss our findings and provide policy conclusions (Section 5).

2. BUSINESS MODELS BUILDING ON THE BLOCKCHAIN AND ICOs

Digitalization has brought new forms of finance for startups. Crowdfunding was probably the first form in this development. The first platforms have emerged in 2008 and the industry has professionalized, with significant growth rates every year since then[1]. However, new technologies have brought the digitalization a step further, including the invention of the blockchain, which enables new forms of contracting and issuance of tokens and securities. Recently, startups have started using the blockchain to raise money in the form of an ICO.

An ICO, which is sometimes referred to as *crowdsale*, can be chosen for different reasons. The simplest form of an ICO is done by a newly created startup in need for initial funding to develop a product or service. In an ICO, the owners launch a crowdfunding campaign to raise money in exchange for tokens. These tokens can be used by backers to consume a product or service, which

[1] See Cumming et al. (2019a) for an analysis of the limited number of fraud cases in crowdfunding.

the startup plans to develop in the future. For example, the token can become a means of exchange for services provided on the platform that is supposed to be created. In this case the tokens created are often referred to as *utility tokens*. Unlike in the traditional crowdfunding model that takes place on platforms like Kickstarter and where the creators describe their project in a pitch on the website, in an ICO the founders outline their project in a whitepaper. Whitepapers have no standardized format and describe the product or service to be developed and how the ICO is going to take place. While the funds the startup uses are published publically on the blockchain, there is no auditing of the project spending based on the funds that have been raised once the ICO is completed.

While this business model largely resembles reward-based crowdfunding, there are also many differences. First, the tokens will be created through an ICO so that the crowd can buy more tokens than what they need for consumption purposes, because the excess tokens can be resold on the secondary market. Moreover, the fact that the tokens are traded later makes them a tradable asset, more in line with a security-type. In fact, since trading takes place on exchanges before the platform goes online, investors may also participate in the ICO by buying tokens with the intention of selling them shortly after on an exchange to make profits. In some cases, tokens are not created as means of payments for services provided on the platform, but the sole purpose of the token is to participate in the future profits of the startup. In this case, the tokens created are referred to as *securities* or *investment tokens*.

Finally, the value of the tokens is related to the chances of project success. If the project cannot be developed, the tokens become essentially worthless. In contrast, the value of the token appreciates when the project becomes successful so that early backers benefits too. Most often,

startups use Ethereum as the blockchain of choice as this was one of the first blockchains that supports complex and autonomous self-executing contracts. In some cases, the issuer also creates an independent blockchain on which the token is running.

2.1. Examples of ICOs

An ICO is a new and innovative model of financing a venture, in which there exists a multitude of different business models. We consider the common characteristics of an ICO by analyzing some of the earliest cases that have emerged.

In April 2016, the German developer Simon Jentzsch had developed one of the first digital decentralized autonomous organization *The DAO*. The DAO resembled a venture capital fund that no longer relied on hired investment managers and a board of directors but on autonomous self-executing contracts. While investors of traditional investment funds typically face an agency problem, where fund managers potentially act in their personal interest and not in their investors' best interest, The DAO intended to solve this problem by leaving the decision-making process of the venture capital fund to computer algorithms and the owners. Unlike many other crowdfunding campaigns The DAO was not funded with USD or EUR but by means of Ether Tokens ("1 ETH") of the Ethereum blockchain. In an ICO The DAO raised 11.5 million Ether, which were at the time worth around 150 million USD. Owners maintain a pro rata voting right in line with their token share in the organization. Any profits The DAO would have generated in the future were supposed to be distributed according to the token share the respective investors held. Investors had a right to withdraw their initial Ether investment until they executed their voting right in the venture capital fund for the first time. It is worth mentioning that only one month after the The

DAO's ICO, potential hackers diverted around 3.6 million Ether worth around 50 million USD away. The problem was solved by what is called a hard fork, but The DAO failed quickly thereafter.

Another example of an ICO is the eSports platform FirstBlood. In October 2016, the platform issued almost 86 billion FirstBlood Token ("1 S₮") worth 465,313 Ether (ETH) in an ICO. Many ICOs try to generate momentum in the ICO early on. FirstBlood initiated a "power hour" during the first hour of the ICO, when FirstBlood tokens were offered at a rate of 170 1S₮ to 1 ETH. Thereafter, the rate was adjusted to 150 1S₮ to 1 ETH. Finally, the rate was linearly decrease every week until it stood at 100 1S₮ to 1 ETH. Unlike The DAO, FirstBlood capped the ICO at the equivalent of 5.5 million USD, which the start-up raised in 58 seconds. After that ceiling was reached the algorithm did no longer accept investments. At the end of the ICO, token transfers were locked for two months. The proceeds raised in the ICO were used for the development, release, and operation of the eSports platform FirstBlood. In a next step, players could earn tokens depending on their skills in eSports contests. Like The DAO, FirstBlood was built on top of the Ethereum blockchain. In the case of an eSports platform self-executing contracts help to settle disputes among players and verify game results.

ChronoBank was an ICO that seeks to establish an international market for labour-hours. The platform specializes in occupations such as e-commerce support, cleaning, warehousing, industrial work, construction, and freelancing. ChronoBank issued two types of tokens: Labour-Hour Tokens ("1 LHT") and TIME tokens. TIME tokens guarantee their holders a share of the fees involved in issuing and transacting Labour-Hour tokens. TIME tokens can thus be thought of as dividend paying shares of the ChronoBank organization. Labour-Hour tokens are more like a currency used by users to trade their labor. Overall, 88% of the TIME tokens were issued to the

crowd, 10% were maintained by the ChronoBank team, and 2% are reserved for early contributors and advisors. Self-executing contracts enable Labour-Hour Tokens to be redeemed for labor-hours through traditional, legally binding contracts with labor-offering companies.

In sum, many tokens created during an ICO are transferable and tradeable on a platform. However, some tokens have properties of a currency or units of account and others are more similar to a security. If they come with rights attached similar to the ownership rights of a firm, regulators might indeed classify them as securities.

2.2. When are Tokens Securities?

From a legal perspective, offering securities that are not registered is illegal. Thus, the question is whether the token created constitutes a security. In the United States, whether a transaction involves a security is determined by means of the Howey test, which was developed in the seminal SEC v. W. J. Howey Co. court judgement. According to the test, a security is involved in a transaction if someone (1) invests his money in (2) a common enterprise and is led to (3) expect profits (4) solely from the efforts of the promoter or a third party. According to Alberts und Fry (2015), cryptocurrencies are generally not securities because they are lacking two important criteria outlined in the Howey test. First, cryptocurrencies like Bitcoin are not investments in a common enterprise, as they can be used to make any form of payment. Second, the purchasers cannot expect profits from the purchase based on the efforts of the seller of the cryptocurrency. Nevertheless, in SEC v. Shavers the SEC has applied securities regulation to investment funds that have invested in Bitcoin companies.

Valkenburgh (2016) notes that the Howey test is an efficient guide for deciding whether tokens pose a threat to their users. The more the token fits under the definition of a security, the more its users should be protected by regulation. Whether a token is considered a security largely depends on the way it is used. In any ICO, individuals directly or indirectly invest their money. While the investment in the tokens that are created during an ICO requires the use of a cryptocurrency, backers can invest fiat money in cryptocurrencies via a third-party conversion service. Per definition an ICO involves the investment in a common enterprise, namely the project or firm to be developed by the founder. The third criterion is arguably not always fulfilled in an ICO. While some backers might use their investment speculating that the venture itself and tokens become more valuable, others might solely use their tokens as unit of exchange to transact on the platform. In the latter case, the tokens might maintain a stable value and could be considered as a utility token. The difference whether a token constitutes a security or not might in fact come from the nature of the token and the respective business model of the startup.

Some tokens are exhaustible and considered as a product, where the consumption of the token acts as proof of this claim. On the other hand, non-exhaustible token may be considered a form of memberships. In this case, the transaction underlying the ICO can be seen as a form of compensation rather than investment. In Europe, MiFID II, Article 4, 1. (44) defines what transferable securities are. Generally, securities must be transferable and tradeable on financial markets, they should not be payment instruments and they should have rights attached similar to the ownership rights of a firm.

2.3 Examples of Fraud Cases

Exit Fraud

In many cases, ICO issuers do not have the intention to build up a business, but instead to disappear with the collected money. This type of fraud is often referred to as *Exit Fraud*, and is often combined with a fake team in which fictious people are presented as team members of the ICO. The fraudsters of the ICO Benebit, for example, used photos of employees of a school in the U.K. to represent a team.[2] This, however, became public after the fraudsters had already raised $2.7 million USD through the ICO. Before the ICO started, the issuer tried to look as legal and reliable as possible. They were active on social media and, for example, on twitter for over a year before the ICO began. In addition, they spent around $500,000 USD for marketing purposes and were highly rated by ICO review websites. But as soon as they were detected as fraudsters, the website of Benebit disappeared and the social media accounts were deleted.[3]

Securities Fraud

After the SEC published the DAO Report in July 2017, the regulator sued several companies for securities offering by means of unregistered digital tokens. One recent case is the offering of Kin Token by the Canadian company Kik Interactive Inc. Kik is running a messaging application named Kik Messenger but due to a decreasing number of app-users and low revenues, the company faced liquidity problems in late 2016. In order to recover from this financial distress, the company created the Kin Token and started an ICO in May 2017. In the published whitepaper, the founder

[2] www.thsboys.org.uk/school-information/staff/
[3] https://news.bitcoin.com/benebit-ico-runner-2-7-million-investor-funds/

of the company stated to develop the "Kin Ecosystem," in which the token holder can use Kin to purchase goods and services. Moreover, the value of the token would increase due to a limited number of tokens. The company raised funds of approximately $100 million USD from more than 10,000 investors, of which more than half were U.S. investors.[4] In June 2019, the SEC concluded that the token offering by Kik fulfils the four criteria of the Howey test: *"Investor's purchases of Kin were an investment of money (1), in a common enterprise (2), with an expectation of profits for both Kik and the offerees (3), derived primarily from the future efforts of Kik and others to build the Kin Ecosystem and drive demand for Kin (4). Consequently, Kik's offers and sale of Kin in 2017 was an offer and sale of securities."*[5] For this reason, the SEC sued Kik Interactive Inc. for unregistered security offering in the federal court of Manhattan, New York.[6]

Ponzi Scheme

Another example of fraudulent activities in the ICO market is the crypto-lending platform Bitconnect with its token BCC. The England-based company successfully ran an ICO in December 2016, performed as one of the best cryptocurrencies on coinmarketcap.com in 2017, and, according to Bitconnect, it represented a market value of $4.1 billion USD.[7] Bitconnects business model was based on the following scheme. After investors deposited their Bitcoin into the Bitconnect BCC exchange platform and purchased its digital token BCC, the investors could use the token for two programs: First, investors can lend their token back to Bitconnect as part of its

[4] https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf
[5] https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf
[6] https://www.nytimes.com/2019/06/04/business/sec-kik-kin-coin.html
[7] Chohan (2018): Bitconnect and Cryptocurrency Accountability; https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales

"Bitconnect Lending Program." Bitconnect pretended to reinvest this token and promised a monthly return of up to 40%. Second, Bitconnect guaranteed a monthly return of up to 10%, if the investor holds the token for more than fifteen days in his or her BitConnetQT-wallet ("Bitconnect Staking Program"). In January 2018, the Texas State Securities Board and the North Carolina Securities Division aimed to shut down Bitconnects business with cease and desist letters due to an unregistered security offering of BCC. Additionally, through the guaranteed investment returns the regulators stated that Bitconnects business model resembles a *Ponzi Scheme*. In February 2019, also the FBI started investigating against Bitconnect.[8]

Pump and Dump, Phishing, and Hacking

Fraud in the ICO market does not necessarily emanate from the company running the ICO, something we call external fraud in our analysis. Another fraud category are *Pump and Dump* schemes, which have been investigated in the context of ICOs by Hamrick et al. (2018) and (Li et al., 2019). In a pump and dump scheme, a fraudster artificially inflates the price of a token through false information, in order to sell the token that was initially cheaply bought at a higher price.

Moreover, numerous examples show that fraudsters are active in sending phishing mails or hacking into company's IT systems. This, for example, was the case with the Israel-based ICO crypto portfolio management platform named CoinDash. As soon as the public ICO-phase started in July 2017, a malicious attacker changed the official wallet address on the CoinDash's website. Thus, investors sent their money to the false address until CoinDash shut down the website and,

[8] https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/seeking-potential-victims-in-bitconnect-investigation

according to Coindash's blog, the hackers captured 43,000 ETH within seven minutes.[9] In September 2017 and February 2018, Coindash announced that the hackers sent back 10,000 ETH and 20,000 ETH, respectively. In a similar way, fraudsters could steal around $1 million USD from potential investors of the ICO The Bee Token. While the ICO was running, investors who fell victim to phishing mails sent their money to false wallet addresses.[10] The company confirmed the phishing attack and suspected that the attackers were able to gain personal information in form of e-mail addresses, first names and surnames through illegal access to a third-party vendor.[11]

Other Fraud

Besides these frequent and well-documented forms of fraud, there have already been numerous other ways in which investors have been cheated by ICO companies or corporate outsiders. Some ICOs falsely claim to have partnerships with well-known companies such as Boeing, PayPal or Walt Disney – this was the case with the ICO Titanium Blockchain.[12] DeCLOUDs was another ICO, which sought to establish a decentralized trading platform of precious metals like platinum, gold, silver, and palladium. The self-executing contracts were developed by Stas Nikolaev and Christian Schroeder. According to the white paper of the ICO the advantage of deCLOUDs is that it enables investors to trade precious metals on a peer-to-peer basis via an alternative stock market and to earn returns from the appreciation of precious metals. How the latter benefit of deCLOUDs would materialize remained unclear from the white paper. Another benefit of deCLOUDs was that investors could use precious metals to purchase consumer products or services. Like other ICOs,

[9] https://blog.coindash.io/coindash-tge-hack-findings-report-15-11-17-9657465192e1
[10] https://www.coindesk.com/bee-token-phishing-scam
[11] https://medium.com/@thebeetoken/security-update-on-the-phishing-incident-c8ff647841b8
[12] https://www.sec.gov/litigation/complaints/2018/comp-pr2018-94.pdf

deCLOUDs offered special terms for early bird investors. DeCLOUDs generated 100 million deCLOUDs tokens, out of which 80 million were distributed to the crowd in the ICO, 10 million were kept by the developer team, and 10 million are reserved for early contributors and strategic partners. According to deCLOUDs the German DAB bank supported the startup with a 5 million EUR investment. As it turned out, the picture was a scam and the founders disappeared with the money they had collected.[13]

3. DATA COLLECTION

3.1. Methodology for data collection

Our sample consists of 1,393 ICOs, which are listed on Icobench.com and Icorating.com, and ended their fundraising campaign before July 1st, 2018. The first ICO in our sample started in September 2016. Both websites belong to the largest ICO listing websites worldwide. These websites provide information on the ICOs, such as financial details, team information, links to social media channels, and ICO characteristics like pre-ICO phase, token ticker or location of the ICO issuer (Huang et al., 2019). This information was collected with the help of screen scraping.

Identifying fraud cases with certainty is not possible, because of the short time since the ICOs took place and the rare incidence of final judicial decisions. Also, the public often uses the term "scam" for simply referring to the fact that many projects are bad. However, the mere fact that a project has bad business prospects does not make it a scam. Fraud assumes some form of intent

[13] See https://medium.com/@playkey/how-to-tell-if-an-ico-is-a-scam-df00c6f0047c

to deceive investors by either the issuer or some outsiders. This is particularly difficult to prove, so our focus is on suspected and confirmed fraud. Suspected fraud refers to media coverage about fraudulent campaigns on high-quality print or online media. Reports about a bad business model or simply claiming that the founders are fraudsters is not enough to classify the ICO as suspected fraud. Confirmed fraud refers to cases where a trustworthy source like the SEC, another governmental agency, or the ICO issuer itself has confirmed that the fraud took place. We also considered exit frauds as confirmed when the communication with the issuer stopped two weeks after the end of the funding period and was not initiated again. Confirmed exit frauds were also often associated with a disappearance of the website of the issuer.

Because we focus on fraud, our sample will inevitably be smaller than a sample of projects with bad business prospects. Different methods have been proposed to identify fraud. For example, a recent article in the Wall Street Journal suggested to look at plagiarism in the whitepaper text.[14] However, such an approach will necessarily lead to many falsely identified fraud cases, because honest issuers could copy the content of whitepapers to save in legal and administrative costs, a behavior often observed in the fintech domain (Dorfleitner et al., 2019). Through the increasing standardization of whitepaper formats, there is further an increasing use of templates, which leads to plagiarism for other reasons than the type of fraud we are examining here. Our method is therefore more conservative to ensure reliability in the cases we classify as fraud, at the expense of possibly missing some fraudulent issuers out.

[14] See https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115 (last viewed on October 16, 2019).

To identify ICO fraud cases, we rely on the method that was developed by Cumming et al. (2019a) for crowdfunding. From October 2018 to January 2019, we ran an extensive search on Google and searched for the following three terms: 1) name of the ICO, 2) "ICO" and 3) "fraud" or different synonyms for fraud: "scam", "phishing", "pump and dump" and "ponzi". Based on this method, we could identify 274 fraud cases; 188 suspected and 175 confirmed fraud cases. Some ICOs were classified as suspected and confirmed fraud, because multiple fraud types were involved out of the seven categories described in Section 2.3. To ensure that our coding system is reliable and coherent, detailed explanations were provided for each fraud category and when to classify a scam as suspected or confirmed (see Appendix Table 1). In particular, we had a second researcher, who was not involved in the project, code all fraud categories independently. Finally, in case or coding was not consistent with the second researcher, we discussed the coding and in four cases had the reclassify the respective fraud category.[15]

3.2. Summary Statistics on Fraud Cases

Table 1 summarizes our findings in terms of number of fraud cases identified, by fraud type. The most common fraud category are phishing attacks. The bulk of phishing attacks were formally confirmed by the founders, after they detected them, feared that their funds get stolen, and consequently warned their investors. The next most common fraud type is exit fraud, for which 25 could be confirmed and 21 were suspected. For all other categories, suspected fraud cases are more common than confirmed fraud cases. In case of securities fraud the ICO issue was sometimes accompanied by one of the other fraud types. So far, we were able to identify 13

[15] In nine cases we had to change the detected to a suspected fraud and vice versa.

suspected security fraud cases, but only 3 confirmed one. Furthermore, we were able to identify one confirmed Pump and Dump scheme, with 31 suspected cases. Finally, 27 ICOs were related to a Ponzi scheme.

- Table 1 around here -

3.3. Summary Statistics on ICOs

Table 3 presents summary statistics for our sample. All variables are defined in Table 2. In terms of general sample characteristics, 88.7% of the ICO have used the Ethereum blockchain. On average, 57.1% of the token are offered during the ICO, and only 44.1% do a pre-sale prior to the funding period. Founder information, such as the number of founders involved in the project is included in 94.1% of the whitepapers (*Team info available*). This percentage is slightly lower for fraudulent cases, as expected. Finally, information on how much was ultimately raised (*Amount raised*) could be retrieved in 61% of the cases only, despite extensive and systematic search efforts.

There is great variation in the amount raised between the ICOs in the sample, with an average of USD 18.8 million and a median of USD 6.3 million. With USD 41.4 million the average amount is, however, significantly higher for fraudulent cases, which are the ICOs where the benefits from fraud are also highest. One further possible reason for this difference is that ICOs that have been identified as being fraudulent during the first days of the issuance will be stopped early on and

thus not included in our sample. All our fraudulent cases are those that have been identified as such after the ICO was over.

While overall fraudulent ICOs tend to have disclosed less information, the differences in disclosure are not statistically significant in a multivariate setting as we will show below. Differences may appear in the quality of the information, something which however is more difficult to assess for non-professional investors. An important difference here concerns information disclosure on how the funds are going to be used, which is only provided in 28.5% of the fraudulent cases as opposed to 45.4% for non-fraudulent cases. However, as will be shown below, it hardly helps predict fraud. There are also no meaningful differences in terms of number of social media used. In terms of financial details included in the offering, one important difference is the presence of a soft cap, which is less common in the fraudulent cases (28.5% versus 44.6%).

- Table 2 around here -

Fraudulent ICOs show important differences as compared to the remaining ICOs that were not identified as fraudulent. ICOs that are frauds are by far larger in terms of funds raised. While some of this difference may be attributed to the fact that fraud is less likely when the amount collected is particularly small, because the gains from a fraud is limited, we still observe a large difference when considering only ICOs that raised at least USD 15 million. The positive relationship between the amount raised during the ICO and fraud is confirmed in a multivariate regression setting (see Table 4).

- Table 3 around here -

There may be differences in the quality of information that was not captured in our study and that require – similar to venture capital investments – a good understanding about the ICO process and a due diligence of risky projects by investors. For example, the case of deCLOUDs has shown that posting a photo with German DAB bank with the intention to certify the quality of the ICO is not sufficient for the issuer to provide a credible quality signal, because the signal itself must be verified and non-fraudulent. Especially retail investors may refrain from collecting more information due to the cost of verifying these signals relative to the small size of their investments.

4. RESULTS

We now turn to assessing whether the differences between fraudulent and non-fraudulent ICOs identified in the univariate analysis also hold in the multivariate setting. To this end, we run Probit regressions with three separate dummy variables: *Confirmed Fraud*, *Suspected Fraud*, and *Fraud*. The latter equals 1 if an ICO is either a suspected or confirmed fraud, and thus combines both subcategories in one variable. Results are presented in Table 4. We include a large set of factors, while ensuring limited multicollinearity issues among our explanatory variables. Models (1)-(3) uses the largest possible sample based on a large set of factors. In Models (4)-(6), we further include *Amount raised* and *Token distributed* as additional factors. In particular, adding the variable *Amount raised* is useful given that we found in the univariate setting that fraudulent ICOs raised almost four times more than non-fraudulent ones. These additions, however, reduce our sample to about half.

- Table 4 around here -

Most factors are not significant, hinting to the fact that predicting fraud is very difficult. The presence of a soft cap reduces the risk of fraud; however, this significant result disappears when controlling for the amount raised. One reason why a soft cap could reduce fraud is because a larger soft cap requires a large participation by investors, similar to the all-or-nothing effect in crowdfunding (Cumming et al., 2019b). If not enough investors find the issuance sufficiently trustworthy and valuable, it will fail. Therefore, entrepreneurs who plan to fraud are less inclined to define a soft cap, since they bear the risk of not raising any amount at all.

One factor that consistently leads to higher fraud is when the startup has disclosed its code on GitHub. This results is at first sight surprising, given that disclosing the code is typically viewed as a sign of trustworthiness and transparency (Dabbish et al., 2012; Amsden and Schweizer, 2019; Howell et al., 2019). The difference in the probability of having a fraudulent offer is 6.6-7.4%, depending on the specification considered (Model (3) or (6)). Our results therefore stand in contrast to the common view that disclosing information on GitHub is good. A closer look at what type of frauds are associated with disclosure on GitHub offers a first clue on why fraud might become more prevalent (see Table 5). Phishing and hacking attacks are more common when code is published on GitHub (65.0% versus 44.0%), which is a main type of fraud in this particular case. Table 5 presents the distribution of fraud cases by disclosure on GitHub. Fraud cases where the code was disclosed before the ICO on GitHub are more often external than internal frauds, as opposed to fraud cases without prior disclosure. In contrast, exit frauds, security frauds and Ponzi schemes are less likely, all of which are internal frauds. These observations suggest that GitHub induces more often externally-driven phishing and hacking attacks. One likely reason is that

phishing and hacking attacks become easier for corporate outsiders when the code of the venture is disclosed. Thus, while the literature has argued that disclosing the code on GitHub is helpful to build trust between the startup and the investors, we find that it attracts external fraudsters to misuse the disclosed information to their own advantage and at the expense of investors. Thus, there is a clear tradeoff in deciding to disclose information on GitHub.

- Table 5 around here -

Returning to Table 4, another important result is that having raised more funds is associated with a greater likelihood of fraud (Models (4)-(6)), confirming our initial univariate finding that size matters. One reason proposed before is that the benefit of fraud is higher because there is more money to steal. In economic terms, a one-standard deviation increases in the amount raised leads to an increase in the fraud probability of 38%, which is a substantial effect.

An underlying assumption is that the significant result on GitHub is due to external and not internal fraud. Indeed, issuers' benefits from fraud are unrelated to whether the code is disclosed on GitHub. However, the fraud is facilitated for corporate outsiders, thus the increased risk of external fraud. In order to corroborate this assumption, we run again the same analysis as in Table 4 but separately for external and internal fraud cases. Results provided in Table 6 confirm that the effect of GitHub is driven by external fraud (the first six columns regress on external fraud, the last six on internal fraud).

- Table 6 around here -

5. CONCLUSIONS & POLICY IMPLICATIONS

ICOs combine the financing of a venture through a large crowd with the issuance of a new digital token. Therefore, ICOs share many similarities with equity and reward-based crowdfunding. This implies that the experience gained by national regulators in the crowdfunding domain – especially regarding equity crowdfunding – as well as the knowledge obtained by market participants may be useful for the discussion on whether and how to regulate ICOs. ICOs could be particularly useful when people want to own the platform they are using or would like to use the tokens as means of exchange. For example, the users of LinkedIn or Facebook could own the platform themselves and use tokens to pay for hosting and programming services of the website.

The establishment of professional platforms where ICO issues could take place, similar to equity crowdfunding campaigns that are frequently run on specialized platforms and some countries are even required by law to use a platform (Hornuf, Klöhn and Schilling, 2018), may facilitate the implementation of both, formal regulation and self-regulation.[16] These platforms may even be existing equity crowdfunding platforms integrating ICOs, as they have done similar expansions for other asset classes such as real estate crowdfunding, fixed income products, and secondary markets. In fact, combining crowdfunding and ICOs may be optimal to overcome the current inefficiencies of crowdfunding or the shortcomings of ICOs respectively (Ackermann et al. 2020). Moreover, these platforms could use small business credit scoring, a technology that has been used by financial institutions to evaluate applicants for small loans that involves analyzing data about the owner of the firm and the limited data about the firm itself (Berger and Frame, 2007).

[16] Crowdfunding campaigns in the early days of the market were also run on individual websites set up by the issuer; for example, Trampoline Systems in the UK.

Using such platforms might not only reduce the likelihood of fraud, but also decrease the costs of capital (Li et al. 2019).

In contrast to findings in equity crowdfunding (Cumming et al. 2019), the extent of information disclosure offers little opportunity to identify possible fraud, presumably due to the increasing use of template whitepapers. A more thorough analysis of the whitepapers is therefore needed. This could be done by institutional investors, in line with the notion that it is often optimal to share ownership (Narayanan and Lévesque, 2019). Alternatively, specialized platforms might be in a comparatively better position to run background checks and analyze the truthfulness of the information in the whitepapers, because unlike one-time investors and issuers they can specialize in conducting such a due diligence (Coffee, 2006). This raises questions about the usefulness of fraud ratings websites to identify possibly fraudulent ICO issuances.

REFERENCES

Ackermann, E., Bock, C., and Bürger, R. (2020). Democratising entrepreneurial finance: The impact of crowdfunding and Initial Coin Offerings (ICOs). in Moritz, A. et al. (eds) *Contemporary developments in entrepreneurial finance: An academic and policy lens on the status-quo, challenges and trends*, p. 277-308.

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

Alberts, J., and Fry, B. (2015). Is bitcoin a security? *Boston University Journal of Science and Technology Law*, 21(1): 1-21.

Amsden, R., and Schweizer, D. (2019). Are blockchain cowdsales the new 'Gold Rush'? Success determinants of initial coin offerings. Available at SSRN: https://ssrn.com/abstract=3163849.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2): 169-217.

Berger, A.N. and Frame, W.S. (2007). Small business credit scoring and credit availability. *Journal of Small Business Management*, 45(1): 5-22.

Coffee, J. (2006). Gatekeepers: The role of the professions in corporate governance: The professions and corporate governance. Oxford: Oxford University Press.

Cumming, D.J., Hornuf, L., Karami, M., and Schweizer, D. (2019a). Disentangling crowdfunding from fraudfunding. Available at SSRN: https://ssrn.com/abstract=2828919.

Cumming, D.J.,Leboeuf, G., and Schwieenbacher, A. (2019b). Crowdfunding models: Keep-It-All vs. All-Or-Nothing. *Financial Management*: forthcoming.

Dabbish, L., Stuart, C., Tsay, J., and Herbsleb, J. (2012). Social coding in GitHub: transparency and collaboration in an open software repository. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative*: 1277-1286.

Dorfleitner, G., Hornuf, L., and Kreppmeier, J. (2019). Promise not fulfilled: FinTech and the General Data Protection Regulation. mimeo.

Fish, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing*, 34(1): 1-22.

Hamrick, J.T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., and Vasek, M., (2018). The economics of cryptocurrency pump and dump schemes (December 2018). CEPR Discussion Paper No. DP13404. Available at SSRN: https://ssrn.com/abstract=3310307

Huang, W., Meoli, M., and Vismara, S. (2019). The geography of initial coin offerings. *Small Business Economics*, forthcoming.

Hornuf, L., Klöhn, L., and Schilling, T. (2018). Financial contracting in crowdinvesting - Lessons from the German market. *German Law Journal*, 19(3): 509-578.

Howell, S., Niessner, M., and Yermack, D. (2019). Initial coin offerings: Financing growth with cryptocurrency token sales. *Review of Financial Studies*, forthcoming.

Kaal, W.A., and Dell'Erba, M. (2019). Initial coin offerings: Emerging practices, risk factors, and red flags. *U of St. Thomas (Minnesota) Legal Studies Research Paper No. 17-18*. Available at SSRN: https://ssrn.com/abstract=3067615

Li, T., Shin, D., and Wang, B. (2019). Cryptocurrency pump-and-dump schemes. Available at SSRN: https://ssrn.com/abstract=3267041

Li, J., Wu, Z., and Zhang, L. (2019). Family involvement, external auditing, and the cost of debt: Evidence from U.S. small firms. *Journal of Small Business Management*, forthcoming.

Liebau, D., and Schueffel, P. (2019). Cryptocurrencies & Initial Coin Offerings: Are they scams – An empirical Study. *The Journal of the British Blockchain Association*, 2(1): 1-7.

Narayanan, M. and Lévesque, M. (2019). Distributing start-up equity: A theoretical foundation for an emerging practice. *Journal of Small Business Management*, forthcoming.

Valkenburgh, P. (2016). Framework for securities regulation of cryptocurrencies (Coin Center Report). Washington, DC.

TABLE 1: Distribution of Fraud Cases Identified (N = 1,393)

Multiple fraud types are possible for an ICO.

Fraud Type	No. Suspected Cases	No. Confirmed Cases
Exit Fraud	21	25
Security Fraud	13	3
Ponzi Scheme	27	0
Pump and Dump	31	1
Phishing / Hacking	28	128
Other Types	68	18
Total	188	175
Percentage of sample	13.5%	12.6%

Table 2: Definition of Variables

VARIABLE	*DEFINITION*
	Dependent Variables
Suspected Fraud	Dummy variable that equals 1 if the ICO is a suspected but not confirmed fraud case, and 0 otherwise.
Confirmed Fraud	Dummy variable that equals 1 if the ICO was confirmed by the issuer or an independent regulator or the communication of the issuer stopped two weeks after the end of the funding period confirmed fraud case, and 0 otherwise.
Internal Fraud	Dummy variable that equals 1 if the ICO was initiated by the issuer, and 0 otherwise; we consider as internal fraud: exit fraud, security fraud, Ponzi scheme, and those classified as other type of fraud.
External Fraud	Dummy variable that equals 1 if the ICO was initiated by an outsider to the issuing firm, and 0 otherwise; we consider as external fraud: a pump and dump, phishing, or hacking.
Fraud	Dummy variable that equals 1 if the ICO is a suspected or confirmed fraud, and 0 otherwise.
	ICO Characteristics
Offshore Country	Dummy variable that equals 1 if the ICO is located in an offshore country according to the FSF–IMF 2000 list, and 0 otherwise. Source: Offshore Financial Centers - Background Paper (2000).
Company Age	Number of days between the date of Twitter registration and start of the funding period.
Funding Period	Number of days the ICO lasted. Source: *Icobench.com* and/or *Icorating.com*
Pre-Sale	Dummy variable that equals 1 if the ICO had a pre-ICO, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Whitelist	Dummy variable that equals 1 if the ICO has a whitelist where potential investors could pre-register, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
KYC	Dummy variable that equals 1 if the ICO had a KYC process, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Investor Limitations	Dummy variable that equals 1 if the ICO is restricted to investors from certain countries, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
ETH Platform	Dummy variable that equals 1 if the token of the ICO is created on the Ethereum blockchain, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
GitHub	Dummy variable that equals 1 if the issuer provided code content in the repository section of GitHub, and 0 otherwise. Source: GitHub
	Team Characteristics

Team Info Available	Dummy variable that equals 1 if a team was listed on *Icobench.com* and/or *Icorating.com*, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Team Size	Number of team members. Source: *Icobench.com* and/or *Icorating.com*
Advisor	Dummy variable that equals 1 if advisors are listed on *Icobench.com* and/or *Icorating.com*, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Involved in other Project	Dummy variable that equals 1 if at least one team member is involved in another ICO in our sample, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
	Financial Details
ICO Price	Token price during the ICO in US-Dollar. Source: *Icobench.com* and/or *Icorating.com*
Token Distributed	Percentage of tokens available for sale during the ICO. Source: *Icobench.com* and/or *Icorating.com*
Soft Cap	Dummy variable that equals 1 if the ICO has minimum funding goal, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Hard Cap	Dummy variable that equals 1 if the ICO has a maximum funding target, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Hard Cap in USD	Amount of the maximum funding target in USD. Source: *Icobench.com* and/or *Icorating.com*
ln(Hard Cap)	Natural logarithm of the hard cap. Source: *Icobench.com* and/or *Icorating.com*
Bonus	Dummy variable that equals 1 if the ICO offers a discount for early investors, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Minimum Investment	Dummy variable that equals 1 if the ICO requires a minimum investment, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Accepting Fiat	Dummy variable that equals 1 if the ICO accepted fiat currency, and 0 otherwise. Source: *Icobench.com* and/or *Icorating.com*
Nbr_Accepting	The number of different cryptocurrencies the issuer accepted during the funding period. Source: *Icobench.com* and/or *Icorating.com*
	Social Media activity
Nbr Social Media	Number of Social Media accounts on Twitter, Facebook, Reddit, Telegram, Slack, Medium, and Bitcointalk.
Twitter Account	Dummy variable that equals 1 if the ICO was registered on Twitter, and 0 otherwise. Source: Twitter
Facebook	Dummy variable that equals 1 if the ICO was registered on Facebook, and 0 otherwise. Source: Facebook
Reddit	Dummy variable that equals 1 if the ICO was registered on Reddit, and 0 otherwise. Source: Reddit
Telegram	Dummy variable that equals 1 if the ICO was registered on Telegram, and 0 otherwise. Source: Telegram
Slack	Dummy variable that equals 1 if the ICO was registered on Slack, and 0 otherwise. Source: Slack

Medium	Dummy variable that equals 1 if the ICO was registered on Medium, and 0 otherwise. Source: Medium
Bitcointalk	Dummy variable that equals 1 if the ICO was registered on Bitcointalk, and 0 otherwise. Source: Bitcointalk
Tweets	Number of tweets on Twitter. Source: Twitter
Twitter Followers	Number of followers on Twitter. Source: Twitter
	Information Disclosure
Token Distribution	Dummy variable that equals 1 if the ICO issuer disclosed how tokens are distributed among different stakeholders, and 0 otherwise. Source: *Icorating.com*
Info on Use of Funds Available	Dummy variable that equals 1 if the ICO issuer disclosed information about the planned use of funds, and 0 otherwise. Source: *Icorating.com*
Video Pitch	Dummy variable that equals 1 if the ICO disclosed a video pitch on *Icobench.com*, and 0 otherwise. Source: *Icobench.com*

TABLE 3: Summary Statistics on Main Variables

The subsample of fraud cases includes both suspected and confirmed cases.

							Subsample of Fraud Cases (N = 1119)		Subsample of Non-Fraud Cases (N = 274)		Diff. Mean Test	
Variable	No. Obs.	Mean	Median	Std. Dev.	Min	Max	Mean	Std. Dev.	Mean	Std. Dev.	Diff.	p-value
Fraud:												
Suspected Fraud	1393	0.109	0	0.312	0	1	0.555	0.498	- -	- -	- -	- -
Confirmed Fraud	1393	0.113	0	0.316	0	1	0.573	0.496	- -	- -	- -	- -
Fraud	1393	0.197	0	0.398	0	1	- -	- -	- -	- -	- -	- -
Internal Fraud	1393	0.105	0	0.306	0	1	0.533	0.500	- -	- -	- -	- -
External Fraud	1393	0.119	0	0.324	0	1	0.606	0.490	- -	- -	- -	- -
ICO Characteristics:												
Amount Raised	845	18.762	6.316	146.095	0.000	4198.0	41.443	287.899	11.070	18.341	30.373	0.081
Offshore Country	1393	0.313	0	0.464	0	1	0.314	0.465	0.313	0.464	0.001	0.972
Company Age	1178	297.310	112	531.660	0	3748	336.970	570.030	287.640	521.740	49.330	0.192
Duration of ICO	1383	40.459	31	31.764	0	382	35.766	40.119	41.598	29.291	-5.832	0.024
Pre-Sale	1392	0.441	0	0.497	0	1	0.339	0.474	0.466	0.499	-0.127	0.000
Whitelist	1393	0.183	0	0.387	0	1	0.113	0.317	0.200	0.400	-0.087	0.000
KYC	1393	0.610	1	0.488	0	1	0.700	0.459	0.588	0.492	0.112	0.000
Investor Limitations	1393	0.220	0	0.414	0	1	0.124	0.330	0.243	0.429	-0.119	0.000
ETH Platform	1393	0.887	1	0.316	0	1	0.880	0.326	0.889	0.314	-0.010	0.657
GitHub	1393	0.461	0	0.499	0	1	0.511	0.501	0.449	0.498	0.062	0.064
Team Characteristics:												
Team Info Available	1393	0.941	1	0.235	0	1	0.912	0.283	0.948	0.222	-0.036	0.052
Team Size	1282	7.828	7	6.146	1	52	8.291	6.047	7.718	6.166	0.573	0.161
Advisor	1311	0.568	1	0.496	0	1	0.540	0.499	0.574	0.495	-0.034	0.312
Involved in other Project	1393	0.553	1	0.497	0	1	0.609	0.489	0.540	0.499	0.070	0.035
Financial Details:												
ICO Price	1357	10.627	0.25	221.750	0	7554.6	12.222	183.550	10.237	230.200	1.985	0.879
Token Distributed	934	0.571	0.6	0.202	0.0003	1	0.572	0.211	0.571	0.200	0.001	0.964

Soft Cap	1393	0.414	0	0.493	0	1	0.285	0.452	0.446	0.497	-0.161	0.000
Hard Cap	1393	0.668	1	0.471	0	1	0.606	0.490	0.683	0.466	-0.077	0.019
Hard Cap in USD	929	51.541	20	342.090	76968	9734.1	65.920	270.084	48.412	355.906	17.508	0.369
Bonus	1393	0.470	0	0.499	0	1	0.343	0.476	0.501	0.500	-0.158	0.000
Minimum Investment	1393	0.276	0	0.447	0	1	0.201	0.401	0.295	0.456	-0.094	0.001
Accepting Fiat	1203	0.128	0	0.334	0	1	0.134	0.341	0.127	0.333	0.007	0.764
Nbr Accepting Crypto	1203	2.032	1	1.586	1	13	1.926	1.215	2.056	1.656	-0.130	0.144
Information Disclosure:												
Token Distribution	1393	0.817	1	0.387	0	1	0.796	0.404	0.822	0.383	-0.027	0.325
Info on Use of Funds Available	1393	0.421	0	0.494	0	1	0.285	0.452	0.454	0.490	-0.169	0.000
Video Pitch	1379	0.719	1	0.450	0	1	0.757	0.429	0.709	0.454	0.048	0.100
Social Media Activity:												
Nbr Social Media	1393	5.127	5	1.793	0	8	5.197	1.823	5.109	1.786	0.088	0.472
Twitter Account	1393	0.852	1	0.355	0	1	0.858	0.350	0.851	0.356	0.007	0.770
Facebook	1393	0.869	1	0.337	0	1	0.861	0.346	0.871	0.335	-0.010	0.666
Reddit	1393	0.550	1	0.498	0	1	0.588	0.493	0.541	0.499	0.047	0.159
Telegram	1393	0.756	1	0.430	0	1	0.635	0.482	0.786	0.411	-0.150	0.000
Slack	1393	0.267	0	0.443	0	1	0.394	0.490	0.236	0.425	0.158	0.000
Medium	1393	0.632	1	0.483	0	1	0.628	0.484	0.633	0.482	-0.005	0.879
Bitcointalk	1393	0.740	1	0.439	0	1	0.723	0.449	0.744	0.436	-0.022	0.469
Tweets	1173	637.8	241	1605.3	1	30100	839.8	1316.5	588.2	1665.4	251.6	0.007
Twitter Followers	1171	9506.4	2896	33713.3	1	894000	25411	69239.0	5597.9	12822.0	19813.1	0.000

Table 4: Determinants of Fraud Cases

This table shows Probit regressions, where the dependent variable is a dummy equal to 1 when the ICO is classified as a fraud case, and 0 otherwise. We consider three different measures of fraud: *Confirmed Fraud*, *Suspected Fraud*, and *Fraud* (which equals 1 if *Confirmed Fraud* or *Suspected Fraud* equals 1). Coefficients reported are marginal effects. Robust standard errors are used for testing the significance of coefficients. Significance levels: * p<0.10, ** p<0.05, *** p<0.01.

	(1)	(2)	(3)	(4)	(5)	(6)
	Confirmed Fraud	Suspected Fraud	Fraud	Confirmed Fraud	Suspected Fraud	Fraud
Offshore Country	-0.0015	0.0064	0.0119	-0.0040	0.0336	0.0223
Company Age	0.0000	-0.0000	-0.0000	-0.0000	0.0000	-0.0000
Duration of ICO	-0.0002	-0.0001	-0.0000	-0.0004	0.0005	0.0003
Pre-Sale	-0.0256	-0.0155	-0.0324	-0.0038	0.0210	0.0088
Whitelist	-0.0386	0.0214	-0.0112	-0.0169	0.0293	0.0247
KYC	0.0279	-0.0004	0.0222	0.0372	0.0082	0.0341
Investor Limitations	-0.0263	-0.0437	-0.0656*	-0.0187	-0.0487	-0.0734
GitHub	0.0612***	0.0165	0.0655***	0.0613**	-0.0019	0.0738**
Advisor	-0.0192	0.0150	-0.0014	-0.0595*	0.0276	-0.0241
Involved in other Project	0.0251	0.0177	0.0308	0.0371	-0.0143	0.0216
Soft Cap	-0.0491**	-0.0414**	-0.0782***	-0.0476	-0.0320	-0.0754*
Hard Cap	0.0422*	-0.0121	0.0254	0.0068	-0.0018	-0.0103
Bonus	0.0114	-0.0335	-0.0108	0.0159	-0.0321	-0.0106
Minimum Investment	-0.0496**	0.0128	-0.0314	-0.0492	0.0002	-0.0419
Accepting Fiat	0.0296	0.0285	0.0334	0.0502	-0.0227	0.0373
Nbr Accepting Crypto	-0.0103	-0.0069	-0.0095	-0.0054	-0.0132	-0.0108
Info on Use of Funds Available	-0.0024	-0.0460**	-0.0339	-0.0137	-0.0288	-0.0256
Video Pitch	0.0223	0.0438*	0.0552*	-0.0741*	-0.0213	-0.0836*
Amount Raised				0.0010*	0.0008**	0.0026***
Token Distributed				0.0030	0.0591	0.0783
Observations	967	967	967	451	451	451
Pseudo R-squared	0.060	0.064	0.054	0.084	0.081	0.087
AIC	664.757	591.999	892.243	353.471	288.289	446.579

TABLE 5: Sample Distribution of Fraud Cases, by GitHub Disclosure

	Subsample of Fraud Cases with GitHub==1		Subsample of Fraud Cases with GitHub==0		Diff. Mean Test	
Variable	Mean	Std. Dev.	Mean	Std. Dev.	Diff.	p-value
Suspected Fraud	0.500	0.502	0.612	0.489	-0.112	0.062
Confirmed Fraud	0.629	0.485	0.515	0.502	0.114	0.057
Internal Fraud	0.429	0.497	0.642	0.481	-0.213	0.000
Exit Fraud	0.093	0.291	0.246	0.432	-0.153	0.001
Security Fraud	0.050	0.219	0.067	0.251	-0.017	0.547
Ponzi Scheme	0.064	0.246	0.134	0.342	-0.070	0.053
Other Fraud	0.271	0.446	0.358	0.481	-0.087	0.122
External Fraud	0.729	0.446	0.478	0.501	0.251	0.000
Pump and Dump	0.171	0.378	0.060	0.238	0.112	0.003
Phishing /Hacking	0.650	0.479	0.440	0.498	0.210	0.000

Table 6: Determinants of Fraud Cases

This table shows Probit regressions, where the dependent variable is a dummy equal to 1 when the ICO is classified as a fraud case, and 0 otherwise. We consider three different measures of fraud: *Confirmed Fraud*, *Suspected Fraud*, and *Fraud* (which equals 1 if *Confirmed Fraud* or *Suspected Fraud* equals 1). Coefficients reported are marginal effects. Robust standard errors are used for testing the significance of coefficients. Significance levels: * p<0.10, ** p<0.05, *** p<0.01.

	External Fraud						Internal Fraud					
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Confirmed Fraud	Suspected Fraud	Fraud	Confirmed Fraud	Suspected Fraud	Fraud	Confirmed Fraud	Suspected Fraud	Fraud	Confirmed Fraud	Suspected Fraud	Fraud
Offshore Country	0.0027	0.0023	0.0085	0.0111	0.0309	0.0336	0.0044	0.0242	0.0299	-0.0017	0.0419*	0.0304
Company Age	0.0000	0.0000	0.0000	-0.0000	0.0000	0.0000	-0.0000	-0.0000	-0.0000	-0.0000	-0.0000	-0.0000
Duration of ICO	-0.0006	-0.0002	-0.0005	-0.0003	-0.0006	-0.0004	0.0001	0.0002	0.0004*	-0.0005*	0.0006	0.0005
Pre-Sale	-0.0294	-0.0036	-0.0316	-0.0063	0.0094	-0.0054	-0.0019	-0.0085	-0.0060	0.0076	0.0286	0.0278
Whitelist	-0.0167	-0.0178	-0.0210	-0.0027	-0.0599	-0.0138	-0.0231	0.0203	0.0036	-0.0195	0.0386	0.0345
KYC	0.0156	0.0067	0.0231	0.0419	-0.0121	0.0389	0.0096	-0.0082	0.0000	-0.0115	0.0021	-0.0124
Investor Limitations	-0.0299	0.0043	-0.0388	-0.0394	0.0375	-0.0489	-0.0041	-0.0348	-0.0396	0.0217	-0.0433	-0.0261
GitHub	0.0566***	0.0275**	0.0690***	0.0577*	-0.0141	0.0594*	0.0141	0.0074	0.0101	-0.0039	-0.0061	-0.0042
Advisor	-0.0236	0.0064	-0.0162	-0.0664**	0.0342	-0.0347	0.0036	0.0159	0.0154	-0.0020	0.0118	0.0154
Involved in other Project	0.0538**	0.0248	0.0659***	0.0694*	-0.0048	0.0507	-0.0209*	0.0010	-0.0207	-0.0210	-0.0042	-0.0285
Soft Cap	-0.0307	-0.0318**	-0.0502**	-0.0459	-0.0329*	-0.066**	-0.0149	-0.0223	-0.0307*	0.0080	-0.0163	-0.0082
Hard Cap	0.0340	-0.0157	0.0159	0.0170	0.0029	0.0181	0.0195	0.0112	0.0213	-0.0141	-0.0145	-0.0298
Bonus	-0.0051	-0.0320**	-0.0156	0.0007	-0.0422*	-0.0148	0.0162	-0.0243	-0.0014	0.0072	-0.0182	0.0009
Minimum Investment	-0.0426*	-0.0068	-0.0493**	-0.0308	-0.0117	-0.0437	-0.0185	0.0180	0.0068	-0.0182	0.0029	-0.0144
Accepting Fiat	0.0026	-0.0031	-0.0200	0.0093	0.0000	-0.0099	0.0503**	0.0423	0.0548*	0.0513*	-0.0114	0.0312
Nbr Accepting Crypto	-0.0051	-0.0167**	-0.0068	-0.0020	-0.0181*	-0.0021	-0.018***	-0.0068	-0.0114*	-0.0179**	-0.0130	-0.0174*
Info on Use of Funds Available	-0.0099	-0.0449***	-0.0304	-0.0150	-0.0486**	-0.0298	-0.0032	-0.0230	-0.0169	-0.0070	-0.0151	-0.0112
Video Pitch	0.0096	0.0278	0.0239	-0.0779**	-0.0105	-0.084**	0.0088	0.0176	0.0282	-0.0173	-0.0312	-0.0312
Amount Raised				0.0009*	-0.0001	0.0009				0.0001	0.0008**	0.0010**
Token Distributed				-0.0286	0.0062	0.0122				0.0191	0.0407	0.0765
Observations	967	967	967	451	385	451	967	967	967	451	451	451
Pseudo R-squared	0.078	0.204	0.106	0.101	0.198	0.109	0.075	0.038	0.036	0.126	0.082	0.067
AIC	600.79	320.94	670.45	326.05	149.7466	355.24	289.71	504.40	577.29	149.05	261.35	292.02

Appendix Table 1: Definition and examples of fraud categories

PHISHING / HACKER ATTACK	
Definition	Phishing attacks include fake e-mails, fake websites, fake airdrops, fake social media accounts, and hacking into a company's account or website in order to route investors to a fake wallet address. A hacker attack refers to a bad actor stealing money from a company's blockchain wallet.
Suspected	Phishing or hacking attacks are categorized as suspected if there were rumors of such attacks.
Confirmed	We categorized phishing or hacking attacks as detected if the company confirmed that it was the victim of a phishing or hacker attack.
SECURITY FRAUD	
Suspected	Either the ICO issuer is under investigation by a regulator of committing security fraud or rumors that the issued token is an unregistered security token occurred.
Confirmed	A regulator (e.g., the SEC) confirmed that the ICO issuer committed security fraud.
PONZI SCHEME	
Suspected	Examples: (i) Rumors that the company's business model is based on a ponzi scheme occurs on website(s). (ii) The company shows a tool for calculating ROI on its website or whitepaper. The company promises profits to investors. (iii) A third party website shows a ROI scheme which is based on the promised profits for investors (e.g., BehindMLM). (iv) The company or a team member is involved in a possible Ponzi company.
Confirmed	Confirmation by the ICO issuer or a regulator that their business model is based on a ponzi scheme. In that case investments are used to pay guaranteed profits to earlier investors.
PUMP AND DUMP	
Suspected	Accusations about pump and dump scheme have occurred.
Confirmed	The ICO issuer confirmed that its coin was the victim of a Pump and Dump scheme.

EXIT FRAUD

Definition	The founders of the company disappear after the funding period without any announcement of repayments to investors.
Suspected	An accusation about an exit fraud of the company could be found, but the time of latest corporate communication cannot be determined because both the website and the social media accounts are no longer available.
Confirmed	Disappearance is assumed when both the website and social media communications have been discontinued. At least one social media account must show that the company stopped its communication immediately after the ICO (within two weeks). Unless fraud has already been confirmed (category Other Fraud) or exit fraud accusations occurred within two weeks after ICO. The social networks investigated are Twitter, Facebook and the company's own blog.

OTHER FRAUD

Bounty Scam:

Suspected	Claims in forums (e.g., Bitcointalk, Reddit) that bounty hunters did not get paid with tokens for their work.
Confirmed	Claim of a corporate partner that the company is not willing to pay the bounty hunters.

Fake team / fake company:

Suspected	Claims that the team or a team member could be a fake person or identity theft took place.
Confirmed	Evidence that a team member is a fake person trough reverse image searches or statement from the person whose identity was stolen.

Issues with token distribution/refund:

Suspected	Accusation that the distribution of tokens after the ICO or, in the case the soft cap has not been reached, the refund is either delayed and/or lower or is missing.

False claims about partnerships:

	False claims by the ICO issuer about cooperations with other companies or claims of cooperations with fraudulent companies.
Suspected	Only accusation without evidence.
Confirmed	Denial of the apparent cooperation by the other company or confirmation of false claims by a regulator.

Bug in smart contract code:

Suspected	Accusations about a bug in the smart contract code, which leads to a money loss either for the company or for the investor.
Other fraudulent activities identified:	The company is associated with fraudulent conduct or suspicious persons or institutions: e.g., investigation or legal action against the company (except security fraud and ponzi investigations); company is associated with suspicious individuals or institutions, such as persons who have been investigated, sued for or involved in fraudulent activities.
Suspected	Accusations of fraud/scam which implicate a bad/fraudulent intention by the founder/company (or an external person or institution) and cannot be attributed to the above categories. Claims without evidence or investigation.
Confirmed	Confirmation of fraudulent activity by a regulator.