

## PEER REVIEWED RESEARCH

OPEN ACCESS

ISSN Online: 2516-3957

ISSN Print: 2516-3949

[https://doi.org/10.31585/jbba-2-1-\(5\)2019](https://doi.org/10.31585/jbba-2-1-(5)2019)

**Competing Interests:**  
None declared.

**Ethical approval:**  
Not applicable.

**Author's contribution:**  
DL and PS<sup>2</sup> designed and coordinated this research and prepared the manuscript in entirety.

**Funding:**  
None declared.

**Acknowledgements:**  
The authors would like to thank Bobby Ong and the Coingecko team for their proactive support.

## Cryptocurrencies & Initial Coin Offerings: Are they Scams? - An Empirical Study

Daniel Liebau<sup>1</sup>, Patrick Schueffel<sup>2</sup>

<sup>1</sup>IE Business School, IE University, Spain

<sup>2</sup>HEG Fribourg School of Management, Switzerland

**Correspondence:** [dliebau@faculty.ie.edu](mailto:dliebau@faculty.ie.edu)

**Received:** 15 January 2019 **Accepted:** 20 March 2019 **Published:** 2 April 2019

### Abstract

The volume of Initial Coin Offerings (ICOs) had risen steeply with an all-time high market capitalisation of close to 1 trillion USD in December 2017. Since then the digital asset market has slumped, retreating to approximately 200 billion USD by mid-2018. Stakeholders of the crypto industry have pondered the reasons for this retrenchment and are increasingly focusing on the notion that many ICOs could be scams. A recent industry study even went as far to claim that 80% of all ICOs are indeed scams. In this paper, we investigate the question whether these scams are as common as claimed. We do so by first defining what a scam is and secondly, by drawing on empirical data to assess the number of cases fitting such a definition. Building on Principal Agent Theory and based on the statistical analysis of our empirical data set we attempt to establish the current state of affairs with regards to scams in the crypto-currency world. The results of our study divert from salient beliefs.

**Keywords:** *blockchain, scam, ICO, digital assets, ethics, crypto-currency, token*

**JEL Classifications:** *D01, D21, D26, D53, D84, K24*

### 1. Introduction

An Initial Coin Offering (ICO) is an unregulated process for capital-raising typically used by firms in the cryptocurrency field as a substitute for the controlled funding methods applied by other financial intermediaries [1]. The volume of ICOs had risen sharply with an all-time high market capitalisation of close to 1 trillion USD in December 2017. Since then the digital asset market has retreated to approximately 200 billion USD by mid-2018. Stakeholders of the cryptocurrency industry have since contemplated the causes for this retrenchment. While this “increasingly popular way to raise capital for Blockchain technology start-ups” [2, p.2] has become the method of choice for many crypto firms in order to raise capital, its performance increasingly often lacks behind expectations [3]. Consequently, numerous exponents of the cryptocurrency industry are increasingly focusing on the notion that many ICOs could be scams. A recent industry study went as far as to maintain that 80% of all ICOs are indeed scams.[4] However, it is generally acknowledged that poor economic performance cannot automatically be equated with a scam. Moreover, it is highly questionable that high failure rates are idiosyncratic to the novel phenomenon of the ICO. We, therefore,

argue that a more differentiated view on ICOs and potential scams is necessary. Hence, with this study, we intend to investigate the question of whether and when ICOs can justifiably be called a scam. We believe that investigating this problem is of importance because scholars and practitioners alike have recently made rather coarse statements on this subject matter which were further amplified by the broader media. Economist Nouriel Roubini’s testimony to the US Senate Hearing on “Exploring the Cryptocurrency and Blockchain Ecosystem”, for instance, was subtitled “Crypto is the Mother of All Scams” [5] and Economics scholar Saifedean Ammous recently portrayed the Ethereum project as “a worthless scam” [6]. As ICOs nevertheless receive increasing attention not only by the media but also by investors, we deem it a worthwhile endeavour to investigate the magnitude of true scams in this area.

This article is organised in the following manner. First, we lay out the theoretical foundation of our research along with definitions of the terminology used. Secondly, the research methodology is explained sideways with the sample and data collection method. In a third step, we present the

results, before discussing them in a fourth phase. The article concludes with highlighting its contributions as well as its limitations and specifically the many possible future research directions with regards to the subject of scams in the Blockchain ecosystem.

## 2. Theoretical Foundation

Investigating scams is a multifaceted undertaking, and the term scam is not being used identically by all scholars, practitioners and the broader media. On the contrary, we believe that investors frequently mistake a poor economic performance for a scam and that this misjudgement is then further conveyed and amplified by the broader media. Over the next paragraphs we, therefore, provide a brief overview of the theory we ground our research on as well as the terms “scam” and “economic performance”.

### 2.1 Principal-Agent Theory (PAT)

Agency Theory is a framework explaining how objectives are reached by separate players interacting with each other. As such it elucidates self-goals and other-goals and how distinct actors, so-called Principals and Agents, deal with difficulties in their coexistence. These challenges mostly arise from conflicts of interest between the Agent and the Principal [7]. Examples of such relationships include investor and broker, teacher and student, physician and patient as well as lawyer and client.

The conclusion that “agency, or acting for another, is pervasive” [8, p.1] holds in many aspects of life, and the cryptocurrency industry is no exception to this. Drawing on the findings of Mitnick [8] we employ the following four assumptions: first, actors are rational and sensibly weigh returns against investments. Second, actors will always seek for increasing returns. Third, the underlying model is a static one, that is there is no change in the actors’ behaviour and learning. Lastly, acting on behalf of a third party may lead to fundamentally “different behaviour than acting for oneself.” [8, p.4].

We deem PAT to be highly suitable to analyse the ICO phenomenon as the business entities’ can be delineated as follows: The Principal is the investor/token buyer and agent is the software developer /token issuer, depicted in Figure 1.

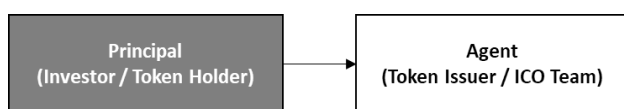


Figure 1. Principal and Agent in the context of for-business ICOs

The ICO team typically outlines the purpose, benefits and roadmap of their project in a whitepaper. The Principal, for ideological, economic or other reasons entrusts the Agent with funds to progress the project in question. The ICO team becomes the Agent acting on behalf of the Principal. The following parts of PAT are specifically appealing to consider in the context of ICOs and the Blockchain ecosystem:

ICO projects typically exert considerable discretionary power over capital and resource allocation upon completion of the ICO. This corresponds with the assertion that “[t]he agent’s problem is basically that of a choice of acts to best satisfy his preference for self and other goals” while being endowed with “considerable discretion with respect to the agent’s goals” [8, p.34]. Such a constellation leaves the agent with the task to resolve a trade-off between self-goals and the agent’s goals. We, therefore, pose that it is tempting for ICO teams to engage in fraudulent activities, especially in the absence of incentive systems that usually “include negative mechanisms like sanctions, threat of force, or reduction of agent return”. [8, p.35] These incentive systems which typically reduce the likelihood of conflicts between the Principal and the Agent hardly exist in the crypto industry, increasing the risk for the Principal.

Then again this leads our thoughts to the subject of policing. “The cheapest method of policing the agent with respect to policing the principal’s goals is to have the agent do it himself.” [8, p.39]). Some, not all, ICOs work against a timeline with milestones. If a project does not hit the milestones, the community of Principals will publicly (mostly through social media) complain. Since many ICOs list their token on exchanges very swiftly after the ICO is complete, these complaints can impact the token price adversely. In summary, we consider the policing mechanisms available in the token world relatively weak and therefore conflicts of interest for the Agent are foreseeable.

### 3. Scam

The Oxford Dictionary defines a scam as “[a] dishonest scheme; a fraud.” [9]. In a similar vein, Merriam-Webster states that a scam is “a fraudulent or deceptive act or operation” [10]. In turn, a fraud is an unlawful, respectively criminal act as it “consists of some deceitful practice or wilful device, resorted to with intent to deprive another of his right, or in some manner to do him an injury” [11]. In the context of business, scams are therefore regularly seen as acts throughout which the scammer purposefully deprives the trustful investor of his or her funds to advantage to the scammer. Consequently, the investment will not perform to the extent initially suggested by the scammer and believed by the investor. By comparison, the above-mentioned study by Dowlat, delineates scams in the following way: “Identified Scam (pre-trading): Any project that expressed availability of ICO investment (through a website publishing, ANN thread, or social media posting with a contribution address), did not have/had no intention of fulfilling project development duties with the funds, and/or was deemed by the community (message boards, website or other online information) to be a scam.” [4, p.23].

### 4. Economic Performance

Economic performance is the evaluation of a firm’s success measured in monetary terms. It comprises its assets as well as liabilities and its ability to generate profits. Ultimately economic

performance will determine the likelihood of organisational mortality.

Timmons Jeffrey and Spinelli [12] estimated that the survival rate of new ventures is approximately 60% after the first year and 10% over ten years. Conducting research specifically on "new, adolescent, young, emerging and high-tech, technology, technology-intensive, and technology-based» ventures Song, Podoyntsyna, Van Der Bij and Halman [13, p.9] reported more fine-grained results. After analysing a longitudinal data set of 11,259 New technology ventures (NTVs) established between 1991 and 2000 in the United States, the authors conclude that the survival rate of NTVs with five or more full-time employees is only 36 per cent after four years and that this survival rate drops further to 21.9% after five years [13]. As Blockchain technology is a rather young phenomenon and technology is at the core of any crypto project, start-ups and NTVs and NTVs can provide interesting benchmarks.

## 5. Research Methodology

### 5.1 Sample

As we strive to establish the extent of scams among ICOs worldwide, the level of our analysis was set to a macro level. Accordingly, we collected global data from relevant international ICO Web sites, such as ICO Data [14], Token Market [15], ICO Bench [16], Coin Index [17], ICO Watch List [18], and CoinGecko [19]. While those sources did mention the ICO of the Decentralized Autonomous Organization (DAO), we decided to exclude this ICO from our sample as it would overly skew the data analysis with its emission volume of more than USD 150 million.

The decision to use the 2016 cohort was based on the rationale of providing a long enough time frame required for potential plaintiffs to file legal proceedings against fraudulent ICOs. Furthermore, 2016 was chosen as the number of ICOs throughout that year was already a multiple of the previous years, hence yielding a more solid base for a quantitative analysis than the cohorts of 2014 and 2015. To be included in the sample an ICO had to meet the following two criteria: first, it must be a public offering, i.e. advertised through the pertinent outlets of the crypto community and second it must have completed its ICO during the year 2016. Based on the defined sampling criteria a sample size of 45 was obtained.

### 5.2 Method

In our attempt to elicit the true ICOs scams we conducted a descriptive multi-level analysis on our sample. First, we scanned the Lexis Nexis Database for any news related to the sample ICOs. Lexis Nexis is considered to be among the most comprehensive news databases globally, providing interfaces to 36'000 international sources [20]. Search delimiters were set to cover only news items as of 2016 or younger. Each ICO was checked along with the keyword "scam" as well as the synonyms \*fraud", "sham" "deceit", "con", and "hoax". Second, whenever

any of these search terms in conjunction with an ICO yielded a result, we furthermore conducted a more in-depth search for any resulting legal proceedings or court cases that may have emerged subsequently. Third, if court cases were initiated, we investigated whether a verdict was delivered yet, if so, what the ruling was. The cut-off date for our data sampling process was the 8th of January 2019.

## 6. Results

Table 1 reports the ICOs of 2016 along with the findings from our descriptive multi-level analysis. Next to selected demographics of the ICOs such as token name, funds raised, ICO end, the table indicates whether the ICO was mentioned in the news as a scam, fraud, sham, deceit, con or hoax. We also counted these words in case they were used as verbs or adjectives. The dataset furthermore provides information on whether a lawsuit was initiated against any ICO of the 2016 cohort and if so, what the court's verdict was. Next, to this information, we gather a set of control variables, such as the issuing price of the token as well as its current price and performance in the market. The total number of subjects in the sample was 45. Of those 45 projects, three (6.7%) were referred to in the context of a scam in the news at least one time: DinarDirham, E-dinar, and Bitconnect. Bitconnect was furthermore named a fraud, deceit, and con. Lawsuits were initiated against two projects (4.4%): E-dinar and Bitconnect. In the case of one project (2.2%), Bitconnect, the court ruled that it was a fraudulent scheme whereas the court ruling for E-dinar stated that it was a legitimate token.

Looking at the control variables further points are noteworthy: For 22 of the 45 objects, respectively for 49% of the cases, no data could be obtained for the issuing price or the current price or both. Cases of missing data were labelled as, "n.a.". Consequently, no performance figures could be calculated for those projects. For those ICOs, however, for which financial performance figures could be calculated they vary from near total losses of the investment (-98%) to a significant multiplication in value (+15.541%). As we demonstrate in Table 1 an evenly distributed portfolio of these ICO tokens (we assumed 1000 USD allocation to each project) would have yielded a hypothetical return of approximately 598.71% over the two years and eight days period analysed.

## 7. Discussion

Drawing data from a global sample of international ICOs, this study shows that far less than the alleged 80% of ICOs are scams in the legal sense of the word. On the contrary, we could only identify one case (2.2%) where an ICO would match the definition of a scam as provided above. Even if we assumed that this figure is underestimated due to a large number of unreported cases, an adjusted estimate increasing this number previously reported 80%. What is more, even if we assume the worst-case scenario that the 22 projects for which we cannot obtain data on the issuing price or the current price or both turn all out to be scams we would see fundamentally different results



Table 1: Analysis of Initial Coin Offerings (ICOs), cohort of 2016.

No	Name	Token	USD Raised	End of ICO	Issuing Price	Current Price (8.1.2018)	Delta	Initial investment	Total Return	% with n.s.	Scam	Fraud	Sham	Deceit	Con	Hoax	Law Suit	Verdict: fraudulent
1	DigixDAO	DGD	5,500,000	3/1/2016	3.23529	21.15885	554%	1000	5540									
2	Lisk	LSK	6,500,000	3/21/2016	0.07647	1.40638	1733%	1000	17331									
3	Waves	WAVES	16,010,008	5/31/2016	0.18835	2.93855	1460%	1000	14602									
4	Newbium	n.a.	38,180	5/31/2016	n.a.	n.a.	n.a.	1000	0									
5	Pluton	PLU	1,000,000	6/24/2016	1.17647	0.54633	-54%	1000	-536									
6	Rise	n.a.	1,188,823	6/24/2016	n.a.	n.a.	n.a.	1000	0									
7	ICO OpenLedger	ICOD	1,388,427	6/30/2016	2.93754	0.11189	-96%	1000	-962									
8	Stratis	STRAT	600,945	7/26/2016	0.00715	1.11835	15541%	1000	155413									
9	Incent	INCNT	1,000,000	9/1/2016	0.04346	0.04472	3%	1000	29									
10	DinarDirham	DNC	n.a.	9/3/2016	n.a.	n.a.	n.a.	1000	0		Y							
11	BlockPay	BLOCKPAY	675,000	9/5/2016	0.12435	0.04775	-62%	1000	-616									
12	NEO	NEO	3,758,871	9/7/2016	0.18794	8.39597	4367%	1000	43674									
13	Bitpark Coin	BITPARK	291,356	9/15/2016	0.10400	n.a.	n.a.	1000	0									
14	FirstBlood	1ST	5,500,000	9/25/2016	0.06428	0.03230	-50%	1000	-497									
15	Iconomi	ICN	10,682,516	9/26/2016	0.10500	0.21120	101%	1000	1011									
16	DeClouds	DC	288,426	10/5/2016	n.a.	n.a.	n.a.	1000	0									
17	Lykke	LKK	2,800,000	10/9/2016	0.05600	0.02202	-61%	1000	-607									
18	Synereo	AMP	4,700,000	10/18/2016	0.1597	0.02	-87%	1000	-875									
19	eBoost	EBST	140,000	10/27/2016	0.20000	0.02322	-88%	1000	-884									
20	SingularDTV	SNGLS	7,500,000	10/29/2016	0.01500	0.01104	-26%	1000	-264									
21	Bitgirls	TOPEKABU	n.a.	10/31/2016	n.a.	n.a.	n.a.	1000	0									
22	DECENT	DCT	4,126,300	11/6/2016	0.10715	0.12314	15%	1000	149									
23	Kibo Lotto	KBT	3,039,813	11/10/2016	0.00000	n.a.	n.a.	1000	0									
24	Golem	GNT	8,596,000	11/13/2016	0.01048	0.07064	574%	1000	5740									
25	Komodo	KMD	1,983,781	11/14/2016	0.02204	0.76213	3358%	1000	33580									
26	ETC/Win	n.a.	1,309,000	11/23/2016	0.00000	n.a.	n.a.	1000	0									
27	Arcade City	ARC	699,187	11/28/2016	n.a.	n.a.	n.a.	1000	0									
28	Nexium	NXC	115,500	11/30/2016	0.00400	0.00621	55%	1000	553									
29	Decentralized Co	n.a.	n.a.	11/30/2016	n.a.	n.a.	n.a.	1000	0									
30	Mass coin	MASS	252,432	12/1/2016	0.00000	n.a.	n.a.	1000	0									
31	Nodio	NOD	81,487	12/1/2016	n.a.	n.a.	n.a.	1000	0									
32	Golos	GOLOS	462,000	12/4/2016	0.10000	0.00956	-90%	1000	-904									
33	Ark	ARK	342,593	12/11/2016	0.00995	0.44753	4338%	1000	43378									
34	E-dinar	DER	n.a.	12/14/2016	n.a.	0.00858	n.a.	1000	0		Y						Y	N
35	vSlice	VSL	1,800,000	12/15/2016	n.a.	0.00289	n.a.	1000	0									
36	eGaaS	EGS	64,000	12/15/2016	n.a.	n.a.	n.a.	1000	0									
37	Roundcoin	ROUND	96,338	12/18/2016	n.a.	n.a.	n.a.	1000	0									
38	Bankcoin	BANKCOIN	1,000,000	12/19/2016	0.25000	0.00476	-98%	1000	-981									
39	Hacker Gold	HKG	645,000	12/21/2016	0.04004	n.a.	n.a.	1000	0									
40	PRCOIN	PRCOIN	823,340	12/21/2016	n.a.	0.00012	n.a.	1000	0									
41	BlockCDN	BCDN	303,000	12/25/2016	n.a.	n.a.	n.a.	1000	0									
42	Darcus	DAR	297,426	12/26/2016	0.02000	0.01774	-11%	1000	-113									
43	ebits	EBZ	285,035	12/26/2016	0.00000	n.a.	n.a.	1000	0									
44	Bitconnect	BITBitconnectNE	450,289	12/31/2016	n.a.	n.a.	n.a.	1000	0		Y	Y		Y	Y		Y	Y
45	Branch	BLT	n.a.	12/31/2016	n.a.	n.a.	n.a.	1000	0									
<b>TOTAL</b>			<b>36,336,274</b>					<b>45,000.00</b>	<b>314,420.80</b>	<b>18</b>	<b>3</b>	<b>1</b>		<b>1</b>	<b>1</b>		<b>2</b>	<b>1</b>
in percentage								100%	698.7%	40.0%	6.7%	2.2%		2.2%	2.2%		4.4%	2.2%
Sum of n.a.'s:			3,032,367					Total ROI	538.71%									
% of total raised:			3.3%					Annualized R	164.33%									

by several hundred percent, it would not get close to the than established previously: These 22 cases would account for 49% of the ICOs observed and not for 80% as reported formerly [4].

### 7.1 Survival

At the same time, the worst-case failure rate of 49% may not be idiosyncratic to the field of ICOs. 51% survivors is relatively close to the above mentioned 60% survival rate for NTVs. Literature provides abundant evidence that other factors may also contribute to such high failure rates in similar settings. A plethora of factors can influence an organisation's performance and thus ultimately its survival. The number of potential antecedents to a firm's performance is large, especially if the company is not only of young age but especially if it ventures into international markets. This is typically the case with organisations conducting an ICO. Research has shown that companies of a young age are subject to higher failure rates than older ones. A substantial number of small firms typically fail early on after their inception [21, 22] because they suffer from what scholars call "liability of newness" [23]. At the same time,

it was established that companies which enter a foreign institutional environment suffer from "liability of foreignness" [24]. Consequently, ICOs typically suffer from those two disadvantages at the same time. Previous research has shown that companies of a young age are subject to higher failure rates than older ones. A substantial number of small firms typically fail early on after their inception [21, 22] because they suffer from what scholars call "liability of newness" [23]. This concept suggests that young firms are particularly vulnerable to mortality because they still have to generate the necessary routines, relationships, and reputations that are required to efficiently operate in their respective surroundings [23]. Drawing on the findings of Lumpkin et al. [25] Sapienza, Autio, George and Zahra [26] allege that young firms are more likely to exhibit an entrepreneurial orientation to internationalization, which results in a higher risk-taking proclivity, greater propensity to innovation and a more proactive stance, yet they point out that these firms have a very limited stash of reserves which makes them extremely vulnerable in case of organizational mistakes. Anand and Delios [27] and Hamel et al. [28] contend that over time firms will increasingly be able to utilise their reputation, brand, marketing channels, social capital, company culture and

customer loyalty to ease disruptions caused by the business environment or by internal mistakes.

Companies that enter the international domain are typically confronted with a range of costs associated with their expansion. Typically, such costs include learning costs, but more specifically also adjustment costs for adapting to the foreign environment [24]. Foreign entrants typically display a lack of familiarity with legal, social, and economic conventions, as well as consumer preferences and cultural features of the targeted foreign markets. In addition, firms that enter foreign markets are typically obliged to modify their routines and processes to properly operate within these markets. Whilst these companies typically do benefit from the experience they had previously made with market entries when further entering subsequent markets [29], these companies are nonetheless faced with the task of adapting some of their existing processes and creating some new ones in order to optimally serve this foreign market. Creating those routines and adapting others will consume additional resources [30]. These costs can be significant and enduring and in the worst case fatal to the venture [31]. Besides, companies regularly incur yet additional costs associated with their internationalization. These costs stem from an increased organizational and environmental complexity which leads to additional costs for governance, coordination, and transaction that may outweighing the benefits gained from internationalization [32]. Lastly, internationalization increases ventures' exposure to financial and political risks resulting from currency fluctuations, governmental directives, and trade regulation [33, 34].

Taken together liability of newness and liability of foreignness can pose severe obstacles to new ventures conducting business internationally. Sleuwaegen and Onkelinx [35] established that 29% of their surveyed international new ventures had to withdraw from the international market place and, as a consequence, failed to survive altogether.

## 7.2 Financial performance

The results pertaining to the financial performance of the ICO also yielded some interesting insights. As mentioned before, assuming a worst-case scenario an investor investing in all tokens throughout the 2016 ICO vintage would have suffered a total loss for many of them. However, those tokens which survived would have handsomely compensated for those losses. As mentioned above, an evenly distributed portfolio of ICO tokens would have yielded an interest of approximately 164% p.a. or 598.71% total return over the ca. two-year period. Despite all controversy, it may even occur justifiable to the rational investor to be scammed in individual cases as long as other portfolio components display the growth in value leading to the above returns. Of course, caveat emptor remains true and historical performance was seldom a good predictor of future performance. Other recent ICO research focusing on historical returns during the same period could be an indication of bubbles [36] which explain these abnormally high returns after such a short period, even in the start-up space.

## 8. Limitations and future research directions

This study is not exempt from limitations which in turn enable other researchers to contribute. We encourage further studies on scams in the crypto sphere considering variations in the methodological as well as empirical setup. Moreover, as our study is solely an ex-post observation which is only of limited utility to crypto investors, we issue a call to put a larger emphasis on investigating the antecedents of scams.

### 8.1 Methodology

Mitnick [8, p.9] maintains that so-called “collapsed relations” where Agent and Principal are identical are not in the scope of the PAT. Consequently, one could argue that differences may exist between a more community-based, more decentralised ecosystem, such as Bitcoin and pure for-business entities that use the ICO mechanism as a means of funding their proprietary business. In the context of Blockchain, such relationships are best depicted as “interwoven decentralisation” where ICO teams, ecosystem users, and token holders can be both Principals and Agents at the same time. Borders may not be as clearly defined as initially assumed, leaving the subject interlocked as depicted in Figure 2.



Figure 2: Principal and Agent in the context of cryptocurrencies & interwoven decentralization

Building on the findings of Mitnick [8] further aspects of PAT offer additional research directions in the context of ICOs. We consider the following four topics as particularly noteworthy. First, as Mitnick [8, p.17] puts it “[a] rational party would not enter into a contract if he/she did not expect it to be fully and perfectly operative, i.e. all parties will abide by it (Alternatively, of course, the party may expect the contractual arrangement to malfunction to his benefit)”. Henceforth, the research questions arise whether ICO teams understand that a SAFT contract - which virtually does not contain any investor rights - will indeed malfunction? Moreover, does this understanding of the extremely skewed risk-taking by the Principal, turn ICO teams into scammers? Secondly Mitnick [8, p.17] points out that “[t]he rational contracting party with preference characterised by some measure of risk aversion, i.e. security rather than adventure, will demand that some guarantees or assurances accompany the contract.”. Here, the following research questions emerge: Does this suggest that most ICO investors are indeed not rational since “assurances and guarantees” are most commonly missing in current SAFT agreements? How can this be aligned with current research on asset-bubbles such as Zetzsche, Buckley, Arner and Föhr [37]? Thirdly, Mitnick [8, p.18] argues that valid agreements should be kept. Validity requires an absence of ... fraud or deceptions”. Building on the previous research questions we therefore ask whether a SAFT without investor rights be considered a “valid” contract? Furthermore, we suggest considering the consequences if it was

not a valid one. Fourth, throughout this study we have focused on the Principal as the investor and token holder and the Agent representing the token issuer and ICO teams. Consequently, there is the opportunity to expand ICO scam research to other actors in the ecosystem such as centralised exchanges, market makers and actors on social media aiming to deceive potential investors through misleading statements and false offerings. Fraudulent market practices in today's securities markets such as "Pump and Dump" as observed by Li, Shin and Wang [38] in the crypto-currency markets may be considered a scam.

## 8.2 Empirical Setup

As outlined above the basis of our empirical research was the 2016 cohort of ICOs. The subsequent years, 2017 and 2018 displayed a vast increase in ICOs. Hence, the most obvious opportunity to build on our research is to replicate our study with data comprising those two vintages. While the total amount of ICO projects increased drastically, it remains to be seen if the percentage of scams changed as well.

## 8.3 Antecedents to scams - The Crypto Scam Probability Index (CSPI)

In order to warn investors of scams ex-ante, we would welcome any research contributing to a Crypto Scam Probability Index (CSPI) in order to potentially spot dubious projects before investors put their money into them. The underlying notion is to create a mechanism that can be used to protect investors from bad actors. A comprehensive set of meaningful factors for such an index would need to be established. Yet, first indicators have already been raised by journalists [39], being 1) plagiarism, 2) identity theft and 3) advertising of improbably returns. Clearly, we foresee that this set is extensible for numerous factors such as whether SAFTs had been used, how much have been raised, whether developers are actively working on the project etc. Applying hierarchical regression analysis [40] and /or necessary condition analysis [41] to the 2017 cohort of ICOs researchers could empirically identify relevant factors predicting ICO scams.

For illustration purposes we suggest designing the CSPI along the following lines:

$$\Pi_{SCAM} = \sum \frac{1}{a}SU + \frac{1}{b}AR + \frac{1}{c}DA + \frac{1}{d}KD + \frac{1}{e}VE + \frac{1}{f}SO + \dots + \frac{1}{z}XY$$

For each factor coding and weighting according to its importance in the context of ICO scams is required, where  $\sum a, b, c, d, e, f, \dots, z \equiv 100$  and where the variables capture the following facts (not comprehensive!)

SU: SAFT was used (no = 0; yes =1)

AR: amount of funds raised (USD 0-15m = 0; >USD 15m =1)

DA: developers are active (no = 0; yes =1)

KD: KYC on clients is done (no = 0; yes =1)

VE: vesting is required (no = 0; yes =1)

SO: code is open source (no = 0; yes =1)

XY: other factors

## Conclusion

So far, literature yields only limited insights on scams in the context of ICOs. This paper enhances our knowledge about this phenomenon, contributing to existing cryptocurrency research. Using a global sample, this study has revealed that the magnitude of ICO scams is much smaller than initially anticipated. The article offers alternative explanation for the allegedly poor performance of ICOs by relating them to studies from entrepreneurship literature. Moreover, this paper sketches a possibility of how scams could be more easily identified ex ante in the future.

## References:

- [1] P. Schueffel, *The Concise Fintech Compendium*, Fribourg: School of Management Fribourg, 2017.
- [2] A. de Jong, P. Roosenboom, and T. van der Kolk, "What Determines Success in Initial Coin Offerings?," *Available at SSRN 3250035*, 2018.
- [3] ICO Rating, *ICO Market Research Q3 2018*, ICO Rating, Saint Petersburg, 2018.
- [4] S. Dowlat, *Cryptoasset Market Coverage Initiation: Network Creation*, 2018.
- [5] K. Rooney. "Bitcoin is the 'mother of all scams' and blockchain is most hyped tech ever, Roubini tells Congress," 11 January 2019; <https://www.cnbc.com/2018/10/11/roubini-bitcoin-is-mother-of-all-scams.html>.
- [6] F. Gheorghe. "A Bitcoin Maximalist Just Compared Proof Of Stake To The Fed (And Why This Isn't The Case)," 11 January 2019; <https://beincrypto.com/a-bitcoin-maximalist-just-compared-proof-of-stake-to-the-fed-and-why-this-isnt-the-case/>.
- [7] J.-J. Laffont, and D. Martimort, *The theory of incentives: the principal-agent model*. Princeton university press, 2009.
- [8] B. Mitnick, "The theory of agency: A framework," 1975.
- [9] Oxford English Dictionary, "scam, n.," *Oxford English Dictionary Online*, 27. November, Oxford University Press, 2018.
- [10] Merriam-Webster, "scam, n.," Merriam-Webster Inc., 2018.
- [11] Black's Law Dictionary, "What is FRAUD?," *The Law Dictionary*, Sureswift Capital, 2018.
- [12] A. Timmons Jeffrey, and S. Spinelli, "New Venture Creation," *Irwin, Homewood III*, 1990.
- [13] M. Song, K. Podoymitsyna, H. Van Der Bij, and J. I. M. Halman, "Success Factors in New Ventures: A Meta-analysis\*," *Journal of Product Innovation Management*, vol. 25, no. 1, pp. 7-27, 2008.
- [14] ICODATA.io, "ICO Status," 2018.
- [15] TokenMarket, "Past ICOs," TokenMarket Ltd., 2018.
- [16] ICO Bench, "Browse ICOs," 2018.
- [17] Coin Index, "Browse Initial Coin Offerings," ICOindex.com, 2018.
- [18] ICO Watch List, "Welcome to the ICO Watch List!," 2018.
- [19] Coingecko. "ICO," 10 December, 2018; <https://www.coingecko.com/en/ico>.
- [20] LexisNexis, "LexisNexis, the world's leading provider of news, business and legal information," RELX Group, 2018.
- [21] J. E. Everett, and J. Watson, "Do small businesses have high failure rates? Evidence from Australian retailers," *Journal of Small Business Management*, vol. 34, no. 4, pp. 45-62, 1996.
- [22] W. M. Ladzani, and J. J. van Vuuren, "Entrepreneurship training for emerging SMEs in South Africa," *Journal of Small Business Management*, vol. 40, no. 2, pp. 154-161, 2002.



- [23] A. L. Stinchcombe, "Social Structure and Organizations," *Handbook of Organizations*, J. G. March, ed., pp. 142-193, Chicago: Rand-McNally, 1965.
- [24] S. Zaheer, "Overcoming the liability of foreignness," *Academy of Management Journal*, vol. 38, no. 2, pp. 341-363, 1995.
- [25] G. T. Lumpkin, and G. G. Dess, "Clarifying the entrepreneurial orientation construct and linking it to performance," *Academy of Management Review*, vol. 21, no. 1, pp. 135-172, 1996.
- [26] H. J. Sapienza, E. Autio, G. George, and S. A. Zahra, "A capabilities perspective on the effects of early internationalization on firm survival and growth," *Academy of Management Review*, vol. 31, no. 4, pp. 914-933, 2006.
- [27] J. Anand, and A. Delios, "Absolute and relative resources as determinants of international acquisitions," *Strategic Management Journal*, vol. 23, no. 2, pp. 119-134, 2002.
- [28] G. Hamel, and C. K. Prahalad, "Strategy as stretch and leverage," *Harvard Business Review*, vol. 71, no. 2, pp. 75-84, 1993.
- [29] F. Vermeulen, and H. G. Barkema, "Learning through acquisitions," *Academy of Management Journal*, vol. 44, no. 3, pp. 457-476, 2001.
- [30] W. Mitchell, J. M. Shaver, and B. Yeung, "Foreign entrant survival and foreign market share: Canadian companies' experience in United States medical sector markets," *Strategic Management Journal*, vol. 15, no. 7, pp. 555-567, 1994.
- [31] J. V. Singh, R. J. House, and D. J. Tucker, "Organizational change and organizational mortality" *Administrative Science Quarterly*, vol. 31, no. 4, pp. 587-611, 1986.
- [32] S. Zaheer, and E. Mosakowski, "The dynamics of the liability of foreignness: A global study of survival in financial services," *Strategic Management Journal*, vol. 18, no. 6, pp. 439-663, 1997.
- [33] A. K. Sundaram, and J. S. Black, "The environment and internal organization of multinational enterprises," *Academy of Management Review*, vol. 17, no. 4, pp. 729-757, 1992.
- [34] D. M. Reeb, C. C. Y. Kwok, and H. Y. Baek, "Systematic Risk of the Multinational Corporation," *Journal of International Business Studies*, vol. 29, pp. 263-279, 1998.
- [35] L. Sleuwaegen, and J. Onkelinx, "International commitment, post-entry growth and survival of international new ventures," *Journal of Business Venturing*, vol. 29, no. 1, pp. 106-120, 2014/01/01/, 2014.
- [36] H. Benedetti, and L. Kostovetsky, "Digital tulips? Returns to investors in initial coin offerings," *Returns to Investors in Initial Coin Offerings (May 20, 2018)*, 2018.
- [37] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators," *University of Luxembourg Law Working Paper*, no. 11, pp. 17-83, 2017.
- [38] T. Li, D. Shin, and B. Wang, "Cryptocurrency pump-and-dump schemes," *Available at SSRN*, 2018.
- [39] The Wall Street Journal. "A Flood of Questionable Cryptocurrency Offerings - Search for hundreds of projects showing signs of plagiarism, identity theft and promises of improbable returns," 09 January, 2019; <https://www.wsj.com/graphics/whitepapers/>.
- [40] J. F. Hair, R. L. Tatham, R. E. Anderson, and W. Black, *Multivariate Data Analysis*, 5th Edition ed.: Prentice Hall, 1998.
- [41] J. Dul, "Necessary Condition Analysis (NCA)," *Organizational Research Methods*, vol. 19, no. 1, pp. 10-52, 2015.

<sup>i</sup> We accounted for any fraud case, independent of its regulatory status, i.e. whether it is an unregulated utility token or a regulated security token.

<sup>ii</sup> The Simple Agreement for Future Tokens (SAFT) is a contract offered by ICO teams to investors. It conveys the rights in tokens prior to the development of the tokens' functionality.